A Comparative Analysis of the Prevention and Control of Electronic Crime in the Financial Sector

Cyber Risk Management

The full names of the author	Emiko SAITO, BA LL.M
The qualification for which the thesis is submitted	Doctor of Philosophy
The name of the institution to which the thesis is submitted	Sir John Cass Business School
The department or organisation in which the research was conducted	Faculty of Finance
The month and year of submission	September, 2003

CONTENTS

VOLUME I

VOLUME II

List of Figures and Tables

Figures

Tables

Acknowledgements

The author has been supported by many institutions and individuals. She could not have completed her research without their generous support.

At first, her grateful thanks are due to the Anglo-Japanese Centre for Financial Regulation for granting her research. She personally owes a profound debt to Dr Chizu Nakajima, Director, the Anglo-Japanese Centre for Financial Regulation, City University Business School, who directed and supervised her throughout. She also gratefully acknowledges the support of Professor Barry Rider, Director of the Institute of Advanced Legal Studies, University of London and Fellow of Jesus College, University of Cambridge, not only for his constant concern but also for the fact that he introduced her to doctoral research.

She was given a great deal of advice and support by scholars and colleagues. In particular, she would like to thank Professor Gerry Dickinson and Dr Chris Person, City University Business School, Dr Richard Vogler, Senior Lecturer in Law, University of Sussex, and Dr Mahmood Bagheri and Dr Mohammed Nurullah, Research Officer, Officers, the Anglo-Japanese Centre for Financial Regulation. Thanks also to Ms Annette Whittaker, Ms Susan Farren and Ms Catherine Stokes, Secretary to the Anglo-Japanese Centre for Financial Regulation, and Mrs Margaret Busgith, PhD Course Officer, for their valued support. Ms Phoebe Collins, Mrs Annabel Connellan and Ms Poly Victoros saved several errors and inaccuracies along the way.

The research was completed by the courtesy of all the following institutions and individuals: Mr M. Norris, Manager, Hiscox Technology of Hiscox, Mr Philip Titley, Divisional Director (Non Marine Division), Prentis Donegan & Partners Limited, Mr H Emura, Senior Researcher, Mr H Fujita, Senior Researcher, Mr H Ogura, Manager, Security & Audit Research Dept., Mr K Taniguchi, Senior Researcher, Mr M Tachikawa, Senior Researcher, Electronic Banking Research Dept., and Mr S Watai Senior Researcher, General Research Dept., the Centre for Financial Industry Information Systems (Japan), Mr A. Trenton, Solicitor, Taylor Wessing, Mr M. Uchiyama, Head of Stock Market Department, and Mr K. Yoshida, Head of Foreign Stock Group, Listing Department, Tokyo Stock Exchange (Japan), Mr S. Takenaka, Deputy Chief Representative, Tokyo Stock Exchange, Inc. (UK), Mr N. Uemura, senior analyst in Japan Rating and Investment Information, Inc., Mr K Hori, Insurance division, Supervisory Dept., Mr H. Naka, Director, Non-Bank Finance Companies Office, Banks Division II, Supervisory Department, Financial Services Agency (Japan), Mr T. Uranishi, Deputy Director General, Supervisory Department, Mr N. Hara, Director and General Manager, Mr J. Sugita, Manager of International Department, and Mr A. Hozumi, Manager, Research and Development Department 2, the Marine and Fire Insurance Association of Japan, Inc., Mr T. Ichiki, Manager,

Corporate Planning Department, and Mr M. Takahashi, Assistant manager, Liability Insurance Group, Commercial Lines Underwriting Department, Mr T. Nagai, Assistant Manager, New Interactive Information & Solution Planning Office, Information and Space Dept., the Tokyo Marine and Fire Insurance Co. Ltd., Mr F. Ohkawabata, Manager, and Mr T. Matsuura, Chief Underwriter, Property and Casualty Underwriting Group, Products and Services Development Department, the Chiyoda Fire and Marine Insurance Co. Ltd., Mr S. Takano, Manager, and Mr H. Okumura, Assistant Manager, Liability Division, Fire and Casualty Department, Mr K. Morita, Assistant Manager, Property Underwriting Division, Fire and Casualty Department, and Mr T. Tsuda, Assistant Manager, Commercial Lines Planning and Consultation Department the Sumitomo Marine and Fire Insurance Co. Ltd., Mr Y. Takase, Assistant Manager, Liability Insurance Group, Non-Marine Underwriting Department, Mitsui Marine and Fire Insurance Co. Ltd., Mr A. Okabe, Manager, Liability and Casualty Section, Property and Casualty Underwriting Department, Mr T. Amagai, Deputy Manager, Commercial Property Section, and Mr H. Iritani, Assistant Manager, Liability Insurance Division, Liability and Casualty Section, Property and Casualty Underwriting Department, the Yasuda Fire and Marine Insurance Co. Ltd, Mr Y. Fujita, Manager of Production & Underwriting Department, Lloyd's Japan, Mr C. Brown of Financial Institutions Underwriting and Mr L. Fielder of Manager, Professional Lines, Zurich London Limited, Mr R. Coello, Account Executive, and Mr J. Naish, Advisor of Global Financial & Executive Risks Practice, Willis Limited, Ms S. Alton of Safeonline Limited, Mr T. Matsumura, Regional Manager of Japanese Business Division, AIG Europe (UK) Limited, Mr N Iwashita, Manager, Institute for Monetary and Economic Studies, Bank of Japan, Mr Y. Miyai, President, Mr T. Yoshida, Managing Director, Mr M. Komura, Director of Planning Division, Mr H. Doumen, Group Chief and Mr T. Miyagawa of Planning Devision, Japan Net Bank, Mr M. Inoue, Group Chief and Mr S. Yanagi, Vice president of IT Planning Department, Sumitomo Mitsui Banking Corporation, Mr T. Okada, General Manager and Mr M. Matsumoto, Member Firms Department, Japan Securities Dealers Association, Mr A. Morikawa, Managing Director, JISA Business Support Co., Ltd., Y. Yamaka, General Manager of Global Transaction Services Planning Division and M. Yamaguchi, Assistant to the General Manager of IT Planning Office, The Dai-Ichi Kangyo Bank, Limited, Ms Jackie Knight, Senior Consultant, BIS North Region - Strategy & Change, IBM Global Services, Mr Eric Westacott, SwissRe, Mr H. Kindaichi, Deputy Chief Representative in Europe, Mr S. Kobayashi, Representative in Europe, Bank of Japan (UK), Ms C. Dandridge, Active Underwriter, Syndicate 609, Atrium, Dr M. Fujimoto, Consultant, Research & Consulting Dept.4, the Sumitomo Marine Research Institute, Inc., Mr K. Goto, Senior Research Fellow, Mitsui Kaijyo Research Institute, Mr I. Harrison, Specialty Lines, Beazley, Mr K. Tagaya, Deputy Manager, Mr K. Inaba, Manager of Casualty Group, Non-Marine Underwriting Dept., the Taisei Fire & Marine Insurance Co., Ltd., Mr Y. Nagatani, Manager, Mr T. Inoue, Manager, Casualty Insurance Division, Product Design & Development Dept., the Dowa Fire & Marine Insurance Co., Ltd., Mr S. Imagawa, Manager, Legal

Department, Nomura Research Institute, Ltd., Mr Y. Kimura, Deputy Director-General, Tax Bureau, Ministry of Finance, Mr M. Kamakura, Technical Manager of Fire & Casualty Insurance Section, Underwriting Department, Mr T. Yae, Mr S. Nagata, Manager of Fire & Casualty Insurance Section, Products Development Department, Mr T. Sugiyama, Superintendent, Fire & Casualty Insurance Section, Underwriting Department, the Fuji Fire & Marine insurance Co., Ltd., Mr S. Kandatsu, Underwriter, Mr H. Yamanaka, Chief Underwriter, Liability Insurance Division, Property & Casualty Underwriting Department, the Nippon Fire & Marine Insurance Co., Ltd., Ms M. Kitamura, Assistant Manager of Non-Marine Underwriting Dept., the Koa Fire & Marine Insurance Co., Ltd., Mr Y. Miyakawa, Mr Y. Sato, Researcher, Planning Office, Mr M. Kobayashi, Director, IT Security Centre, Information-Technology Promotion Agency, Japan, Mr K. Murakami, Deputy Manager, Non-Marine Planning Group, Production Planning & Underwriting Department, Kyoei Mutual Fire & Marine Insurance Company, Mr T. Mori, Manager, Information Risk Management, KPMG Business Assurance Co., Ltd., Mr N. Oguro, Senior Manager, KPMG Financial K.K., Mr M. Moroi, Director, Japan England Insurance Brokers Ltd., Mr Y. Oogane, Deputy Manager, Property Division, the Tokyo Marine Risk Consulting Co., Ltd., Mr T. Sato, Mr M. Matsubara, Deputy Manager, New Product Group, Nichido Fire & Marine Insurance Co., Ltd., Mr G. P. Rutledge, Deputy Chief Counsel, Pennsylvania Securities Commission, Ms J. Rhodes, Vice President, J.P.Morgan & Co., Incorporated, Minister T. Shikibu (Finance), Embassy of Japan (London), Mr K. Shimada, Deputy General Manager, Products Development Department, the Dai-Tokyo Fire and Marine Insurance Co., Ltd., Mr J.F. Threshie, Development Director, Lloyd's Japan, Mr M. Tanaka, Senior Economist, Business Planning Department, Japan Centre for International Finance, Dr K. Ueda, Professor of Risk and Insurance, Department of Commerce, Sensyu University, Mr H. Urano, Deputy Manager, Hachijûni Bank.

Her thanks are also offered to her referees, Mr Norihiko Maeda, Mr Katsumi Hirano, Mr Atsutoshi Oshima, Mr Akio Kawaguchi, Mr Katsuya Motizuki and Dr Guglielmo Verdirame.

Many others have supported and rallied both professionally and privately: Ms Felicite Douce De La Salle, Ms Julia He, Ms Isabelle Dervaux, Ms Tracy Paradise, Mr and Mrs Paul and Yoko Griffiths, Mrs Toshiko Trenton, Ms Daniela Richino, Ms Carmen Davila Gaza, Mrs Meiling Huang, Ms Minako Toru, Ms Kazumi Ishii, Mrs Tomoko Amano, Ms Masumi Ohboshi, Mrs Mie Itaya, Ms Kyoko Tsuda, Ms Nicole Thompson, Mrs Emiko Nakamura, Ms Keiko Okabe and Mr Minoru Yubuchi.

While in the UK, she received enormous support from Mr and Mrs Chris and Colette Turton, Mr and Mrs William and Sylvia Boyce, Mr and Mrs Tony and Ros Tiernan, Mr and Mrs Richard and Rosanna Fullerton, Mr and Mrs Mike and Penny Weeden, Dr Colin and Mrs Mary Bullough, Mr and Mrs Kennedy, Mrs Margot Bylo and Mr and Mrs Tim and Val Whittaker. Their

warm wishes were always encouraging.

She cannot end without thanking her father, brother, sister, brother-in-law, nephew and niece for their support and patience. Without their understanding, she would never have commenced her research.

Thanks again for the support and kindness of all who helped her. This work is dedicated to the memory of her mother.

Emiko SAITO

Kawasaki, Japan
December 2002

Declaration

I grant powers of discretion to the University Librarian to allow this thesis to be copied in whole or in part without further reference to me. This permission covers only single copies made for study purposes, subject to normal conditions of acknowledgement.

Abstract

Businesses constantly face a variety of crises which could result in the loss of financial resources and good reputation: human error, crime, employees' unlawful behaviour, technical failure and the like. These are all categorised in one word: "risk". With the rise of cyberspace, new risks have come into existence and interest in this issue is significant. With regard to risk management, the financial industry, a core business that no company can do without, is likely to be one-step ahead of other industries. Thus, in this thesis I have chosen to examine and compare the management of cyber risk in the financial industries of Japan and the UK.

Some types of risk, such as human error and technical failure, are likely to occur accidentally, but it is necessary to analyse others, particularly crime and unlawful behaviour. Through the comprehension of risk types, we can understand how each risk management method works.

As for the suggested risk management methods, the thesis begins by discussing how criminal and civil law and regulation deal with risk. However, law and regulation are not the perfect solutions for businesses. An alternative is insurance. Since the 1980s, insurance industries in Japan and the UK have developed products to deal with computer crime or cyber risk. The most popular method is to strengthen computer security. It is also crucial to resuscitate the morality and ethics of employees and firms themselves. The development and spread of the concept of operational risk worldwide is to encourage firms to deal with the situation. Outsourcing, Alternative Risk Transfer, Alternative Dispute Resolution and other new technology are also discussed as risk management methods.

To prove that cyber risk is avoidable by the application of these methods and theories, there are two issues which need to be discussed: cyber money laundering and account aggregation services.

It is essential to be aware that cyber risk is unique for each individual firm and industry, so there is no single risk management method against cyber risk. Therefore, it is important to ascertain which methods are practical for each firm and combine them like a patchwork.

List of Abbreviations

ADR	Alternative Dispute Resolution
Aggregation	Account aggregation services
ART	Alternative Risk Transfer
ATC	Australian Telecommunications Commission
BBB	Bankers Blanket Bond
BBS	Bulletin board system services
BCCI	Bank of Credit and Commerce International
BIS	Banks for International Settlement
BSI-DISC	British Standard Institute — Delivering Information Solutions to Customers
CCI	Computer Comprehensive Insurance
CCP	Computer Crime Policy
CD crime	Crime using a cash dispenser
CDL	Calvin Designer Label
Chubb	Chubb Group of Insurance Companies
CMA	Computer Misuse Act 1990
CDPA	Copyright Designs and Patents Act 1988
CRDR	Copyright and Rights in Databases Regulations 1997
D&O	Directors & Officers Liability Insurance
Destination site	Aggregator's website
DIC	Difference-in-Conditions coverage
DIL	Difference-in-Limits coverage
DKB	Dai-Ichi Kangyo Bank
DNS	Domain name system
DPA	Data Protection Act 1998
DTI	Department of Trade and Industry
E-commerce	Electronic commerce
E-money	Electronic money
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation of USA
FIB	Financial Institution Bond
FISC	The Centre for Financial Industry Information Systems of Japan
FSA	Financial Services Authority of the UK
G8	State of Government of the eight major industrialised democracies
Host website	Targeted institution's website
IBJ	Nihon Kôgyô Bank (the Industrial Bank of Japan)
IC	An integrated circuit
ICAEW	Institute of Chartered Accountants in England and Wales
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organisation for Standardization
IT industry	Information and Communication Technology industry
JFSA	Financial Services Agency of Japan
JIPAC	Japan Intellectual Property Arbitration Centre

JNB	Japan Net Bank
Kangin	Dai-ichi Kangyô Bank
KYC	Know Your Customer
LSE	London Stock Exchange
METI	Ministry of Economy, Trade and Industry
MFG	Mizuho Financial Group
Mitsui	Mitsui Marine and Fire Insurance Co. Ltd.
MoJ	Ministry of Justice
NPA	National Police Agency
OECD	Organisation for Economic Cooperation and Development
Playboy	Playboy Enterprises Inc
PIP	Professional Indemnity Policy
SMBC	Sumitomo-Mitsui Banking Corporation
Sumitomo	Sumitomo Marine and Fire Insurance Co. Ltd.
The association	The Marine and Fire Insurance Association of Japan, Inc.
The Committee	The Basel Committee on Banking Supervision
The New Accord	The New Basel Capital Accord
Tokyo Marine	Tokyo Marine and Fire Insurance Co. Ltd.
TSE	Tokyo Stock Exchange, Inc.
UCAL	Unauthorized Computer Access Law
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
UNDCP	UN International Drug Control Programme
UN manual	United Nations manual on the prevention and control of computer-related crime
WIPO	World Intellectual Property Organisation
WWW	World Wide Web
Y2K	Year 2000 (or Millennium) Bug problem
Yasuda	Yasuda Fire and Marine Insurance Co. Ltd.

Table of Cases

UNITED KINGDOM

UNITED STATES

List of National Legislation and International Convention

UNITED STATES

FRANCE

INTERNATIONAL CONVENTION

Introduction

Along with the popularity of computers and the Internet, the mass media have introduced "computer crime" as a fashionable phrase. Crime has become complicated by the development of technology, and the law has been struggling to combat a new type of crime. In fact, the loss caused by hackers and computer viruses reached 1.5 trillion dollars (equivalent to £2.7 billion) in 2000[1]. It is said that

"...although crime might pay, combating it usually doesn't[2]".

Supporting this statement, an Amazon spokeswoman admitted that many fraud cases were simply not investigated[3], due to lack of tangible evidence and the passing of time[4]. If your business is always at risk and you believe that law will not always provide a remedy for losses, what can you do to protect your own business?

After researching the impact of law and regulations on computer crime, the next issue to consider was the sustainability of a company when a crime is committed against it. However, it was evident that computer crime was only at the tip of an iceberg of business vulnerabilities. A company is very likely to face other types of risks much more frequently than computer crime. Business vulnerabilities means any factor or cause that makes a company lose a business opportunity or profits; in other words, a "risk". Those vulnerabilities vary: they could be caused by a company not managing computer software properly in terms of software license agreements, for example. It is sometimes noted that a company does not provide appropriate training for its employees, who may believe their freedom of speech gives them a right to disclose a company's confidential information. This would make a company defenceless, so that anyone, whether an insider or outsider, could commit a crime against a company. Or it may result from an employee's simple error or technical failure. Those factors are ordinarily categorised as an operational risk. These could result in the loss of financial resources and the good reputation of a company to a greater or lesser degree. Nonetheless, the law does not always provide a solution, unless any illegal factors are involved. It is worthwhile examining a more extensive range of risks

---

[1] See 'Hacker Insurance', <http://www.business2.com/content/channels/technology/2001/01/30/25554> (print out on file with author).

[2] See 'Net crime poses challenge to authorities', <http://news.cnet.com/news/0-1007-200-850601.html?feed.cnetbriefs> (print out on file with author).

[3] Amazon spokeswoman Sharon Greenspan said, "We were frustrated with law enforcement because a lot of these cases are small in monetary value...They wouldn't investigate because it didn't meet their criteria to open an investigation." See *ibid.*

[4] Rehman, who investigated high-tech crime for the Florida Department of Law Enforcement for ten years, said, " ...law enforcement's hesitation to combat such fraud has to do with the lack of tangible evidence and the amount of time it takes to investigate. " See *ibid.*

rather than a crime only. Companies must be proactive in avoiding or minimizing any risk to themselves[5].

Considering the sustainability of a company in the face of various risks, there are two major research questions. Firstly, does a risk definitely have a great impact on a company when it is realised? Cyberspace has been a buzzword in recent years. Many people are concerned to some degree; some believe it is risky, some think of it as a business opportunity. If any risk is realised, does a company suffer the loss of financial resources and its good reputation? If the answer to this question is no, it is surely not worth pursuing this research. If the answer is yes, it is critical to provide expedient means for a company to avoid or minimise risks.

What if a bank loses its clients' account information? Most companies keep backup data on a mobile device such as a diskette or CD-ROM. Whether the recorded media is stolen or simply lost, it is self-evident that the company loses its good reputation at once and that it would cost money to recover. Therefore, the answer to the first question is yes: it is highly probable that a company would lose financial resources and its good reputation if any risk were realised. On such an occasion, a company must be able to show its transparent and sound governance to its investors.

What should a company do to be attractive to investors? It is necessary to defrag or optimise risks, which are dispersed all over a company, by using various methods based on a single concept. In reality, all risks cannot be concentrated in one specific department: they are spread throughout the departments and functions of a company whether the staff perceive it or not. Furthermore, the same types of risks could occur in only a few different departments. It is quite likely in the company that a certain risk may be properly managed and the performance improved in X department, whereas Y department, may show a lesser performance as a result of a fiasco in managing the same risk. Therefore, the same types of risks must be defragged under a single concept, and all risks spread throughout the company must be optimised by the best available means, otherwise company optimisation will not work properly.

To conduct company optimisation most effectively, there are five main factors to consider:

(1) Sensitivity
It is critical to be responsive to a new risk;

[5] This thesis focuses on financial institutions in Chapter I.

(2) Adaptability/flexibility
The company must be flexible to variable situations;

(3) Centralisation
To have a single concept is essential;

(4) Resistance
As a result of implementing risk management methods, the company must be highly resistant to risk, and;

(5) Resilience
If a risk is realised, it is crucial that the company has a feasible quick recovery plan.

This research shows the effective methods of avoiding or minimising the impact of a risk. In a society that depends on computer networks, any minor risk could trigger a larger one in the whole market. By conducting the analysis based on two vital questions, the thesis concludes with ideas to build a secure economy.

The research is conducted through a model known as a "containment policy". By attacking risks through different methods, it is possible to avoid or minimise a risk. There are two main pillars of risk management. The first pillar is to seek legal assistance. Organisations, and profit-making companies in particular, are most likely to avoid this assistance for the purposes of keeping up a good reputation. However, concealing involvement in a deplorable or unfortunate affair tends to attract more trouble. It is likely, at such a time, that a criminal may take advantage of a company's reluctance to act. In addition to this, any organisation can be vulnerable to a lawsuit. If a party brings a lawsuit against a financial institution, the latter will end up paying damages as well as having its reputation injured. In reality, there are some cases in which certain companies are actively involved in assisting government authorities. For instance, eBay and Yahoo.com have united in developing standards for the Federal Trade Commission in the USA. It is said that eBay is working with the US regulators[6]. Although law and regulations are sometimes considered to be unfriendly or impractical in actual practice, the aforementioned cases prove that it is possible, through companies' involvement, to change them into something useful. Therefore, it is wise to develop a way of reducing "cyber-risk" in both the present and the future.

---

[6] The author is grateful to Mr M. Norris, Manager – Hiscox Technology of Hiscox, and Mr P. Titley, Divisional Director (Non Marine Division), Prentis Donegan & Partners Limited, for their invaluable comments and advice.

There are two possible approaches in seeking legal assistance: the criminal law approach and the civil law approach. Law and regulations have two aspects in helping to manage risks: firstly, as a deterrent to crime; and secondly, in providing relief measures for an injured party. However, the legal approaches are not always offered, or, if offered, are not timely due to delay in the legal system. It is not unusual that the available countermeasures are insufficient and out of touch with reality.

The second pillar is to seek protection through insurance. Since the late 1990s, insurance products to cover cyber-risk have been available. They are very dynamic and are becoming better known in the financial sector. Purchasing an insurance policy also provides relief measures when a risk is realised. This would also be effective as a guarantee for a business partner. Both the attitudes towards such insurance products and the use of these products in the Japanese and British insurance markets will be analysed in a comparative context.

It is not always possible to avoid cyber-risk completely with the two aforesaid countermeasures: it is possible to define these methods as external risk management methods. There are also internal risk management methods such as outsourcing, following international standards and the like that organisations are able to employ by themselves. It is essential to the implementation of compliance and corporate governance for companies not only to avoid risk but also to exhibit sound business operations to investors. Employing security standards is also an important subject for discussion. One of the critical elements in managing risk is strengthening computer security. Since information technology (IT) is developing at light speed and would be out of date before a discussion of what was currently available could be completed within the thesis, it was decided that it should be excluded from the thesis.

This thesis will be composed of nine chapters with an Introduction and Conclusion. Chapter I, entitled "Risks — A Guide to Business Vulnerabilities", defines the types of risks. By understanding this, it can be clearly shown what companies would potentially lose when risks are realised.

Chapter II, entitled "An Analysis of Cyber-Risk", is focused on risks, mainly in relation to illegal acts. It examines the development of the notions, classification and characteristics of computer crime and its impacts. Public interests and the social impact of illegal acts are discussed in depth. The fundamental methods of risk management are also introduced and pursued in the following chapters.

In Chapter III, "An Analysis of the Scope of Criminal Law", criminal law is the focus. It is critical to analyse how far criminal law can provide

a remedy for companies when they suffer damage from illegal actions. With a comparative analysis of legislative approaches both in Japan and the UK, this chapter also probes international cooperation against crime.

Chapter IV, "An Analysis of Civil Law", considers the three points below, as Japanese civil law and English common law and statutes are analysed:

(1) How does an incident happen?
(2) Which parties are involved?
(3) What legal interests are involved?

Considering the basic principles of civil law in both countries, potential injury to property is categorised into five areas: proprietary privileges, intangible property, domain name system, personal rights and economic losses. Those classifications help to determine what civil remedy is available when business risks are realised.

Chapter V, "An Analysis of the Available Insurance Products in the Japanese Insurance Market", looks at insurance products designed to manage the risks. Since the 1980s, computer comprehensive insurance products have become available in the Japanese insurance market for minimising the impact of computer-related risks. An on-the-spot survey covers practically all the Japanese insurance companies.

Chapter VI, "An Analysis of the Available Insurance Products in the British Insurance Market", is constructed similarly to the previous chapter. Since the British insurance market leads the Japanese market, this chapter also shows the differences between these two markets in particular.

In Chapter VII, "An Analysis of the Various Risk Management Methods", various types of risk management methods other than legislation and insurance are carefully examined. For instance, information technology and the implementation of a security policy for it is indispensable.

From Chapters II to VII, the types of risks and the methods of managing the risks are carefully analysed. Depending upon the type of businesses and the scale, it is essential for companies to select which methods are most appropriate. By establishing the aforesaid methods, the majority of risks become avoidable. This will be proven by examining two entirely different issues: cyber money laundering (in Chapter VIII), and a new financial service called account aggregation services (in Chapter IX). The latter issue is a new business service that may incur losses; the former is a crime risk. These two completely different issues will be good examples to test the analyses conducted in Chapters I through VII.

Account aggregation services are new financial services in the market that have not, thus far, been discussed enough from the viewpoint of risk management. Chapter VIII, "An Application of Cyber Risk Management for Account Aggregation Services", introduced the benefits and drawbacks of the services. Discussing the general and legal issues, the chapter explores the balance of the benefits and risks of such services.

Chapter IX, "An Application of Cyber-Risk Management Against Money Laundering and Cyberspace", focuses on how computers and the Internet could be abused by money launderers. In recent years, money laundering has been targeted by financial institutions in the fight against terrorism and organised crime. Moreover, cyber money laundering has been an issue, although no serious case has yet been reported. In general, computers and the Internet make it easier for criminals to wash dirty money. Financial institutions must be very cautious in order not to fall victim to criminals, and they definitely need to take appropriate preventative measures. This chapter helps financial institutions come up with precautions against future risks.

In the present work, all analysis is to be done comparatively between Japan and the UK[7]. The Japanese government started to reform its financial sector in 1997, which was referred to as the British Reform. Moreover, the Japanese insurance market keeps watching the trends in the foreign insurance market, especially the British market, as Japan has fallen behind compared with Britain. However, it is sometimes true that implementing high technology produces new risks that low technology does not. Therefore, it will be worth researching whether or not the Japanese companies would be able to sustain a loss more so than British companies.

Since these are such recent topics, available sources are very limited. Therefore, the analysis is based on direct inputs such as interviews and exchanges with both the private and public sectors. These inputs were all factual and up-to-date accounts of actions taken and first-hand opinions from the financial market. Questionnaires were also distributed covering a wide range of market participants. Seminars and conferences were good opportunities to exchange information with other scholars as well as to confirm the originality of the research. Existing literature and actual incidents were referenced freely.

In its conclusion, this thesis will attempt to outline a model solution to risk management for financial institutions. By providing various effective risk management methods, each company can customise its own

[7] The US data could be used to show comparisons with the Japanese or British data if there were no available public data in Japan and Britain.

risk management framework in compliance with its business disposition. This will be the quickest method to defrag the risks of not only a financial institution but the whole financial industry also. Moreover, effective risk management methods will be applicable for not only the financial industry but any other industry as well. In consequence, this will help to create a sound economy.

Chapter I: Risks — A Guide to Business Vulnerabilities

To date, many benefits from technology have been enjoyed. A "computer" was not a common object twenty years ago, and "cyberspace" was a word seen only in science fiction novels. Ten years ago, computers were in a transition period as business tools, while cyberspace remained a fantasy. Nowadays, computers are basic tools in both business and the household. By using a computer, a modem and a telephone line, an electrically sent message (widely known as email) is delivered from home to a friend in the office, or even to a stranger on the other side of the globe.

Today, cyberspace is accessible to the vast majority of people in the western world. Nonetheless, perceptions of computers and cyberspace may vary. The majority of people are most likely to relate to the most familiar objects. For instance, there are many types of computers: personal computers, workstation computers, super computers etc. Unlike a television, computers have many different facilities. Some people suggest computers should be defined more precisely. Defining cyberspace is also problematic, because the word refers to space[8]. Hardy defines cyberspace as 'the world of electronic communication on the computer network'[9]. It is however, unnecessary to be cautious about defining computers or cyberspace in this thesis. Firstly, this thesis focuses on financial institutions, therefore here, computers simply refer to business tools used in the daily business transactions of financial institutions. Secondly, the human operator makes decisions, not the actual computer, and the operator is responsible for all consequences.

Cyberspace is also restricted within the perimeter of financial businesses. As previously mentioned, a home Internet user generally accesses the Internet via a modem, telephone line, and personal computer. In the business world, many companies use an Intranet throughout a

---

[8] "Cyberspace" has diverse definitions. For instance, In a website it is defined as "unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is generally used to describe the virtual world of computers", and the other defines as "While cyberspace should not be confused with the real Internet, the term is often used simply to refer to objects and identities that exist largely within the computing network itself, so that a web site, for example, might be metaphorically said to "exist in cyberspace." According to this interpretation, events taking place on the Internet are not therefore happening in the countries where the participants or the servers are physically located, but "in cyberspace".
See 'definition of Cyberspace',
<http://www.sharpened.net/glossary/definition.php?cyberspace> and 'definition of Cyberspace: Word iQ', <http://www.wordiq.com/definition/Cyberspace> (print out on file with author).

[9] There was a movement amongst academic authorities, such as the University of Pittsburgh, USA, to consider the potential danger of Internet crime and a course in "cyberspace law" (not "Internet law") has been launched. "Cyberspace law" is the general word for "Internet law" in the USA, thus, it seemed necessary to define what cyberspace was. See I. T. Hardy, 'The Proper Legal Regime for "Cybespace"' (1994) 55 U. Pitt. L. Rev. 993, in K. Hirano & S. Makino, '*Hanrei Kokusai, Internet hô - cyberspace niokeru houritsu jousiki* (Cyberspace Law: ethics of cyberians and

company (including the branch offices) as a business entity unit. This internal company network is entirely controlled and usually connected, outside the company, under the observation of a particular internal department. While it is common to have an email address on a business card, even if a company has well equipped computer systems, it is not necessary for all employees to have a business-oriented email address. For instance, some Japanese financial institutions restrict email addresses to a certain level of employee. Other institutions restrict outgoing messages. Even if companies do not employ policies like these, they are extremely likely to observe their employees' email usage — whether or not it is reasonable — based on internal policies. It is a well-known fact that a company is technically able to read emails addressed to its employees without letting them know that the email accounts are monitored. However, less well known is the fact that Web-based email services are also vulnerable to privacy violations due to their technical nature[10]. In 1999, Xerox fired approximately 40 of its 92,000 employees, accusing them of spending too much time on "non-Xerox related sites". More specifically, those 40 employees had been browsing pornographic Internet sites at work[11].

The purpose of Internet usage restriction is not initially based on such employee abuse cases. It is mainly a precaution to reduce or minimize the potential risk of problems caused outside the Intranet. By excluding the factor of Internet, some types of risk are eliminated from businesses: hacking, computer viruses, etc. In reality, restricting the email facility would probably not mean missing a critical business opportunity. If so, is it possible to exclude a whole company from cyberspace? Technically, it is possible to do so. The question is whether such exclusion from cyberspace has any consequences. Electronic commerce (hereinafter "e-commerce") is a 'buzzword'. There are huge numbers of predictions and expectations regarding the expansion of e-commerce and any type of Internet transaction. The Internet population is significantly expanding and the majority of people can observe (although not necessarily use) computers almost anywhere, not only in homes or offices, but also in places like an Internet café[12]. On the other hand, it is not simple to describe the expansion of e-commerce, especially compared to the overblown predictions published a few years ago.

---

spirits of self-governance)' (1998) Prosper, Tokyo at 62-63.

[10] See 'Web-based email services offer employees little privacy', <http://news.com.com/2102-1017-246543.html> (print out on file with author).

[11] See 'Xerox fires 40 for online pornography on clock', <http://news.com.com/2100-1001-231058.html?legacy=cnet&feed.cnetbriefs> (print out on file with author).

[12] Previously, it was impossible to access the Internet without computers. However, these days, it is possible to browse websites via mobile phones. Online businesses offering services via mobile phones are not included in this thesis because the suppliers of online services do not supply services from mobile phones. They are merely one of the service channels for consumers.

Apart from the issue of the extent to which e-commerce is invading the proportion of "brick and mortar" stores, e-commerce, at least, will not be completely erased. The crucial reason for the public's reluctance to purchase online is the security issue: the heart of their concerns centers around the safety of inputting credit card details online. The balance of evidence suggests that e-commerce would flourish if a secured method of payment system were established. This would surely be persuasive in diminishing the impression that online shopping and services are insecure. Nonetheless, it may not be a good idea for businesses to stand aside, even if cyberspace is full of uncertainties. It is likely that making a profit from online services over other channels is quite difficult at the present stage. However, offering online services is one of methods with which a "brick and mortar" store facilitates its customers. A typical example of this is financial institutions.

Financial institutions actively market online financial services. For instance, insurance companies have started to deal in insurance products online; securities firms offer online services; banks offer online banking etc. The types of online services are, however, not exactly the same as services offered over the counter. Due to current technical, security and/or other reasons, it is not possible for online customers to receive all services. In the case of banks, although there are some incorporeal Internet banks[13], the majority of financial institutions are still "brick and mortar" stores. They offer a range of traditional services both over the counter and online, while offering the rest of their services only over the counter. Specifically, customers have to know exactly what services are available online (or not), and have a good command of using these services. The purpose of offering online services is not necessarily to attract new customers or make a huge profit. It may simply be a nod to competition. This results in all financial institutions having mostly the same services and facilities, and thus they fail to discriminate their businesses from one another. As previously mentioned cyberspace has not yet been entirely explored as a potential market. If online services do not make a profit, it should remain questionable whether the risk of entry into online business outweighs the profit potential. It is a critical decision: whether it is worth taking risk within cyberspace, especially if a company is only offering online services as a gesture. However, if it succeeds in (slightly) changing long-held consumer views, a gesture is interchangeable with prior investment. The current social phenomenon of the world is oriented towards information networking. Even if online businesses do not make a profit at present, the investment is a necessary expense for the future. Making a profit out of cyber business is the next step. Cyberspace is unlikely to be a treasure island; it is wrong to believe that just having a

[13] For example, they are Egg (UK) and JapanNet Bank (Japan).

website will make a business its fortune. Whether the purpose is a mere gesture or prior investment, opening the door of a business to cyberspace is risky for various reasons, and the business needs to be well prepared before taking the existing risks in cyberspace.

Cyber risk — risks existing in cyberspace. What are they? They can broadly be divided into two categories: risk of losing business funds or business opportunities, and risk at being liable for damages. Of course, these categories are not unique to cyberspace, although, as both risk loss of funds or opportunities and present the risk of litigation, most industries loathed them. So, while these categories are important, they are not practical for defining what cyber risk is. When examining cyber risk, any related factor to cyberspace must be considered. In earlier times, cyber risk meant, to some degree, computer crime. The more technology flourishes, the more the potential for damage. Moreover, to make things worse, technology makes committing computer crime easier and detection very difficult. In essence, crime is wrong or anti-social actions, and law and regulation are the means of reducing and discouraging such behavior. This thesis proves that computer crime is a type of "risk" within society. Indeed, to keep a sustainable stabilized economy, it is very important to avoid both the crimes and the damage caused by those crimes, particularly in the financial sector.

However, computer crime indicates an illegal act. In other words, it means there is a risk that anyone can commit an offence. Technically speaking, computer crime does not involve human error or systemic failure. In addition to this, as technology is developed and improved, computer crime simply became an insufficient term to cover a wide range of network-related offences. Therefore, it is appropriate to use the term "cyber risk" as a blanket term, which stems from the use of computers or the network systems regardless of the type of perpetrator (an insider or outsider) or occasion (an offence, error or failure).

The financial industry is a core industry anywhere in the world. It is a cogwheel amongst all industries. As such, if this gear deviates from its normal routine, not only other industries but also the nation itself would experience a serious impact. Under the present situation, wherein the economies of the vast majority of nations are intimately related, the world economy would be likely to suffer a financial panic. Indeed, governments, desperate to achieve soundness in their economy in their countries, place considerable attention on cyber risk. Why should the financial market be protected from cyber risk? What would happen if businesses were harmed?

xactly what considerable damage would materialize because of cyber risk? There are at least three significant factors protecting financial

sectors from cyber risk. Firstly, tax revenues and the integrity of the financial market should be considerable issues for governments. There is no doubt that governments are very keen on levying a tax on companies. When a company fails to protect itself from cyber risk — even if it is a small business — it may affect not only that company but also the financial market. For example, it seems reasonable that a certain company reduces revenue. Consequently, tax revenue for the government automatically reduces. Even if the company's revenue does not reduce because of this incident, a certain regulation may allow the company to apply an exemption clause of tax. Secondly, the market is vulnerable to any rumor or criminal act. It is not an exaggeration to say that a small-scale influence might develop into a large undesirable impact on the market. The trigger that leads to a mess in the market is always a trivial issue; the more the world complicates information, the more a small issue is likely to confuse the market. This leads to currency instability, therefore impeding the integrity and stability of the market, and may cause a monetary crisis. Consequently, a government obviously loses its integrity. Additionally, the effects may make it difficult for foreign investors to return. The third factor is the actual cost of combating crime and the realistic amount of damages from such criminal acts. Such cost is unproductive but necessary to prevent crime being committed. If justice and fairness, together with freedom, prevailed in the financial market, its soundness would be enhanced. Furthermore, the public welfare of the general public is protected as a result.

As previously mentioned the financial market has adopted technology and already offers online services. In particular, banks hastened toward introducing Internet banking services to their customers. Compared to other types of online services and e-commerce websites, banking has some peculiarities. Internet banking services are easy to sign up for, as long as one has an ordinary bank account. With a traditional physical bank account, the bank customers would not always worry whether their deposits are secure. They would probably not even worry about a bank robbery because this does not necessarily mean that your money has been stolen. If you go to the bank the next day, you are likely to be able to withdraw cash from the account as if nothing had happened. However, online customers cannot be apathetic to such incidents in regards to cyberspace. Online security is the most important concern for online customers. Furthermore, in an ordinary e-commerce business to customer model (B2C), a transaction can be terminated after the first visit: a customer does not have to come back to the same online shop again. Conversely, the incessant Internet banking services are offered as long as the customer has a bank account. Thus, strengthening the application of the security system is the key issue for banks to avoid cyber risk. Examining these issues, the financial industry is the most vulnerable industry to cyber risk, thus has interests in cyber risk. Hence,

this thesis focuses on cyber risk within financial institutions[14].

It is critical for financial institutions to have appropriate countermeasures in place in order to face cyber risk. Maintaining a sufficient level of cyber risk management is becoming a nucleus of any business with a presence in cyberspace. Some companies may have already conducted research on cyber risk management. What types of solutions are available for financial institutions in particular? Before examining the details, it is necessary to provide a clear framework for cyber risk. Due to the nature of cyberspace, attitudes towards both the typology and impact of cyber risk vary greatly from individual to individual. Hence, it is crucial to establish the specific standard for financial institutions whilst in reality, there are many risk management methods available. Tightening computer security is considered the most essential concern in avoiding cyber risk; however, technology is perishable. The efficiency of the latest computer technology will surely be obsolete within a few months; therefore, this thesis will not proceed with the subject of efficiency. Nevertheless, computer technology will be examined from different positions as it plays such an important role in cyber risk management and therefore cannot be ignored.

[14] Banks and their Internet banking services are discussed, rather than other financial services. This is because people worldwide regularly use banking services, while the nature of other online financial services tends to be one-time-only transactions, such as purchasing travel insurance. Therefore, all issues and solutions of cyber risk will be examined by analyzing Internet banking services rather than any other online financial service.

Chapter II: An Analysis of Cyber Risk

1. Introduction

Only a few years ago, "cyber risk" was not yet a popular term. The rapid growth of modern technology has educated the world to some degree: to date, the majority of people in financial businesses are able to cite at least one or two examples of cyber risk. "Risk" has been a word which appears frequently in financial businesses especially, although the seeds of cyber risk exist in any industry. So, a wide range of causes are suggested.

The phrase, "computer crime", is used to indicate a certain risk in relation to computers and their equipments. The more automated human life becomes, so the more complicated crime becomes. Computer crime is a typical example of this. Computer crime can be committed: (1) easily, (2) within a short time, (3) by anyone, (4) without the criminal necessarily suffering any pangs of conscience, (5) with only a small possibility of disclosure (and can lead to the acquisition of huge amounts of illegal money or to very great satisfaction (e.g. hacking)). Moreover, even if a computer crime is discovered, (6) the case may be concealed by the company concerned, or (7) the criminal will be penalised, but without a long sentence being imposed. It does not confine the type of offenders to insiders (in other words, employees) of an institution. However, it literally does not include any other type of risk but an offence. Referring to risk which financial institutions are likely to face operationally, computer crime is a mere constituent element. The other elements are, for instance, employees' operational errors or computer system failure — there had not been an appropriate word or phrase to comprise *all* related risk. To date, cyber risk is used as a blanket term encompassing all related matters that potentially expose companies and institutions to damage and losses.

Cyber risk seems to be explained by dividing it into three categories: security risk, a risk in relation to the infringement of intellectual property rights, and errors & omissions[15]. The first and third categories include all three elements (computer crime and computer system failure are categorised in security risk, and employees' operational errors in errors & omissions). The rise of the second category suggests that it is the greatest concern of many companies. In fact, the methods of risk classifications vary. For instance, cyber risk contains legal and reputation risk because they are triggered as a result of cyber risk being identified. However, it is not necessary to categorise cyber risk since it is yet in its infancy. Moreover, this categorization seems to be based on an inconsistent concern. Thus, it is practical to refer to cyber risk as any risk with a cyber element, such as a computer or the Internet.

With the rise of the Internet, the types of cyber risk offences in

[15] See 'Risk Management Discussion Forum', <http://260.teacup.com/ysugimoto/bbs> (print out on file with author).

particular have become more colourful. The risk arises from errors and computer failure incurring huge expenses for financial institutions, as a result of the involvement of computers and the networks. However, their variety cannot be increased only by the aforesaid involvement. This is because they are absolutely not caused on purpose. If any case is caused intentionally, it is defined as an offence. Therefore, the exploration of cyber risk shall start to examine computer crime.

Needless to say, neither computers nor the networks themselves commit an offence on their own initiative. The dilemma occurs when the human mind operating them, is a criminal one. Tiedemann argued that it is impossible to estimate the factual figures of computer crime. He also stated that almost all cases in Germany were disclosed by accident[16]. This aspect will be discussed further. A similar opinion has been widely expressed, that many cases remain undisclosed. For example, Murobushi emphasised that estimating the factual figures of computer crime are even "meaningless" — as he proved through American examples[17]. The American Society for Industrial Security reported that there were 30 electronic security breaches per month in 1995, contrasted with less than one per year three months before 1980[18]. This proved the difficulty of obtaining figures for all types of computer crime. On the other hand, the Federal Uniform Crime Reports makes an interesting estimation that "for every 100,000 citizens in USA in 1993, 306 were crooks working in the fields of fraud, forgery, vandalism, embezzlement and receiving stolen goods." It was expected that 50 million people would use the World Wide Web (hereinafter "WWW") by the end of 1997. Therefore, "it is possible to estimate that 150,000 of them will be crooks[19]." If other types of computer crime are considered, such as hacking, software piracy, and unauthorized access, this figure could be estimated as double, triple or more.

Clearly computer crime is of interest not only to the police, but also to academics and industry. For example, the US Federal Bureau of Investigation (hereinafter "FBI") has formed an International Computer Crime Squad to investigate computer fraud and abuse, including intrusions into public switched networks, privacy violations, computer network intrusions, industrial espionage, pirated software and other computer crimes[20]. Furthermore, the Heads of State of Government of the eight major industrialised democracies and the President of the European Commission agreed on combating high tech crime when they held a summit

---

[16] See K. Tiedemann, '*Doitsu oyobi EC niokeru Keizai-hanzai to keizai-keihou* (Economic crime and economic law in the Federal Republic of Germany and EC countries, the translation of 'Wirtschaftskriminalitat und Wirtschaftsstrafrecht' by H. Nishihara & K. Miyazawa) (1990) Seibundo, Tokyo at 167-169.

[17] See T. Murobushi, '*Konpyûta hanzai sensou* (Computer Crime War)' (1987) Sunmark, Tokyo at 27.

[18] See J. Young, 'Spies like us', in *Forbes*, February 1996: at 70-92.

[19] See J. Gantz, 'A city of felons at T1 speeds', in 31 Computerworld 7 (1997) at 33.

[20] See K.J. Mills, 'FBI forms cyber squad', in 9 International Business 7, (1996) at 6.

in Birmingham (UK) in May 1998[21]. They recognised a dramatic increase in transnational crime — caused by globalisation — and the necessity of international co-operation in combating this transnational crime. Although this initiative was aimed mainly at money laundering rather than computer crime, it was still discussed, with the rapidly implemented ten principles and ten-point action plan on high tech crime, being particularly agreed upon: i.e., through co-operation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic data as evidence, while maintaining appropriate privacy protection. Furthermore, it would appear significant that they mentioned combating abuse of the Internet and other technologies. In their declaration, they mentioned the fear of Internet crime, which might be committed in the near future, and thus pose a threat.

Another point to be addressed was their serious attitude towards the Year 2000 (or Millennium) Bug problem (hereinafter "Y2K")[22]. The Y2K problem was not concerned with crime, however. The problem of computers dealing with this transition would have invariably lead to serious confusion, not only for economies but also other sectors, particularly if this critical technological problem had not been solved before the year 2000. With computers identified as indispensable tools for human life, the heads of States of the countries — aware of the seriousness of transnational crime — held the Ministerial meeting on combating transnational crime in Moscow in 1999.

Currently, there are also many institutes researching computer

---

[21] See 'The Birmingham Summit: Final Communiqué - Sunday 17 May 1998', <http://www.g8.utoronto.ca/summit/1998birmingham/finalcom.htm> (print out on file with author).

[22] The Y2K problem involved cyber risk. It was a serious issue in some countries including Japan. It is said that Japan is one of the high-tech countries in general. But this fact does not always mean that infrastructure is well equipped or well organised. In fact, Japan was evaluated a "not well-prepared country" in addressing the Y2K problem by the US government (adapted from S. Kumon, 'Y2K Trouble' (1999) NTT Publishing, Tokyo.). Furthermore, the Japanese government itself was somewhat reluctant to address this problem until the last minute. In reality, many people had profound doubts about the computer system surrounding their daily lives (adapted from S. Levy, 'The Bug That Didn't Bite: Billions of dollars later, Y2K is on the run. The lessons of a millennial computer scare' in Newsweek, 10 January, 2000) and they went shopping for food, water and fuel and withdrew money from banks just in case something happened. Judging from the fact on the fatal day, 1st January 2000, did all doubt, uneasiness and efforts the world has made for the past several years mean "the waste of time and money"? The answer must be in the negative. According to Levy, the Millennium, were it not fixed, was surely proven to cause trouble in computer systems. It is, of course, not necessary to exaggerate that nothing happened due to sufficient efforts having been made. He also mentioned that company CEO's seemed to love ignoring the Millennium bug (*ibid.*). It can be assumed that they knew the costs of fixing the bug would be huge, apart from the doubt as to what extent they understood the seriousness of the Y2K problem. This, in contrast to the obvious fact that not only government officials but also the general public had actually made many efforts to discover and solve, as far as possible, the Y2K problem. As Levy accurately pointed out, if the government ignored the Y2K problem completely and did not take any positive step against it, this attitude could be "criminally derelict" (*ibid.*).

crime: for example, Parker, the authority in the SRI International in California, USA, and the National Computer Centre in Manchester, UK. It would therefore appear that research interest in combating computer crime has been steadily increasing.

2. The Development of the Notions

2.1 Economic crime and White-collar crime

"[Suffering] the economic consequences of computer crime, society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service coordination and national security. Even a small glitch in the operation of these systems can put human lives in danger... The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security[23]."

A materialistic, civilised environment for human beings has been realised for a few decades in particular. Thus most activities in daily life include an economic element. Crimes are, of course, not exceptions. Akiba made a hypothesis that one may commit a crime if the expected profit (which one might receive as a result of committing the crime) exceeds other elements including the risk taken when committing the crime, or the penalty which might be imposed after the trial should the criminal be found guilty[24]. Of course, some people may commit a crime as a result of strong emotions such as anger or a personal grudge. Even in a case where a crime is committed because of these emotions, it is still possible to say that the emotional factor can outweigh ethical or other considerations for the criminal. But the crucial element that provokes criminal action, regardless of whether profit is the goal, is not the same for everyone. Thus, law and regulation define what types of activities are illegal and punishable, and thus (often) prevent people from committing them. It is possible to say that legal profit is not the same as one's personal economic profit. If a loss is incurred by a certain crime, an offset is needed to cover the resulting damage. To adapt this case to economics theory, a loss can be called a "minus profit". This minus profit must, however, be compensated by something. For example, suppose a criminal (defined as X) commits an illegal activity. A third party (defined as Y) will probably incur a loss as a result of X's activity. In this supposed case, X has to be punished, by a fine or detention, to compensate for Y's losses. The final outcome in legal terms is that punishment is a means of recovering economic loss or damage. In other words, a minus profit (loss or damage as a result of crime) is compensated

---

[23] See 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', <http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html> (print out on file with author).

[24] See M. Kishida, '*Hō to keizai* (Law and Economics)' (1996) Sinseisya, Tokyo at 42-43.

for through punishment (a fine, detention and the like)[25]. It would appear that the law is likely to prove to be a deterrent in relation to these "minus profits" and "plus compensations". It is impossible to think and deal with crimes, particularly "white-collar crime" or "economic crime", without considering this idea, because it is impossible to eradicate their economic elements.

Meier and Short describe "conventional wisdom" as illustrating public indifferent to "white-collar crime" as opposed to other types of crimes[26]. This is supported by Sutherland, who stated that indifferent public reaction reflects that "the public...does not think of the businessman as a criminal; the businessman does not fit the stereotype of 'criminal' "[27]. How then can one define white-collar crime? Duff and Gardiner introduced Edelhertz's idea, which suggests that Sutherland's definition mainly excludes violence and death from the province of white-collar crime[28]. White-collar crime is defined as "crime committed by persons of relatively high social or economic status in connection with their regular occupations[29]". It also states that criminologists restrict the term "illegal actions [relating to white-collar crime], to mean that the perpetrators intend principally to further the aims of their organisations rather than to make money for themselves personally." Thus, there are two categories: illegal actions undertaken by perpetrators to make money for themselves, and those illegal actions undertaken principally to further the aims of a company or other organisation. Examples of the former classification are: embezzlement, misappropriation of funds, securities theft, bribery and kickbacks, insider trading, computer crime, and some types of fraud, while those of the latter one are: restraint of trade (i.e., monopolies), misrepresentation in advertising, unfair labour practices, health or safety violations in the workplace, income-tax law violations, and various financial manipulations.

As Friedrichs suggested, it is obvious that the old-fashioned types of crime, such as corruption and bribery, have existed throughout the history of man[30]. Those crimes could be classified as very old-fashioned. In any civilised society at any time in history, corruption and bribery have been common. This simply means that certain crime, after 2000 years, has come to be recognised as white-collar crime. What, then, made the definition difficult when this crime category already existed? The answer is found in the structure of society. The most common social structure in

---

[25] Kishida, *supra* n.16, 96-97

[26] See R.F. Meier & J.F. Short, Jr., 'The Consequences of White-Collar Crime' in G. Geis, R.F. Meier & L. Salinger (eds) 'White-Collar Crime: Classic and Contemporary Views' (1995) The Free Press, London.

[27] *Ibid.*, at 85.

[28] See L. Duff & S. Gardiner 'Computer Crime in the Global Village: Strategies for Control and Regulation - in Defence of the Hacker', in S. Savage & J. Carrie (eds) 24 International Journal of the Sociology of Law (1996) at 211-218.

[29] CD-ROM of 1997 Encyclopaedia Britannica.

[30] See D. Friedrichs, '*Howaito karā hanzai no houritsugaku* (Trusted Criminals)' (1999) Springer-Verlag, Tokyo at 2.

history was feudalism. In this hierarchical society, it was conceptually taboo to accuse someone in the privileged classes, such as aristocrats. This explains the phrase "robber barons" used by Sutherland. This is explained by the phrase "robber barons" that Sutherland's used in his work[31]. The "robber barons" signifies the privileged class in the latter half of the nineteenth century as the exploiting class. Judging from the above, is social status the most important element in defining white-collar crime? Sutherland defined it as: "Approximately... a crime committed by a person of respectability and high social status in the course of his occupation[32]'.

His interest in white-collar crime was based on the anger at corporate criminality. Furthermore, this can be supported by Ross who had an impact on Sutherland[33]. Ross introduced the notion[34] that an entrepreneur engages in illegitimate or illegal activity because of his eagerness to increase profits, thus exploiting his social privileges. He also insisted that such unethical activities are a great menace to capitalist economies. Therefore, it seems reasonable to identify "a person of respectability and high social status" in Sutherland's definition as a person who occupies a critical position. However, this is a complex and problematic issue. Shapiro, who is the representative opponent of Sutherland, objected to this point that the key factor of white-collar crime is infringement on trust[35]. In regard to her theory, social status is only the consequence of white-collar crime and not its entirety. Croall obviously adopted her theory [36]. In reality, Sutherland himself stated that "white-collar criminality is found in every occupation[37]." This statement seems contradictory compared to his early definition. From a practical point of view, Shapiro's theory is wider than Sutherland's. Broadly speaking, high social status could be included in trustworthiness. In other words, people who are in a high class (i.e. aristocrats) or in a high position (i.e. company management) are generally trusted to a greater or lesser degree. However, the converse does not hold true: all trusted people in a society do not always have a high status.

An alternate view is Clinard and Quinney who categorised white-collar crime into two types: "occupational crime", which explains crimes committed against businesses, and "corporate crime", which explains crimes committed by business[38]. Since Sutherland's work in the

---

[31] Friedrichs, *supra* n.22, at 3 and *infra* nn. 24 and 25 and H. Sutherland, edited by K. Schuessler, 'On Analyzing Crime' (1973) The University of Chicago Press, Chicago, at 47.

[32] See H. Croall, 'White collar crime: criminal justice and criminology' (1992) Open University Press, Buckingham at 8 and Friedrichs, *supra* nn.22 at 5 and 23 and *infra* n. 25.

[33] See Friedrichs, *supra* nn.22 to 24.

[34] The notion which Ross developed was called a 'criminaloid'. Sutherland, *supra* n. 23 and *infra* n.29.

[35] Croall, *supra* n.24 at 16 and *infra* n.28 and Friedrichs, *supra* nn. 23-25, at 16.

[36] Croall, *supra* nn.24 and 28, at 10.

[37] Sutherland, *supra* nn.23 and 26, at 48.

[38] M. Wasik, 'Crime and the Computer' (1991) Clarendon, Oxford at 24-25.

1940's, many criminologists have focussed on the backgrounds of criminals as a means of defining white-collar crime[39].

On the contrary, a definition of economic crime hardly exists. Tiedemann explained how German scholars had difficulties finding a definition for economic crime. In the past, especially after World War II, German scholars accepted a broad rather than an exact definition of economic crime. Economic crime was seen to be an offence against German national economic projects. Currently (both in Germany and in other countries) it includes many types of laws concerned with business[40]. Many of them (such as laws for the banking system, credit, or securities) mainly target the executives of the companies since, because of their high positions, they can commit a crime more easily than their employees. Therefore, the German system suggests that any crime is likely to be defined as economic crime if its criminal has a certain status. Any law is also likely to be defined as or be relevant to economic law, if a law particularly has an economic element. However, this interpretation is too broad, and furthermore, it has a fatal defect: it is impossible to judge a criminal who does not have a particular permanent status or position as an economic criminal. On the other hand, Tiedemann also put forward an alternative view, stating that a crime whose purpose is to damage the economy itself, can also be defined as economic crime[41]. However, this is not a practical idea, because one has to know and decide exactly to what extent the economy is going to be harmed when the one commits a crime. If the losses involved in the crime are small — such as those arising from an individual dispute for example — it is impossible to include such a case in economic crime, even though it has economic elements. It is also not practical to place importance on the tools used to commit crime to define it. This is because it would be impossible to deal with a crime which is committed using a new unknown technique and/or tool — this includes technology.

Therefore, it is legally impractical, in future, to place restrictions on the type of tools that may be used in economic crime because it is widely believed that technology will continually evolve. It is also not practical to place importance on the status of a criminal, a target, or a tool. Bearing the aforementioned ideas in mind, what then is the best way to consider an economic crime? It is important to think about whose profit is vulnerable in cases of economic crime. Nevertheless, any type of economic crime may harm not only individual profit but also social profit, especially in cases where the loss is very large. It may also cause economic confusion in a community. In other words, as Tiedemann stated, a state economy consists of an individual gross, therefore it is possible to define economic crime (whether it confuses a state economy intentionally or unintentionally)

---

[39] This point will be elaborated on later in depth.
[40] Tiedemann, *supra* n.9, at 12-13.
[41] *Ibid.*

as a serious crime against a state itself[42]. The other way to define economic crime is to list all types of offences. The Council of Europe published a list of economic offences in 1981, because it recognised the difficulty of giving one exact definition[43]. 16 types of offences were shown, including cartel offences, customs offences, and computer crime. Two terms have already been highlighted: white-collar crime and economic crime. The latter is a much broader interpretation than the former, because the former is included in the latter from the viewpoint of recognising a criminal's status. However, these types of crime must be treated cautiously for some of the reasons which have been mentioned above. Therefore, whereas white-collar crime is not an efficient term, economic crime is more appropriate.

2.2 Computer crime and Cybercrime

Deterrence is unlikely to work efficiently in economic crime. There are some possible reasons: Firstly, someone who has a high status and thus, earns a lot of money, has access to the best lawyers. Secondly, there may be no strict punishment for economic crime to create the necessary deterrence. Thirdly, the possibility of insurance means companies and victims are less likely to view economic crime as a "serious" or dangerous crime. These three reasons can be termed "moral hazard"[44]. Moral hazard is likely to occur when any type of individual profit violates that specific individual's morals values. For instance, one may not feel guilty violating traffic regulations by not stopping at a red light if neither a car nor a pedestrian is present. There are many such petty violations and it is easy to imagine that these are likely to happen without any moral issues arising. Economic crime can be committed in the same thoughtless way. Since a huge amount of illegal profit can be expected from economic crime, it is very easy for a criminal to know which is the more valuable: illegal profit or violated morals. In a sense, economic crime is sometimes the most understandable crime, not only for motivation (=money), but also for how a criminal measures how minus/illegal profit (=money) is more valuable than either moral or plus compensation (= a risk of arrest and penalty).

Before defining computer crime itself, the first question to be discussed is what exactly is considered vulnerable to computer crime. It is possible to divide this answer roughly into two categories: tangible or intangible property. It is fairly easy to understand what tangible property includes (e.g. houses, land, money and the like), and this is also true of intangible property of which a typical example is "intellectual property" (e.g. copyright). Intellectual property as a recognised example of intangible property has already been thoroughly debated by academic scholars. On

---

[42] *Ibid.*
[43] Council of Europe, European Committee on Crime Problems, 'Economic crime' (1981) Strasbourg at 11-12.
[44] M. Kishida, *supra* n.16, at 103-104.

the contrary, it still proves difficult to recognise computer programmes and data as intangible property. For these to be recognised globally will, in all probability, take a long time. This is because computers include not only tangible matters such as the computers themselves, but also intangible matters like data and programmes. Since computer programmes and data are the major target of computer crime, it is essential that academic authorities recognise them as intellectual property. According to the Scottish Law Commission, property is defined as follows (and this would appear to be the majority view in academic circles at present):

> "'Property' means anything of value... but is not limited to, financial instruments, information, including, electronically produced data and computer software and programmes in either machine-readable or human-readable form, and any other tangible or intangible item of value[45]."

It is said that a specific category of computer crime in criminology was set up between the 1970's and 1980's[46]. Computer crime is defined as "any crime that is committed by means of the special knowledge or expert use of computer technology[47]." In fact, as is mentioned, computers have evolved to become a tool, not only for criminals, but also for ordinary business people, and they have been involved in crimes, such as embezzlement and larceny. The problem in recent years is that "computer crime became a serious problem with the proliferation of such technology in the late 20th century." Carroll has even suggested that almost all crime against property could be perpetrated with a computer system[48]. It was observed earlier that the Council of Europe has recognised computer crime as an economic offence. However, there are various terms applied to "a crime committed with a computer": computer abuse, computer crime, computer misuse, and computer-related crime. Parker defined three of these as follows:

Computer crime	: illegal computer abuse implying the direct involvement of computers in a crime;
Computer-related crime	: a broader term covering any illegal act for which knowledge of computer technology is essential for successful perpetration;
Computer abuse	: any intentional act involving a computer and one or more perpetrators which made, or could have made gain, and one or more victims

[45] Scottish Law Commission, 'Computer Crime: Consultative Memorandum No.68' (1996) at 12.
[46] ILC - Internet Lawyers Committee, 'Internet and the Law' (1998) Nihon Hyouron, Tokyo at 56-57.
[47] Encyclopaedia Britannica, *supra* n.21.
[48] J.M. Carroll, 'Portrait of the Computer Criminal', in J.H.P. Eloff & S.H. Solms, 'Information Security - the next decade' (1995) Chapman & Hall, London at 577.

suffered, or could have suffered, loss[49].

Parker adopted the term '"computer abuse" in his work. As he mentioned, it is impossible to define '"computer abuse." If an illegal act does not involve a computer as a tool — if, for example a typewriter is used in lieu of a computer (even though a criminal stills needs the same knowledge and situation as he would for a computer crime) — it would not be included in Parker's definition. However, as these three definitions are very broad, any type of crime can be included. On the other hand, as Parker argued, the mass media can sometimes incite the general public, simply for entertainment, by using the phrase "computer crime". Therefore, there are occasional cases which are difficult to define exactly as computer crime[50]. Wasik, in contrast, divided computer misuse into three levels[51]. Firstly, it was the level of corporate crime where the misuse was central to company policy and carried out by those who held a structural position. Secondly, it was the level of occupational crime wherein individuals committed offences against their employers in the course of their employment. Thirdly, it was the level of misuse by outsiders without authorised access. It would seem that this last level does not deviate from the definition of computer misuse itself. In short, it would appear that these three connect as follows:

Computer-Related Crime > Computer Crime > Computer Abuse

The direction of the mark (>) shows which term provides the broader definition. In short, computer-related crime (which includes many offences involving computers) has the broadest definition, with computer abuse on the opposite pole. Thus, it would seem that computer crime is a more general term compared with computer abuse only. Withal, there is no doubt that any of the above three terms can be included in economic crime. Another definition is that of the US Department of Justice as:

Computer crime: any crime where the perpetrator has to have a technical knowledge of computers to engage in crime[52].

The US Department of Justice definition seems to be similar to Parker's computer-related crime. In fact, it would appear that there is no significant difference among the three terms: computer crime, computer-related crime, and computer abuse. The National Police Agency in Japan has used a similar idea: it recognised computer crime as "a crime against a computer or any illegal act involving a computer[53]." Furthermore, Murobushi suggested changing this definition to "a crime against a

[49] See D. Longley, 'Security and the Law', in W. Caelli, D. Longley, M. Shain, 'Information Security for Managers' (1989) Macmillan, Basingstoke at 320.
[50] See D.B. Parker, 'Fighting computer crime', translated into Japanese by M. Uzawa, (1984) Syujunsya, Tokyo at 12.
[51] Duff and Gardiner, *supra* n.21 and *infra* n.44, at 213-214.
[52] Duff and Gardiner, *supra* nn. 21 and 43, at 29.
[53] A. Kanno, 'Tricks of Computer Crime' (1990) Corona, Tokyo at 29.

computer and/or communication or any illegal act involving a computer and/or communication[54].' However, as this is almost the same as Parker's idea and that of the US Department of Justice, thus it is possible to include his definition in theirs.

The Organisation for Economic Cooperation and Development (hereinafter "OECD") also chose the term "computer-related crime" throughout its work. It stated that the term was acceptable for member countries, and furthermore, a more comprehensive definition would not prove practical for all the different national legal systems[55]. Sieber, who contributed to the OECD's work, insisted on two main vulnerable areas in his work: computer-related economic crime and computer-related infringements of privacy[56]. He explained the reason for this classification as being that other computer-related crimes (such as homicide committed by computer manipulation) have not caused major legal problems. In contrast, the Audit Commission in the UK used the term "computer fraud and abuse" instead of Parker's three terms. However, it also used a more comprehensive definition, defining "computer fraud and abuse" as "any fraudulent behaviour connected with computerisation by which someone intends to gain dishonest advantage[57]." The intention of the Audit Commission is the same as the previously cited authorities and organisations, i.e., that the most important viewpoint is neither deciding on the most suitable term, nor making an exact definition, when considering the seriousness of computer crime and dealing with it properly. As the Council of Europe stated, any exact definition may have certain disadvantages[58]. Therefore, the best solution is found in a definition sufficiently understandable and unambiguous, while still remaining broad rather than precise. Thereby, any computer crime can fit within this definition, even future crimes.

There are many types of offences in computer crime, and these offences will be mentioned, to a greater or lesser extent, in later sections. For example, while hacking is one of the most notorious computer crimes at present, it may prove problematic in relation to the definition of economic crime. Although, as it meets certain necessary and sufficient conditions which define it as computer crime, it is impossible to exclude hacking from that category. However, if economic crime includes only certain crimes with either a motive to obtain money or cause economic damage, hacking does not meet this condition, and computer crime may therefore be excluded from economic crime as a consequence of hacking not being recognised as computer crime. Why? Because hacking is not

---

[54] Murobushi, *supra* n.10, at 246-247

[55] OECD 'Computer-related crime: analysis of legal policy: Being: Information, computer, communications policy: V.10' (1986) OECD, Paris at 7-8.

[56] Sieber, 'International Handbook on Computer Crime: computer related economic crime and the infringements of privacy' (1986) John Wiley & Sons, New York at 37.

[57] Audit Commission for Local Authorities in England and Wales, 'Survey of Computer Fraud and Abuse' (1987) H.M.S.O., London at 7.

[58] Council of Europe, *supra* n.35, at 13.

always harmful; it is sometimes carried out merely for fun[59]. On the other hand, the viewpoint of the Criminal Justice section of the American Bar Association recognises computer crime as an isolated phenomenon rather than a specific action[60]. In fact, a major quandary is making a precise definition based on the proliferation of computer crime due to rapid changes in computing technology. But the proliferation of both computer crime and of computing technology is too rapid and problematic to ignore. However, it is unnecessary to create a specific term for "computer crime." To recognise computer crime as a phenomenon seems to be the best way to incorporate it within economic crime, without having to consider a separate definition.

The massive influence of the Internet over the past five years has created an unexpected situation, with the potential danger of crime through the Internet and the network being inevitable. There are other terms suggesting similar offences: cybercrime, electronic crime, high-tech crime and Internet crime. All of them are comparatively new alongside any of the aforementioned terms. They mostly resemble each other, particularly by one factor: the involvement of computer networks connected by the Intranet internally and by the Internet externally. Technically speaking, there is no big difference amongst them. On the other hand, there is a theory that their scopes are respectively restricted based on the historical process of their development[61]. The minor differences are literally suggested: electronic crime indicates crime being committed electronically. High-tech crime is similar to this: the abuse of high technology is by its nature criminal. High-tech crime is a favoured term since the 1997 Denver summit. Internet crime and cybercrime seem to be almost equivalent terms. However, the most serious types of crime are very likely to fall in cybercrime, such as cyber terrorism. Cybercrime is conceptually defined by the European Commission Joint Research Centre as "the criminal use of any computer network or system on the Internet. Attacks against the systems and networks for criminal purpose. Crimes and abuse from either existing criminals using new technologies, or new crimes that have developed with the growth of Internet technology[62]." It is possible to say that this definition is fluid rather than static. Due to the similarity of the said terms, the choice of a term varies depending on the authorities or research. There is a view that cybercrime is one of the types of high-tech crime[63]. The problem with a strict definition is the

---

[59] Duff and Gardiner, *supra* nn.43 and 44, at 213-214.

[60] The task force of the Criminal Justice section of the American Bar Association did not define computer crime exactly, and viewed it as a phenomenon. A similar view was also showed by Tiedemann. See M.D. Rostoker and R.H. Rines, 'Computer Jurisprudence: Legal Reponses to the Information Revolution' (1986) Oceana, New York at 334.

[61] See '*9. Owarini* (9. The conclusion)', <http://www.law.co.jp/okamura/jyouhou/cybercrime/crime.htm> (print out on file with author).

[62] See European Commission Joint Research Centre, 'Cyber Crime in E-Business Processes: Report of an exploratory study' (2001) European Commission, at 60.

[63] See '*7. Saibâ hanzai* (7. Cybercrime)',

consequent difficulty in applying it to the reality — the *modi operandi* of crimes within any of the said terms are unlikely to be invariable. That is to say that *modi operandi* can change depending on the innovation of technologies or an individual's computer skills. The Joint Research Centre of the European Commission commented that cybercrime is a vague term covering a wide range of issues[64]. In this context, it is appropriate to choose cybercrime out of a possible four terms for two reasons: firstly, cybercrime is more likely to have a broad enough definition to cover the specific risks which financial institutions are likely to face. Secondly, it is necessary to attempt unification within the term "cyber risk".

Wall described cybercrime as the term largely invented by the media[65]. It is extremely likely due to the impact of the term. In 2001, Convention on Cybercrime, prepared by the Council of Europe, was ratified by its member countries and some other countries as well. Within its context, there is no definition of cybercrime provided whereas other terms, such as "computer system" or "computer data", are defined in its Article 1[66]. On the other hand, Clifford suggested describing cybercrime as:

> "When they do so, particularly if the crime could only occur because of how cyberspace operates, the term 'cybercrime' has been used to describe this behaviour[67]."

Project Trawler, the National Criminal Intelligence Service (NCIS), UK, launched in 1996, declared in its report that the terms "computer crime", "information technology (IT) crime" and "cybercrime" are interchangeable[68]. As is seen, they are all necessary for any crime connected with cyberspace. Considering this, it is rather appropriate to say, in this context, that cybercrime is only one portion of computer crime. Introducing computer networks broadens cyber risk significantly. It is true that such brand-new types of offences, which are categorised as cybercrime, are quite likely to incur serious damages and losses for financial institutions. However, there are also traditional types of offences in conducting financial services, which are categorised as computer crime but not cybercrime. From this viewpoint, cybercrime is an appropriate term in a narrow sense only if it is, of necessity, emphasising the impact of brand-new types of offences. In a broad sense, computer crime is the most appropriate term to include all risks that financial institutions are likely to face in the course of their business. Therefore,

---

<http://www.law.co.jp/okamura/jyouhou/cybercrime/crim7.htm> (print out on file with author).

[64] European Commission Joint Research Centre, *supra* n.54, at 1.

[65] See D.S. Wall, 'Cybercrimes and the Internet' in D.S. Wall (ed) 'Crime and the Internet' (2001) Routledge, London, at 2.

[66] Convention on Cybercrime is to be examined in depth in Chapter II.

[67] See R.D. Clifford (ed), 'Cybercrime: the Investigation, Prosecurtion and Defense of a Computer-Related Crime', Carolina Academic Press, Durham at 6.

[68] See NCIS, 'Project Trawler: crime on the information highways' (1999) London.

both computer crime and cyber crime are to be used in this context[69].

2.3 What is Computer Crime?

2.3.1 Classification of Computer Crime and its *modi operandi*

It is clear that one of the difficulties of understanding computer crime is that many different definitions exist. In a narrow sense, there is no global definition of cybercrime. This is also strongly reflected when categorising types of computer crime, because each classification is based on a specific definition. When focussing on the type of perpetrators involved, all cases can be categorised into two types without exception: an "inside job" or an "outside job". For instance, in Japan, all cases used to be simply divided into two types: crime using a cash dispenser (hereinafter a "CD crime") or others until the rise of the Internet. Of course, "the others" should be categorised into subordinate classifications. This section will therefore begin by considering some general theories to classify computer crime.

Parker, the pioneer of computer crime research, developed the idea of six elements of abusive actions against information, which were derived from more than 3,500 computer abuse cases since 1958: availability, utility, integrity, authenticity, confidentiality and possession. Although half of a century has passed since then, this theory still works efficiently. He also demonstrated how those six elements are violated: availability and utility are vulnerable to destruction, damage, or contamination. Integrity and authenticity are vulnerable to:

(1) Entry, use or production of false data;
(2) Modification, replacement, or reordering programme/data;
(3) Misrepresentation;
(4) Repudiation (rejecting as untrue);
(5) Misuse or failure to use as required[70].'

Confidentiality and possession are threatened by access, disclosure, observation or monitoring, copying or stealing. Needless to say, his idea is built on the recognition of information as an asset or property, utilised in business activities to make a profit. It would appear that it is no exaggeration to suggest that this is a fundamental classification, because it generally includes all elements of criminality.

The other approach for categorising computer crime is to focus on the stages at which it occurs. There are usually three stages: input,

[69] Unless it is necessary to emphasize the involvement of cybercrime, computer crime is to be used as a blanket term including cybercrime in this context.
[70] D.B. Parker, 'A new framework for information security to avoid information anarchy', in Eloff, J.H.P. & von Solms, S.H. Information Security-the next decade, (1995) Chapman & Hall, London, at 157-158.

throughput and output. According to Slapa, to enter false or misleading information in a computer system is called "input fraud". It can be divided into two categories:

(1) Positive falsification - actual insertion of additional data
(2) Negative falsification - where data is suppressed prior to processing[71].

"Throughput" is defined as a fraud which occurs during the running programme. Therefore, this requires more technical knowledge (in order to manipulate) than either input or output. Output is simply related to computer products, which can be suppressed, stolen, altered or falsified.

An alternate theory is provided by the OECD who organised an ad hoc working group on computer-related economic crime in 1983, publishing a final report in 1986[72]. This addressed the obvious necessity for identifying the international character of computer crime. The intention of the OECD was: (1) to facilitate information exchange between the OECD-member countries on the subject of computer crime, (2) to observe developments and trends in countermeasures against computer crime in different countries, and (3) to provide common legal policies. To quote the OECD, "international co-operation is necessary not only in order to profit from others' experience but also to avoid unequal conditions of competition and the creation of 'computer crime havens'". It suggested five types of abusive conduct, recommended by the OECD for criminalisation by the enactment of criminal law provisions in each of the member countries:

(1) The input, alteration, erasure and/or suppression of computer data and/or computer programme made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;
(2) The input, alteration, erasure and/or suppression of computer data and/or computer programme made wilfully with the intent to commit a forgery;
(3) The input, alteration, erasure and/or suppression of computer data and/or computer programme, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or telecommunication system;
(4) The infringement of the exclusive right of the owner of a protected computer programme with the intent to exploit commercially the programme and put it on the market;
(5) The access to or interception of a computer and/or telecommunication system made knowingly without the authorisation of the person

[71] See 'Computer Fraud: Slapa Assignment 3', <http://www.scitsc.wlv.ac.uk/ cm5067/slapa/fraud.html> (print out on file with author).
[72] See H.W.K. Kaspersen, 'Standards for Computer Crime Legislation: A Comparative Analysis', in Vandenberghe, G.P.V.(eds) Advanced Topics of Law and Information Technology, (1989) Kluwer Law and Taxation, Boston, at 45.

responsible for the system, either
(i) by infringement of security measures, or
(ii) for dishonest or harmful intentions[73].

The OECD stated that the reason why the above list was solely limited to basic methods (whereas there are more diverse types of abusive conduct) was because it was not easy to formulate them as independent categories; furthermore, they may already be covered by more generally formulated definitions in the criminal code or special laws.

On the other hand, the Audit Commission in the UK provided ten types of incidents in three main classifications as follows:

(1) Fraud
  (i) Unauthorized alteration of input;
  (ii) alteration of computerised data;
  (iii) alteration/misuse of programme;
  (iv) destruction/suppression/misappropriation of output.
(2) Theft
  (i) of data;
  (ii) of software;
  (iii) of computer facilities;
  (iv) Unauthorized private work.
(3) Hacking
  (i) unauthorized access to data and computer facilities;
  (ii) sabotage of facilities[74].' (The Audit Commission. 1985)

This classification, based on the 1984 survey and published in 1987, appears to imply a similar meaning as the OECDs. However, the Audit Commission produced a slightly different and out of date one in 1985. The 1985 classification was based on an older survey, and the Audit Commission adequately developed these old survey results in the 1984 survey. Hacking was, especially, a brand-new category. According to the Audit Commission, hacking means "deliberately gaining unauthorized access to a computer system usually through the use of telecommunication facilities[75]". The appearance of a new category showed the rapid increase of technological progress and that a mere three-year period is sufficient to produce significant changes in ideas and means. The Audit Commission provided an almost identical classification as the OECD, but with minor differences. It added two more classifications:

(4) Virus — distributing a programme with the intention of corrupting a

[73] OECD (1986), *supra* n.47, at 64-65.
[74] See Audit Commission for Local Authorities in England and Wales, 'Computer Fraud Survey' (1985) H.M.S.O., London.
[75] See Audit Commission for Local Authorities and the National Health Service in England and Wales, 'Opportunity makes a thief: an analysis of computer abuse' (1994) H.M.S.O., London, at 8.

computer process;
(5) Invasion of privacy — unauthorized disclosure of data and breaches of data protection legislation[76].

The Audit Commission defined "sabotage" as "interfering with the computer process by causing deliberate damage to the processing cycle or to equipment". Further, the Audit Commission stated that, while it never purported those definitions were valid in the UK, they were still very likely to cause a serious risk to organisations[77].

Attempts will now be made to extend the observation into the realm of academia. Some recent academic typologies are, therefore, to be explained. Firstly, Longley categorised some computer frauds and computer crimes into five types in order to explain the subject to managers:

(1) Fraud or embezzlement in which the computer system is a component of the transaction but in which there is no interference with, or misuse of, the computer's normal operation by legitimate users;
(2) Fraud or embezzlement which takes advantage of some aspect of the normal computer operation;
(3) Fraud or embezzlement in which the computer system is deliberately misused;
(4) Theft of hardware, software, or data;
(5) Ransom of computer system facilities or data[78].

According to Solomon, embezzlement itself means that all schemes include: "(1) overlapping accounts, (2) check kiting or floating, (3) payroll fraud, (4) ghost vendors, and (5) falsified expense accounts[79]." Therefore, Longley's concepts seem to be aimed at the development of more practical methods for managing companies. However, Sieber, a German legal academic, categorised computer crime in a different way entirely:

(1) Fraud by computer manipulation;
(2) Computer espionage, software piracy, and high-technology theft;
(3) Computer sabotage;
(4) Theft of services;
(5) Unauthorized access to data processing systems;
(6) Computer-related tax fraud[80].

The second category represents a new concept. In addition, the second and the sixth categories are primarily concerned with governmental

---

[76] *Ibid.*, at 8.
[77] *Ibid.*
[78] See Longley, *supra* n.41, at 324-325.
[79] See M. Solomon, 'The CU crime that hurts most', in 63 Credit Union Magazine 2, 1997.
[80] Sieber, *supra* n.48, at 37.

rather than business activities. However, they can still be defined as economic crime (even if they are only recognised as a crime against a government), on the basis that such information is a quantifiable national asset. This classification is very similar to that offered by Tiedemann[81]. He introduced the German classification based on Sieber's with two exceptions: Tiedemann included (6) in (1), and changed the explanation of (4), whereas Sieber simply categorised "theft of services", which Tiedemann explained as "theft of time". This term is likely to limit the ambit of theft activity more than Sieber's term, thus creating a substantial gap. It means that "theft of time" is less harmful, because it has the same meaning as the Audit Commission's seventh classification. In other words, Tiedemann's term does not adequately demonstrate that harmless action is a risk serious enough to result in an accusation. Another academic, Cornwall, explained his classification by using the non-technical terms, "data fraud", "data spying", and "data theft". This is a simplification of Sieber's theories which is easier for the general public to comprehend[82]. Wasik mentioned three categories based on the ideas of Sieber; unauthorized access and unauthorized use, fraud and information theft, and associated offences[83].

Tapper introduced a classification of offences in his research. According to him, some of them can be defined into three parts:

The original Florida legislation:
(1) Offences against intellectual property;
(2) Offences against computer equipment or supplies;
(3) Offences against computer users.

On the other hand, the Federal Counterfeit Access Device and Computer Fraud and Abuse Act 1984 defined:

(1) unauthorized computer access;
(2) obtaining private financial information;
(3) abusing federal government computers.

Tapper also introduced both the Scottish and English Law Commissions's classifications, although these are almost identical to the OECD's and/or the Audit Commission's versions[84]. The interesting point is that two sets of classifications, introduced by Tapper, are completely different from any of the other classifications above. Practical legislation is more likely to be widely defined than previous theories. In reality, to establish a broad definition was the only way to prove criminality in the early period of computer crime's advent so that the actual crime could be judged as routine fraud, larceny, and the like.

---

[81] Tiedemann, *supra* n.9, at 169-175.
[82] Wasik, *supra* n.30, at 41.
[83] *Ibid.*
[84] See C. Tapper, 'Computer Law' (1989) Bath Press, Harlow.

Another way to categorise computer crime is by *modi operandi*. It is said that it can be possible to identify several "standard *modi operandi*"; notwithstanding that technology advances rapidly. Kanno has noted that many cases were committed with some mixture of "standard *modi operandi*". The items listed below are standard *modi operandi*:

(1) Trojan horse;
(2) Trap door;
(3) Piggy bag;
(4) Masquerading;
(5) Wiretapping;
(6) Salami;
(7) Logic bombs;
(8) Garbage collection;
(9) Forgery;
(10) Guessing, or password breaking;
(11) Simulation[85].

Although Kanno categorised *modi operandi* into eleven types as above, Parker has offered a somewhat different classification. This is divided into six offence groups with 13 items as follows:

(1) Physical and logical destruction;
(2) Piggie bag and disguising;
(3) Forgery;
(4) Superzapping and wiretapping;
(5) Trap door, Trojan horse and salami;
(6) Attacking operating system, logic bombs and simulation[86].

Referring to two of the destruction methods, Parker also mentioned that both *modi operandi* include crimes committed by the criminal him/herself or a third party who is involved with him/her. As Parker has accurately pointed out, there are only five basic results of offences caused by technical misuse: alteration, destruction, disclosure, unauthorized access and suppression.

The final classification is based upon specific areas. There are seven types of specific issues concerned with computer crime (particularly in the commercial area) which are as follows: copyrights, trademarks, patents, trade secrets, assignments and licensing, unfair competition, and defamation[87]. The last term, defamation, remains undefined both in economic (in theory) and commercial (in practical) sectors. But this sometimes causes serious damage against company business so it could, on balance, be included. Of course there are many other issues which are not able to be included within these seven. Such issues include fraud, intrusion into a structure, forgery, interference with Statutes and the like. All the other issues — for example, the issue of infringement of privacy, murder by misleading a computer, pornography and the like — will not be

[85] Kanno, *supra* n.45, at 41-45.
[86] Parker (1984), *supra* n.42, at 49-136.
[87] See R.A. Kurz, 'Internet and the law' (1996) Government Institutes, Rockville.

mentioned at all, because they do not fit the purpose of this thesis.

Cybercrime falls within any of the aforementioned classifications. There are, however, other types of cybercrime which elude those classifications to a greater or lesser extent. It is worthwhile examining taxonomy of cybercrime closely, including those which come from the classifications.

The European Commission published the report on cybercrime in relation to online business. Although the report did not establish the definition of cybercrime, it expressed that it had carried out the research "whether the computer systems is the target of the activity...or merely the means by which the activity is carried out[88]." As this clearly suggests, cybercrime is divided into these two categories. Computer crime also falls under this theory, thus far. The said report gave examples for each category: viruses, Trojan horses, denial of service, and theft of services for the first category, and spoofing[89], fraud, and forgery for the second category.

In the report, the taxonomy is introduced, which was compiled from the extensive literature of the G8, the Council of Europe, the US Department of Justice and the like. It provides 18 types of cybercrime as follows;

1. Hacking — using individual skills to attack systems;
2. Cracking — using programmes and tools to attack sites;
3. Site spoofing — false sites for frauds and theft of consumer details;
4. Software piracy — illegal use of software or services;
5. Copyright theft — related to piracy and content theft;
6. Content / service theft — the stealing of material which has a financial value;
7. Online theft — credit card numbers and details;
8. Online fraud — the use of false details or credit card to obtain [goods] and services;
9. Identity theft — using another account or computer to carry out an illegal activity;
10. Child abuse and pornography — the generation, sale and distribution;
11. Travellers — child molesters who trawl for young victims on chat lines;
12. Viruses — creating and the dissemination of such;
13. Denial of services — the use of multiple computers to attack a system's inputs;
14. Cyber terrorism — no real indicators of this yet;

---

[88] European Commission Joint Research Centre, *supra* n.54 and *infra* n.81, at 2.
[89] It is defined as "creating illegitimate websites that cop the legitimate trading site published by an established company to illegally obtain credit card numbers and details." European Commission Joint Research Centre, *supra* nn.54 and 80, at 61.

15. Cyber activist — attacking company / country critical infrastructure;
16. Cyber stalking — using the Internet to intimidate, cause fear and alarm;
17. Cyber harassment — using the internet for racial, sexual or other forms of abuse, and;
18. Cyber blackmail — using online records; personal, medical or product to blackmail[90].

The NCIS report added online gambling on the top of the list above[91]. There exist some other types of cybercrime outside of the aforementioned list. The typical examples are "cybersquatting", "industrial espionage" and "social engineering". Cybersquatting has been an issue in relation to domain name. The U.S. federal law (a.k.a. Anti-Cybersquatting Consumer Protection Act) defines it thus: "cybersquatting is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else[92]". This could be similar to fraud or demanding a ransom demand[93]. The biggest concern of all cybercrime is likely to be industrial espionage. It includes not only eavesdropping on digital communications but also stealing confidential information by hacking. It may be unnecessary to actually steal digitally, just peeping at information will suffice. Considering this purpose of the crime, industrial espionage consists of one to three different offences case by case: eavesdropping, hacking and online theft.

In terms of committing a social engineering offence, it is not always necessary to have superior computer skills or knowledge. The offence called social engineering is explained as "hacker-speak for tricking a person into revealing their password[94]." Amongst all the factors and elements of computer security chain, a human being is said to be the weakest link[95]. If a hacker calls the security department of company X to be a new employee who has forgotten or lost his login name and the password, the staff is very likely to give this hacker a temporary login name and password. Even if the staff makes an inquiry to the human resources department, finds out within ten minutes that it is a hacker and then takes action to stop him stealing data from X's computer network, it may give the hacker enough time to obtain data or information[96]. Even a simple email

---

[90] European Commission Joint Research Centre, *supra* nn.54, 80 and 81, at 19.
[91] NCIS, *supra* n.60.
[92] See 'cybersquatting', <http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci213900,00.html> (print out on file with author).
[93] Regarding cybersquattering, it will be explained at length later in Chapter III.
[94] See 'Social Engineering', <http://www.seas.rochester.edu:8080/CNG/docs/Security/node9.html> (print out on file with author).
[95] See 'Social Engineering by Daintry Duffy', <http://www.darwinmag.com/read/120100/defenses_sidebar1.html> (print out on file with author).
[96] See 'Social Engineering', <http://www.atmarkit.co.jp/aig/02security/socialengineering.html> (print out on file with author).

will do: a malicious offender emails anonymously at random, suggesting the removal of a certain file from a computer, which is actually necessary to start up the computer. If the recipient then removes the necessary file from the computer, the computer will not be able to start up again[97]. Social engineering consists of two different offences; a fraud (the stage of playing a trick to get a login name and/or a password) and the following offence (theft, destruction and the like). Thus, social engineering itself may not be suitable to be classified as either cybercrime or computer crime.

2.3.2 Characteristics of Computer Crime

Many people in the world have used computers to some degree. At the very least, it is impossible to know how many people have used a keyboard. Nowadays, computers are the basic tools in society. Is it difficult to use such a basic tool to commit a crime? Of course it is not. If someone has a keyboard with a computer, one can commit a computer crime easily. This assumption can be translated into reality. Imagine a bank clerk. One does not need any special computer skill or knowledge. If one enters some extra information in one's routine, one can commit a fraud within a very short space of time[98]. This is also a very simple and easy action. Other categories of computer crime are not as elementary to commit. The other side of this problem might be "ethics". In fact, it is not difficult to imagine that people might feel concerned about committing a computer crime if a fraud can be committed within a few minutes. As previously mentioned, it is not easy to evaluate morals or ethics in law. These might be better left to company regulations or self-governance.

It has repeatedly been asserted that white-collar crime usually has no victims. Whatever the moral dimension imposing legal responsibility, it must be made clear what the role of criminal law is. If the law does not impose morality, if it does not define which areas should trigger penalties. In actuality, it is impossible to judge such activities and behaviours[99]. However, computer crime obviously has progressed since its advent, and victims can now include not only individuals, but also public bodies such as government.

More than half of computer crime cases at present are likely to occur against information and/or computer programmes. What conditions can be defined as composing elements of illegal alteration? These can be described as follows:

(1) There is no error message in the monitors;

---

[97] See '*Syakai kōgaku* (Social Engineering)', <http://www.ut-info.com/security/se.html> (print out on file with author).
[98] Murobushi, *supra* n.10, at 10-11.
[99] S.Takakubo, T. Nara, W. Ishikawa, & Y. Sato, '*Keihô* (Criminal Law)' (1983) Seirin, Tokyo at 6.

(2) The change is not particularly noticeable, however;
(3) The small change can reflect on the result seriously or on large scale;
(4) All signs are eliminated after the transaction[100].

The European Commission Joint Research Centre identified the characteristics of cybercrime in particular. It concluded that cybercrime cannot be identified by the outcome (for instance, theft or blackmail) and its *modi operandi* is not a feature of the crime itself[101]. Instead of the outcome or the *modi operandi*, there are 14 general characteristics of cybercrime including;

(1) Pervasive;
(2) Remote and difficult to detect and to face;
(3) Global in its operation;
(4) Spans the spectrum from IT literate / skilled hacker to unskilled script user;
(5) Both internal and external to an organisation;
(6) Not age limited;
(7) Internet / web / network focused by the nature of the technology;
(8) For gain as well as malice / online vandalism;
(9) Seen as a technical challenge;
(10) Seen by many as a victimless crime;
(11) IT solutions alone are not sufficient deterrents or detection tools;
(12) Having a very large societal, business and personal impact;
(13) Indicators are often not available or understood;
(14) Successful system attacks can be traced to limited vulnerabilities[102].

They are, however, not at all brand-new characteristics only for cybercrime, having been identified since the advent of computer crime.

Needless to say, technical knowledge is necessary to commit computer crime (and cybercrime) to a greater or lesser extent. If it is committed perfectly, disclosure is not easy and the crime may be exposed only by accident. Unfortunately, the society will be unsound if the only way to expose computer crime is to wait for such an accident. It is meaningless to define computer crime as a serious economic crime if such accidents have to be relied upon for disclosure. Without disclosure, the seriousness and extent of the crime cannot fully be realised.

As Tiedemann suggested, the first peculiarity is that the illegal act does not directly connect with the consequence[103]. It is unnecessary for these two elements to exist in the same place or the same time zone. Connecting and bringing those together onto one line is very important, because this line is absolutely crucial for exposure and investigation. If

---

[100] Kanno, *supra* n.45, at 40-41.
[101] European Commission Joint Research Centre, *supra* n.54, at 16-18.
[102] *Ibid.*
[103] Tiedemann, *supra* n.9, at 166-171.

those two elements are not connected, discovering computer crime proves difficult. As a consequence of this, investigation would take a long time.

Suppose there is a bank named X. Y is an employee and commits a fraud. If X could find a loss, and if X fortunately detects Y's criminality, it might still be very difficult to estimate how much exactly had been lost. If Y is not concerned with X at all, and if Y successfully manipulates a computer from outside and commits a fraud, it is absolutely impossible to find criminal Y. Y might attempt the same type of fraud against another bank. This assumption might not only provide an example as to the relationship between places and times, but also expose another peculiarity, which is that the crime's effectiveness might continue until discovery. It seems reasonable to suppose that the longer it takes for a crime to be exposed, the more the losses will increase. According to the US Time magazine, the average loss from a bank robbery using a gun in the USA is about US $3,300[104]. However, the average loss from a computer crime in the USA is about US $ 430,000. In Japan, a record exists of two bank clerks who committed a serious fraud by inputting false data and successfully transferring about US $ 33,000,000 in 1979[105]. The above three figures, although comparatively old, are substantial.

As Kanno commented, if someone leaves one or more mistake(s) without knowing, this is not an illegal alteration, and even though it might cause a serious error, this mistake is technically called a "bug". On the contrary, if someone makes a mistake(s) knowingly, this action should be categorised as an illegal alteration. This raises an important question: Suppose a company named X develops and sells a number of programmes. (e.g. "software".) To succeed in business, especially in this rapidly progressing market, two elements are crucial: not only brand-new ideas, but also timing. To rush shipping software products to a market might lead to some mistakes. If the X's development group of programmes fails to discover an error before shipping, a "bug" still remains. What if they DO know the existence of the error? Is this illegal? Of course, this assumption is not a typical example of an illegal alteration, because this is not an exact example of alteration. However, it proves the difficulties in distinguishing between wilful negligence and a simple mistake.

It has been suggested that most of computer crime cases are committed by an employee or an ex-employee[106]. The problem of how to categorise an ex-employee, whether as "insider" or an "outsider", has been illustrated by the example of the bank clerk in the previous section. When a total stranger who is defined as an outsider commits a crime, that person may encounter more difficulties or risks than a current employee or an ex-employee. However, an ex-employee may have valuable knowledge at

[104] Murobushi, *supra* n.10, 210-212. Unfortunately, Murobushi did not mention its published year, the volume and the book number.
[105] *Ibid.*
[106] Murobushi, *supra* n.10 and *infra* nn.100 and 101, at 20-21.

his/her disposal, such as how the company works, the daily routine, and the time schedule. Moreover, an ex-employee may know a password or the pattern of a password to access computer programmes or database in the company s/he previously worked for. Therefore, it would seem that an ex-employee is better defined as an "insider" in some cases.

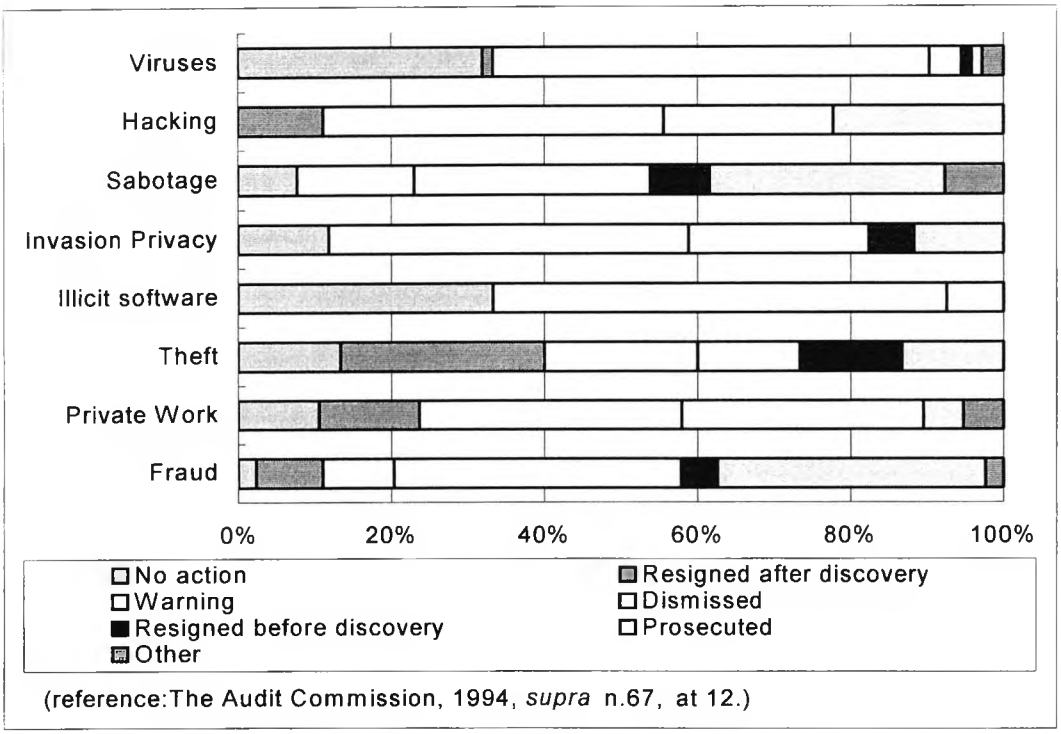
Parker suggested that only 20 to 25 % of all computer crime is reported[107], implying that 75 to 80 % of cases are not exposed. While no one knows if this surmise is true, on the other hand, there is no reason to doubt it. If one takes Parker's figure as a premise that such an extensive portion of cases are not exposed, the proportion of success must be high. There are some possible reasons why such high proportion of cases are not exposed:

It is possible to commit a crime
(1) in a short period;
(2) by remote control;
(3) without any physical evidence;
and;
(4) some sorts of computer crime might be invisible;
(5) inadequate legislation to criminalise the activity[108].

Any of the characteristics thus far mentioned in this section can be connected to each other. There is an assumption that to solve any type of crime against a company easily and with minimum loss, it is best not to notify the police[109]. Therefore, a victim (= a company) can be a potential enemy to the police. It is impossible for the police (or any relevant authority) to compile statistics on computer crime unless cases are reported. Exposure of a committed computer crime might be very dangerous for the public and the social confidentiality of a company, sometimes causing companies to try to solve the matter on their own without reporting it to the police. As the Audit Commission has argued, "organisations are loath to prosecute incidents of computer crime because possible publicity could result in a loss of confidence in their businesses[110]". This is a characteristic not only of computer crime itself, but also for keeping a high proportion of successfully committed computer crime undisclosed. According to the Audit Commission, only 58% of discovered cases are prosecuted, and furthermore, 14% have no action taken against them[111] (Table 1.1).

[107] OECD (1986), *supra* n.47, p.8.
[108] Murobushi, *supra* nn.10, 100 and 101, at 208-210.
[109] Murobushi, *supra* nn.10, 100 and 101, at 215-216.
[110] The Audit Commission (1985), *supra* n.66, at 22.
[111] The data is produced by the Audit Commission's survey conducted in 1987.

Table 1.1 Action taken against perpetrators



(reference:The Audit Commission, 1994, *supra* n.67, at 12.)

Computer crime is also likely to be committed by organised crime, such as the Mafia[112]. One good example is a CD crime. It is possible to indicate a weak area concerning computer crime in Japan which might make the country an accommodating target for computer criminals. Many Japanese, consciously or unconsciously, do not take "security" seriously. In their culture, the premise is still widely accepted that Japan is a very secure country[113]. Consequently, no one dreams that anything could happen to them. Furthermore, no one dreams that someone whom they know well might wrong them, therefore, they do not take sufficient precautions. Even in high security places, such as safety-deposit areas in banks (where people usually cannot go without a security pin), a friend or family member of a security guard may have access. This indicates a potentially dangerous situation.

2.3.3 Characteristics of Computer Criminals

Computer crime is usually categorised as economic crime. Certainly, there are murder cases in which computers are used intentionally (for example in euthanasia cases) or unintentionally, however such cases are usually categorised as murder, not computer crime. It means that a computer is only a tool to murder. Carroll insisted on his idea that a

[112] Murobushi, *supra* n.10 and *infra* n.105, at 10-11.
[113] Murobushi, *supra* nn.10 and 105, at 13.

computer is still only a tool even in cases of serious fraud[114]. This is an appropriate theory. But computer crime can be categorised independently from other crimes, because there are so many styles and characteristics, which make an independent categorisation possible. Therefore, this thesis attempts to provide a general identification of the characteristics of computer criminals.

According to Carroll, the anatomy of computer crime can be analysed in the acronym "MOMM": Motive, Opportunity, Means and Method, and it would appear that these are characteristics for computer criminals, not computer crime itself[115]. The first letter 'M' is for 'Motivation'. To understand criminals' motives in committing crimes is essential, not only for computer crime, but also for any type of crime. Particularly, it is obvious that many computer criminals are likely to be motivated by money. Carroll also described that motivation could be categorised into four elements: for money, ideology, compromise and egotism. It is not difficult to imagine these four elements of motivation, independently or in unison. The second letter "O", is for 'Opportunity'. Carroll defined opportunity as being equated to knowledge and access, and he also stated that these two elements can interfere with communications, computer operating systems, databases, etc., physically or electrically. The third letter "M" is "Means". What the purpose of a computer crime? It is sometimes to fraudulently obtain value, or sometimes to read or copy confidential information including military, diplomatic, law enforcement and so on. The fourth letter "M" is "Method". *Modi operandi* have already been mentioned. Although Carroll categorised all *modi operandi* in great detail, as they are almost identical, so they will not be mentioned here[116].

According to Murobushi's initial report on Japanese profiles of computer criminals — he (not she) is aged about 30, has a very good knowledge of computers or the use of computers, likes games, is "full of fight", and the like[117]. On the other hand, he recognised that not all offenders fall into this category. All the characteristics heretofore mentioned in this chapter can be proven in his latter idea to be examined subsequently. Simplicity and the fact that computer crime can be committed relatively easily encourages ordinary people, who have never previously committed a crime, to take the plunge. Opportunity to offend can, therefore, knock at one's door. Indeed, this categorisation and attendant characteristics do not restrict computer crime to men only. On the contrary, what is called the "sales point" of computer crime is that anyone can do it within a short period of time, without suffering a guilty conscience. Murobushi's statement, bereft of proof or evidence, is largely speculation, there is no proof or evidence. However, he did provide later research about computer criminals in Japan, based on factual cases:

---

[114] Carroll, *supra* n.40, at 582-585.
[115] *Ibid.*
[116] *Ibid.*
[117] Murobushi, *supra* n.10, at 222-225.

(1) Ages: 15-29 year-old for hackers;
25-39 year-old for computer crime except CD crime;
any age for CD crime.
(2) Sex: both. But many fraudulent cases, which occurred in banks, are committed by women.
(3) Others: there are only a few cases in Japan, which need advanced or specific knowledge[118].'

CD crimes are often committed in Japan. These crimes are, however, apt to be detected by both financial institutions themselves and the police comparatively, because they must have an alarm device and a reporting system to the police for CD crime.

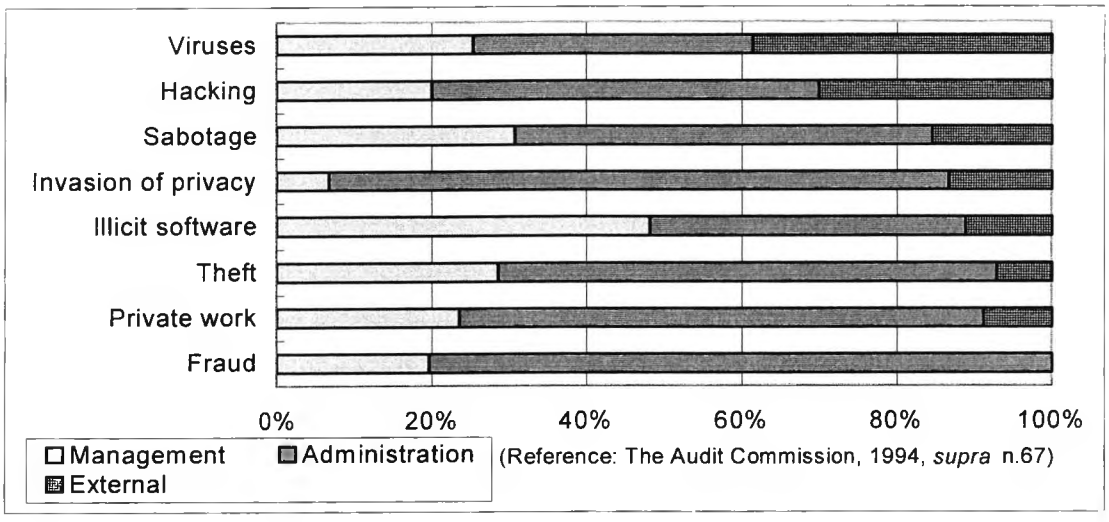
Parker has studied computer criminals with research based on more than 1,000 reported cases and 30 interviews with criminals in the SRI International[119]. His conclusion is that to generalise classification or characteristics of computer criminals requires circumspection. He also mentioned the opinion of a computer security consultant, who explained the popularity of economic crime. In the past, he stated that economic crime was likely to be committed by a managerial class in companies, whereas presently, computerisation demands diverse people in many types of posts. Some of these are important positions and confidentiality is requested, even for those not in a managerial class. In other words, the computer has provided many people with the utility and opportunity to access information. Parker also stressed an interesting point — professional computer criminals never recommit the same type of crime[120]. This opinion remains widely open to debate. It is based on his classification of computer criminals: an amateur, a madman, a system hacker, the professionals, a company or a criminal organisation (e.g.,the Mafia), radicals, or the government. "The professionals" refers to people who make a living through criminal activities. However, as Parker mentioned, they can not always use a computer[121]. Considering this, computer history may not be sufficiently long to produce "the computer crime professionals". Are the computer-age criminals perhaps forthcoming?

As indicated earlier, a high proportion of computer criminals are insiders. According to the Data Processing Management Association, 98% of computer crime was committed by insiders[122]. It also showed that 27% of known perpetrators were motivated by ignorance of proper professional conduct, 26% by misguided playfulness, 25% by personal gain, 22% by maliciousness or revenge. Here is a table, prepared by the Audit

[118] Murobushi, *supra* n.10, at 228-231.
[119] Parker (1984), *supra n.42* and *infra* n.112, at 137-139.
[120] Parker (1984), *supra n.42* and *infra* n.112, at 140-142.
[121] Parker (1984), *supra* nn.*42* and 112, at 143-149.
[122] The figure was suggested by A 1985 survey of the Data Processing Management Association. See D. Bender, 'Computer law, vol.4' (1997) Matthew Bender, New York, at 4B-124.

Commission, to show the perpetrators[123]. (Table 1.2)

Table 1.2: Perpetrators of incidents



Interestingly, the majority of perpetrators are the administrative staff (60%), whereas in the 1990 survey, the majority were in supervisory and managerial positions[124]. This proved the conclusion of the SRI research in the previous section. 85% of perpetrators were insiders, thus demonstrating the premise "Opportunity makes a thief[125]".

It is important to discuss the ethics of computer criminals. It would appear that when people decide to commit a crime, ethics is supposed to play an important role in the decision. Parker highlighted two types of ethics computer criminals may have when deciding to commit a crime. Firstly, computer criminals do not consider it intrusive to use facilities or services if there is no harmful damage. This behaviour is the same as an unauthorized access, which has already been mentioned above. The reason why this is recognised as an illegal action is explained by Parker using the theory of Kant[126] that an unauthorized access infringes on the rights of a legitimate user. Secondly, there is the ethic called known as the "Robin Hood Syndrome" in criminology. The criminals believe that they are committing a crime against a computer which is an inanimate object, and thus there is no victim. Therefore, committing a computer crime is not illegal[127]. It is very difficult to define both these ideas as "ethics", because the ethics which have been previously discussed mostly apply to children, who do not know what is right or wrong. Thus, the

[123] The Audit Commission (1994), *supra* n.47, at 12.
[124] *Ibid.*
[125] The phrase 'Opportunity makes a Thief' is from the title of the Audit Commission, (1994), *supra* n.47.
[126] Immanuei Kant, (1724-1804) a German philosopher.
[127] Parker (1984), *supra* nn.42, 112 and 113, at 242-246.

computer criminal's ethics are still likely to be at the level of self-justification.

2.3.4 Impacts of Computer Crime

2.3.4.1 Three Elements Concerning the Impact of Computer Crime

According to Meier and Short, there are three types of impact on white-collar crime: economic harm, physical harm and damage to the social fabric (including moral climate or climates). They also explained that "economic and physical harm depend to some extent on each other, most typically in the form of economic costs associated with physical damage to health as a result of disease or injury, and in the extreme case, death", and "damage to moral climate or social fabric is presumably partly a function of perceived and experienced economic and physical harm[128]." In their explanation, therefore, "economic harm" is likely to hold a secure meaning for employees' families, but not for the company because they have to pay substantial costs.

Computer crime also includes these elements, to a greater or lesser extent. However, the meaning of "economic harm" in these types of crime is, essentially, more realistic than the meaning of other elements. From the viewpoint of fraud, "economic harm" is usually caused by employees against companies. The meaning of "secure" is supposed to be defined as a second priority. Huge fraudulent "economic harm" can also inflict serious damage on the social fabric. This has been proven by a series of corruption cases in Japan in 1997[129].

If the size of a computer crime is tremendous enough to affect a national economy, it is likely to have an impact on the International economy since national economies have been obliged to develop closer relations with each other and are now mutually influential. To fight computer crime on an international level implies that the crisis that results from a computer crime being committed may threaten universal economic values, particularly on an international level.

2.3.4.2 The Cost of Computer Crime

Estimating the cost of computer crime is said to be meaningless — an immovable fact when researching the subject in depth. The reason is, as has been mentioned, it is impossible to cover all cases, for not all cases are reported to the police or the relevant authorities. Yet, estimating losses still plays a major role in illustrating the huge impact of computer crime.

---

[128] Meier & Short (1995), *supra* n.18, at 94-95.

[129] There had been some corruption cases in 1996-1997 in Japan, for example, Yamaichi and Nomura Brokerage Firms.

The Council of Europe, in 1990, showed some examples of this impact on member countries, such as the German bank clerk who committed an input manipulation and transferred 1.3 million DM. There were 31,000 computer-related incidents in France in 1987, and this loss was estimated at 3.9 million FF[130]. The American Bar Association estimated annual losses ranging from US $145 to 730 million. Backhouse and Dhillon also showed the same figures about the USA. An interesting example occurred in China when a hacker was executed for embezzling a sum worth £122,000 from the Agricultural Bank of China[131]. According to Duff & Gardiner, the total loss was approximately £1.1 million in 1984 with 943 public and private organisations, £2.6 million in 1987, and £2 billion in 1989 in UK[132]. Collier and Spaul in their research insisted that the British annual losses from computer fraud exceeded £407 million[133]. The figures are likely to constantly and rapidly increase day by day. (Table 1.3)

[130] See European Committee on Crime Problems, Council of Europe, 'Computer-related crime: Final report: Recommendation No. R (89) 9' (1990) Council of Europe, Strasbourg, at 33.

[131] This news was also reported but embellished a little in S. Le Doran & P. Rose, 'Cyber Thrillers' translated into Japanese by T. Kuwabara, (1996) Bungei-Syunjū, Tokyo. See J. Backhouse & G. Dhillon, 'Managing computer crime: a research outlook', 14 Computer and Security 7, 1995 at 626-648.

[132] Duff & Gardiner (1996), *supra* n.20, at 214-215.

[133] See P.A. Collier & B.J. Spaul, 'A Forensic Methodology for Countering Computer Crime', in I. Carr, 'Computers and the Law' (1994) Intellect, Oxford, at 145-146.

Table 1.3: Range of Frauds

Range (£)	1987	£	1984	£	1981	£
Not known/Nil	63	---	13	---	17	---
Up to£250	6	730	13	1,287	8	1,055
251-500	7	2,777	4	1,472	6	2,681
501-1,000	5	3,785	7	6,595	4	3,164
1,001-1,500	4	5,064	5	6,438	2	2,600
1,501-2,500	4	7,834	5	9,580	6	12,403
2,501-5,000	9	35,607	9	33,523	3	11,100
5,001-7,500	1	6,853	1	6,000	3	16,491
7,501-10,000	1	8,000	3	26,965	3	26,888
10,001-15,000	---	----------	4	47,679	3	33,767
15,001-20,000	3	54,000	1	20,000	4	80,000
20,001-50,000	8	252,900	6	160,763	4	152,000
50,001-100,000	4	314,500	3	204,000	2	133,000
100,000-250,000	1	193,781	3	609,185	2	430,000
250,001+	2	1,675,520	---	----------	---	----------
Total	**118**	**2,561,351**	**77**	**1,133,487**	**67**	**905,149**

(Reference: The Audit Commission, 1994, *supra* n.67 *et seq.*)

Taking up recent statistics, the Department of Trade and Industry (UK DTI) reported in 2002 that three types of offences (hacking, cyber fraud and software bugs) cost Britain up to £10 billion a year. It obviously includes only three offences; one of the most popular offences (computer viruses) is excluded. It is hardly possible to establish exactly how much businesses have suffered from computer crime. According to the DTI report, 50% of all businesses were victims of such attacks (25% in 2000 and less than one fifth in 1998). It also suggested that four out of five of the biggest companies were victimised by hackers, computer viruses or fraud in 2001. All in all, the report estimated the average cost of each security lapse at £30,000. Several companies disclosed that they suffered over £500,000 as a result of hackers, computer viruses or fraud[134].

The 2002 CSI/FBI Survey (USA) also reported that 90% of respondents had detected computer security breaches within the last twelve months, with 80% acknowledging financial losses. 44% were willing or able to quantify such losses and this reached a reported $455,848,000[135].

[134] See 'Cybercrime - what SME should know', <http://www.blindtiger.co.uk/IIA/uploads/-38c9a362-ed71ce5fa5--761f/CybercrimewhateverySMEshouldknowpdf.pdf> (print out on file with author).
[135] *Ibid.*

Table 1.4: The Cost of Computer Crime					
	Total Annual Losses				(Unit: $ million)
	1997	1998	1999	2000	2001
Theft of proprietary information	20.04	33.54	42.49	66.70	151.23
Sabotage of data of networks	4.28	2.14	4.42	27.14	5.18
Telecom eavesdropping	1.18	0.56	0.76	0.99	0.88
System penetration by outsider	2.91	1.63	2.88	7.10	19.06
Insider abuse of Net access	1.00	3.72	7.57	27.98	35.00
Financial fraud	24.89	11.23	39.70	55.99	92.93
Denial of service	N/A	2.78	3.25	8.24	4.28
Spoofing	0.51	N/A	N/A	N/A	N/A
Virus	12.49	7.87	5.27	29.17	45.28
Unauthorized insider access	3.99	50.56	3.56	22.55	6.06
Telecom fraud	22.66	17.25	0.77	4.02	9.04
Active wiretapping	N/A	0.24	0.02	5.00	0
Laptop theft	6.13	5.25	13.03	10.40	8.84
Total Annual losses	$100,11	$136.82	$123.79	$265.58	$377.82
Grand total of losses reported (1997-2001): $1,004,135,495					
(Reference) The CSI/FBI 2001 Computer Crime and Security Survey, Computer Security Institute, '1 Computer Security Issues & Trends 7', 2001.					

Table 1.4 displays the cost of losses for the past five years in the USA. The 2001 CSI/FBI report explained that 78% of respondents acknowledged financial losses whereas only 37% of them were able to quantify the losses. Thus, there were some reported cases that were unsuccessful in quantifying the losses.

As is obvious thus far, all the above figures remain uncertain to a greater or lesser extent. The introductory part of this section adequately highlights the reason why there is no guarantee of the accessory of such statistics. If Parker's estimation in the previous section is accurate, namely that 20 to 25% of the cases were exposed, all these figures must be increased four times, five times, perhaps, ten times, or more. This result can be recognised as "incredible losses".

There have been established many research institutions and organisations worldwide on computer crime, cyber crime and the like. They mostly correspond with each other to promote combating the said crimes, and publish statistics based on their surveys and research[136].

[136] The activities of those institutions and organisations are beyond the scope of this thesis. Thus, some of their names can be simply introduced here:
* Computer Security Research Centre, the London School of Economics and Political Science (LSE, UK)

2.3.4.3 Public Interest and Social Impact

Computer crime is unlikely to attract public interest, except in cases of serious fraud. This is because, as Meier and Short stated, both victims and perpetrators in computer crime are often organisational[137]. They also mentioned that crimes resulting in physical harm are rated as more serious than crimes resulting in economic harm. Hence, computer crime is unlikely to be familiar to the general public, so they might feel that it could not happen to them. On the other hand, many companies are extremely likely to be interested in computer crime and its impact. According to Longley, computer crime could cause catastrophic consequences for the social fabric[138]. He also warned of the potential danger of immoderate dependence on computer-based technology. Once computer crime is committed, many unexpected matters might hit the company: huge losses, injury, or the denial of human rights. If it targets a government, national sovereignty might be damaged. For instance, there are cases where computer systems were attacked by terrorist groups in France and Italy[139]. It is also easy to create chaos in the world economy, if massive damage is caused in the stock markets' network.

The side effects of computer crime are also considerable. Once computer crime is committed, a company has to spend time and money, not only to recover the former status, but also for investigation, police reporting, and court appearances: in the case of civil proceedings, the legal costs, travel expenses for witnesses etc. are considerably included as the cost (Table 1.5). In extreme cases a company might have to consider spending huge amounts of money on security measures, software modifications etc. to protect the company itself[140].

---

* Computer Security Institute / FBI Yearly Survey
* CERT CC
* High Technology Investigation Association
* Internet Fraud Complaint Centre (IFCC)
* National White Collar Crime Centre (NW3C)
* National Consumers League (NCL) – Internet Fraud Watch

European Commission Joint Research Centre, *supra* n.54, at 6.

[137] Meier & Short (1995), *supra* n.18, at 96-97.

[138] See Longley, *supra* n.41, at 322-325.

[139] *Ibid.*

[140] *Ibid.*

Table 1.5: Incidents and Associated Losses and Costs

Incidents	No.	Loss(£)	Others costs(£)	Total(£)
Input	38	2,240,790	137,000	2,377,790
Output	1	44,000	2,500	46,500
Data	19	140,961	32,000	172,961
Programme	3	101,000	--------	101,000
Theft data	3	2,000	2,000	4,000
Theft software	5	800	500	1,300
Theft facilities	1	1,700	--------	1,700
Hacking	32	100	21,950	22,050
Private work	13	30,000	6,000	36,000
Sabotage	3	--------	--------	--------
Total	**118**	**£2,561,351**	**£201,950**	**£2,763,301**

(Reference: The Audit Commission, 1994, *supra* n.67 *et seq.*)

2.3.4.4 Length of Services and Outcomes of Computer Criminals

From Table 1.6 below, it can be seen that people who contributed to a company or an organization longer periods, were more likely to commit substantial fraud (resulting in immense losses) relatively easily.

Table 1.6: Length of Service

Loss (£)	Service (Years)	
	In post	In organisation
549,865	18	27
44,000	15	15
27,400	10	25
2,214	10	25
24,000	10	24
1,039	10	10
0	10	10
400	10	10
60,000	10	10

(Reference: The Audit Commission, 1994, *supra* n.67 *et seq.*)

Tables 1.7 to 1.9 below are concerned with prosecution in the UK in the 1987 Audit Commission survey[141]. According to the survey, some cases did not appear in these surveys because they were pursued after the employee had resigned. There were only 40 cases (two of them were pending) prosecuted. Whether or not their results (in 118 reported cases) succeeded, is not shown in the mentioned surveys. The Audit Commission

also stated that eleven were committals and six were suspended in the 17 sentences passed, and details of the rest of the cases were not provided. Six cases were fined within ranges from £95 to £34,487.

Table 1.7: Prosecution

Prosecution	No.	Theft Act.	Forgery Counterfeiting Act.	Not Disclosed
Successful	35	22	1	12
Unsuccessful	3	1	---	2
Pending	2	1	---	1

(Reference: The Audit Commission, 1994, *supra* n.67)

Table 1.8: Committal Sentences

Sentence (years)	Fraud (£)
5	1,125,655
4	44,000
4	24,000
3	549,865
3	0
2	193,781

(Reference: The Audit Commission, 1994, *supra* n.67)

Table 1.9: Suspended Sentences

Sentence (years)	Fraud (£)
9	100,000
12	100
12	1,200
18	27,400
24	2,858
24	54,500

(Reference: The Audit Commission, 1994, *supra* n.67)

While the Audit Commission suggested that companies and organizations ought to be compelled to report all computer crime, the Scottish Law Commission stated that there was no general duty to disclose crimes[142].

[141] See the Audit Commission (1987), *supra* n.49, at 22.
[142] *Ibid.*, at 23.

2.4. Problems Involved In The Criminalising Procedure

2.4.1 General Difficulties Criminalising Computer Crime

There can be no doubt that many of the previously shown characteristics make combating computer crime difficult. For example, low public awareness, especially in the attitudes of companies towards computer crime, might embolden criminals to commit crime, and insufficient evidence or statistics creates a dilemma as to what prosecution is most suitable. Regarding an ordinary crime, especially traditional international crimes, certain elements are needed. For instance, in the narcotic context, human effort, vehicles for conveyance, and a route of passage to move the product (e.g. opium) between nations[143]. In the case of conveyance by human effort, a passport is required at a border. The types of activities aforementioned help law enforcement to find, investigate or prosecute a criminal. However, in many cases, nothing similar exists in computer crime[144]. All these issues are problems not only in the domestic dimension but also on an international scale.

How was early computer crime dealt with? It is comparatively easy to imagine authorities, such as the police, being confused as to how to deal with the first computer crime committed, as it was extremely difficult not only to comply with the demands of prosecution, but also to define an offence as a crime. Therefore, in the early days of computer crime, it was probable to prosecute using all types of law and cases, such as intrusion into the structure, fraud, larceny, theft of services or labour under false pretences, receipt of stolen property and so on[145].

Attempts will now be made to focus observation on the difficulties of legislation. It is true that the history of legal response to computer crime has largely been a delayed response to the danger of large-scale fraud[146]. According to the United Nations manual on the prevention and control of computer-related crime (hereinafter "UN manual"), there are some particular reasons: the biggest being "the heretofore impossible has now become possible [by computers] ", and also, technological progress is too rapid for legislation and criminal justice systems to keep pace[147]. As Karnow indicated, the first claim to criminalise an offence using a computer involved the viewpoint of whether the right to control the movement of every electron and fibre cable phone existed or not[148]. According to Duff

---

[143] See 'COMPUTER CRIME', <http://www.kcl.ac.uk/orgs/icsa/crime.htm> (print out on file with author).
[144] *Ibid.*
[145] See The Kightmare, 'Secret of Super Hackers', translated into Japanese by R. Matsufuji, (1995) Noritsu Management, Tokyo at 326.
[146] Kaspersen, *supra* n.64, at 44.
[147] See 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.
[148] See C.E.A. Karnow, 'Future Codes: Essays in Advanced Computer Technology and the Law' (1997) Artech House, London, at 205-206.

and Gardiner, the counter arguments for criminalising hacking existed in the Law Commission[149].

The first argument of the Law Commission was that civil law is ineffective in regulating hacking. Karnow also stated that "when the breaches are mild, use the civil law and sue; when the breaches are considered severe, enter the criminal law[150]." Hacking is unauthorized access in order to damage data and computer programmes, or create work disruption. The Law Commission reached the conclusion that "by criminalising unauthorized access to computer system at a preparatory stage, individuals will be deterred from commission of these ancillary offences[151]." But another, deterrent, argument should be raised: Does this really reduce computer crime offences? Take one assumption: what is the answer to this question, if one is a criminal who enjoys hacking activities, and/or watching how people react to what one has done, will the Law Commission's aim really deter? The answer is likely to be "No". The Law Commission suggested arguments against criminalisation. Firstly, the Commission knew that it was difficult to claim right of privacy, even if privacy was obviously invaded by hacking. Secondly, there were presumable difficulties concerning detection and enforcement. However, as Duff and Gardiner mentioned, there is an acceptable view to this second argument, in case privacy invasion damage caused by hacking or other types of economic offences is serious[152]. Information (in other words, data) is likely to include private affairs (for example, employment records, tax records). As the futurist Alvin Toffler once said, information can be defined as the commodity of the highest value; information being kept in computers, including new product plans, marketing plans, customer lists, and similar information, has great value in a company[153]. The economic harm will be serious even though a criminal may be involved only in hacking, which does not necessarily result in tangible damage. Hacking, though normally considered a violation of privacy, also has a dangerous element, enough to harm a company. Therefore, computer crime includes two fundamental aspects: firstly, infringement of privacy, and secondly, economic damage. As Toffler suggested, it is critical to recognise the value of intangible property (information) in case of abuse.

In the event of criminalising previously unknown types of computer crime, arguments as to a definition will inevitably arise. This is because the extent that offences by computers can be addressed depends on to the extent that a certain definition works in national legislation. There are two methods to define computer crime, broadly or precisely, which have been adequately discussed thus far. The percentage of the general

---

[149] Duff & Gardiner, *supra* n.20 and *infra* n.143, at 218-221.
[150] Karnow, *supra* n.140, at 205-206.
[151] Duff & Gardiner, *supra* nn.20 and 143, at 218-221.
[152] *Ibid.*
[153] D.L. Carter, and A.J. Katz, 'Computer Crime: An Emerging Challenge for Law Enforcement' available on <http://www.crime-prevention.org.uk/> (print out on file with author).

public's knowledge or understanding of computer crime and technology is probably insubstantial. As Rostoker & Rines suggested, all persons involved, such as judges, prosecutors, defence attorneys, and law enforcement officers, should have, at the very least, a somewhat rudimentary knowledge of a computer itself and its usage[154]. Otherwise, it is almost impossible to deal with computer crime properly, as, even if an effective law exists, it will be as useful as casting pearls before swine.

2.4.2 Transnational Difficulties Combating Computer Crime

It is possible to commit a computer crime from remote locations using telecommunications systems; therefore, a place of offence is not limited to one country[155]. Elbra gave one example, "the malefactor [defined as X] can be in one country [defined as A], the relevant computer in another [defined as B], and the victim in a third [defined as Y, and Y's country defined as C]". This enables one to understand the problem of jurisdiction more easily. Which jurisdiction principle works most effectively? Which country can claim a jurisdiction to prosecute X? The OECD reported that the principle of territorial jurisdiction has been considered as the most applicable, since the advent of computer crime.

Furthermore, in the USA and Japan, computer crime cases are prosecuted according to this principle[156]. The UN also mentioned that the primacy of territorial jurisdiction has been generally accepted amongst the UN countries[157]. It is one of the jurisdictions which regards a state territory as important with respect to its sovereignty. That is to say, any country can invoke a computer crime under a national law if a country has criminalised that offence. For example, under the Computer Misuse Act 1990 in the UK, there are two components in offences: unauthorized access and further offence. Whether an offence is first committed in the UK and a further offence in another country, or conversely, the UK can claim jurisdiction. However, two factors are required:

(1) The conduct would have to constitute an offence in the UK, and;
(2) It would be punishable under the law of the other country[158].

There are two doctrines: the ubiquity doctrine and the effects doctrine. The former is considered as determining the place where a crime is committed, and the latter one has been applied in the USA and some Common Law countries such as the UK, in cases of transnational crime. These two doctrines help legitimise claims of territorial jurisdiction[159]. On

---

[154] See Rostoker & Rines, *supra* n.52, at 348.
[155] See T. Elbra, 'A Practical Guide to the Computer Misuse Act 1990' (1990) Blackwell, Oxford, at 19.
[156] See OECD (1986), *supra* n.47, at 66, and Wasik, *supra* n.30, at 196.
[157] See 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.
[158] See Elbra, *supra* n.147, at 20.
[159] 'International review of criminal policy - the United Nations Manual on the

the other hand, if a computer crime is committed in a country where no effective legislation to penalize the criminal concerned exists, extradition for prosecution to the criminal's country of origin, may be impossible without mutual consent. Without mutual conventions between two countries, it might be very complex and take a long time to come to prosecution. For instance, even though the UK established the Computer Misuse Act in 1990, extraditing and prosecuting without international co-operation in a computer crime case is almost impossible. A co-operative policy amongst the countries involved should be included wherein they agree on a mutual definition of computer crime. Nevertheless, even if a convention or treaty exists between two countries involved in a computer crime case, the following issue arises: the principle of double criminality. It is necessary to meet conditions of double criminality for extradition or mutual assistance[160]. That is to say only an offence, which both countries concerned have criminalised, can be penalised and extradited. It may be possible to deal with computer crime on an international level by synthesising two jurisdiction principles. For example, according to the UN manual, the active nationality principle can be applied in conjunction with the territorial jurisdiction. This can only be applied to serious offences[161]. In transnational computer crime cases, collecting evidence proves complex. As a result, without sufficient evidence, prosecution becomes problematic. For successful prosecution of computer crime, these three factors relating to the collection and use of evidence are essential:

(1) The coercive powers of law enforcement authorities to gather evidence;
(2) The specific legal problems of gathering, storing and linking personal data in criminal proceedings; and
(3) The admissibility of evidence consisting of computer records in criminal court proceedings[162].

However, the complicated nature of computer crime, in terms of making it understandable to laymen, such as prosecutors, judges and juries, is likely to prove very difficult. In particular, a language barrier makes transnational crime more hazardous. In such a case, all judicial powers, including the police powers, may not work effectively. A final dilemma in transnational computer crime is imposing penalties after extradition has occurred. This is due to each country having an individualised penalty system. Consequently, an imposed penalty may prove insufficiently severe for the crime concerned.

---

prevention and control of computer-related crime', *supra* n.15.
[160] *Ibid.* Heymann also mentioned the same meaning, but he used 'dual criminality', not 'double criminality'. See S. Heymann, 'Legislating Computer Crime', in 34 Harvard Journal on Legislation 2, 1997.
[161] 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.
[162] The Council of Europe, *supra* n.35, at 70.

2.5. The Future Prospect on Combating Computer Crime

2.5.1 Effective Domestic Legislation

It would seem no longer questionable that computer crime is dangerous enough to criminalise, not only for a company, but also for a state economy. It is essential to criminalise and combat computer crime to protect a country's national interests. Furthermore, the potential danger of computer crime is increasing in accordance with technological progress. Therefore, as the UN manual insisted, criminalising and combating computer crime is vital not only for developed countries but also for developing countries. It is imperative for countries to establish a framework for computer crime and determine its status at a national level before effective legislation can be introduced. Moreover, it is important to draw public attention to computer crime. Establishing working groups with a profound knowledge of computers will be helpful not only for drawing public attention to the problem, but also for suggesting methods to combat computer crime. These working groups should include government, judicial and industrial circles, with mutual co-operation between them[163]. The most important point is for an effective legislation consensus to be established in each country. The UN manual suggested the following measures for the preparation of a national legislation:

(1) Reviewing the present state of legislation in light of the issues raised in [the UN] manual, assessing the substantive and procedural adequacy of their legal and administrative infrastructures and recommending appropriate solutions;
(2) Co-operating in the exchange of experience and information about legislation and judicial and law-enforcement procedures applicable to computer crime;
(3) Undertaking a review of sentencing legislation, policies and practices with a view to developing more effective penal sentencing provisions;
(4) Ensuring periodic reviews and reform of laws, policies and practices in order to incorporate changes arising from technological developments and trends in computer crime;
(5) Inviting educational institutions, associations of hardware and software manufacturers and the data processing industry to add courses on the legal and ethical aspects of computers to their educational and training curricula;
(6) Developing a mechanism to educate potential victims of computer crime and to expose the real extent of computer crime;
(7) In view of international character of data-processing and information technology, sharing security standards and procedural techniques among all sectors of the industry, both nationally and internationally;
(11) Encouraging the creation and implementation of national computer

[163] 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.

security legislation, policies and guidelines;

(12) Encouraging management and senior executives to commit their organisations to security and crime prevention;

(14) Developing and promoting computer ethics in all sectors of society, but especially in educational institutions and professional societies;

(16) Educating the public about the prevalence of computer crime and the need to promote computer ethics, standards and security measures;

(17) Promoting victim co-operation in reporting computer crime;

(18) Training and educating personnel in the investigative, prosecutorial and judicial systems[164].

In order to effectively combat computer crime, periodic reviewing (item 4) and training schemes (items 5 and 18) are essential to ensure that the progress of computer crime and technology are followed. The FBI, on the other hand, indicated several actions, which should be put into action to protect computers in general, such as the using of secure firewalls and encryption[165].

However, legislation in any country combating transnational crime, such as computer crime, must be based on a common consensus, rather than countries adopting legislation primarily to satisfy individual national economies. In particular, it is vitally important to avoid over-criminalisation regarding the extension of existing criminal law to deal with computer crime. Accepting the broad definition as to what computer crime entails may also lead to over-criminalisation. It will further lead to serious confusion in the criminal justice system. It would appear that there are two choices to resolve this problem. The first is to have a precise definition of computer crime, to avoid over-criminalisation. It is necessary to review national legislation, make decisions as to which criminal law is applicable, and make a criterion as to the appropriate extension of legislation on combating computer crime. The UN manual stated one criterion in defining or restricting criminal liability: acceptable extension of criminal law under careful examination and justification — i.e., that offences in this area be limited primarily to intentional acts[166]. Otherwise, the freedom of both individual and international trade may become restricted. Extreme legislation to combat computer crime is also likely to restrict citizens' rights if it proves to be too stringent. Computer crime legislation proves to be too stringent. In addition, commercial profit might incur serious damage if countries restrict the use of computers. The People's Republic of China has the most severe computer crime legislation. The Chinese government decided to control Internet usage in

---

[164] Items 8-10, 13 and 15 are omitted due to their irrelevance. 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.

[165] 'Federal Bureau of Investigation National Computer Crime Squad', <http://www.fbi.gov/programs/compcrim.htm> (print out on file with author).

[166] 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.

September 1996 [167] — restricting not only pornography but also anti-governmental opinion and activities and Taiwanese information, especially political criticism of Chinese government policy. The Chinese cultural, political and legal environments enforce this legislation and resistance is minimal[168].

The second choice is to define not just computer crime itself, but what specifically must be protected. There are some intangible objects at risk in terms of computer crime. In short, they are, for instance, data or information, computer programmes and the like. Strictly speaking, confidentiality, integrity and availability of the said objects must be protected. These issues will be discussed at length in the following chapter.

An interesting example is in France. Legislation called *Loi Toubon*, has been adopted since 1994. Its purpose is mainly to protect French language and culture, and it prohibits educating or going into business solely in a foreign language that is not combined with French[169]. The *Loi Toubon* may have a subsidiary purpose in that the French government aims to protect French profits in commerce through exclusive usage of their mother tongue, as doubt or misunderstanding is eliminated when using one's native language in commercial transactions.

All countries have an individual legal system and culture making it difficult to come to a universal consensus regarding computer crime laws. The choice, whether to modify an existing law or introduce a new law, depends on one country agreeing with another. It is, therefore, imperative to have a common cornerstone for proceeding at the same direction internationally. A suggested solution is to adopt an existing idea, such as the minimum list and the optional list, provided by the Council of Europe, into a national legislation. In particular, this would be instrumental in setting up national legislation to combat computer crime in legislatively developing countries.

2.5.2 The Real International Harmonisation

International harmonisation to combat computer crime raises problematic issues — essentially because computer crime is considered a transnational crime, which can harm the international economy. According to the UN manual, it is necessary to have a strategy to examine and promote crime prevention programmes on both national and international levels, both immediately and in the long term. It also stated

---

[167] There are other countries, where restrictions or the Internet exist: Germany and Singapore. However, these countries have restricted mainly pornography on the website. See K. Ebata, 'Information War' (1997) Far East Economics, Tokyo at 192-194.

[168] H.A. Wan, 'An Analysis of Chinese Laws against Computer Crimes', 5 Journal of Global Information Management 2, 1997.

[169] Hirano & Makino, *supra* n.1, at 59-60.

that this would foster the political will to create a secure information community and the universal criminalisation of computer crime. There are other advantages, highlighted by the UN, for harmonising the procedural processes to combat computer crime:

(2) The expansion of international trade and commerce raises a concomitant need for laws that will adequately safeguard economic interests and facilitate, stabilise and secure economic activities;
(3) International legal harmonisation increases the ability of transnational business and other computer users to predict the legal consequences of criminal misuse of computer systems. Predictability leads to confidence and stability on the international investment market;
(5) Harmonisation can help to avert market restrictions and national barriers to the free flow of information and the transfer of technology;
(6) The harmonisation of laws, including criminal laws, could promote equal conditions for competition;
(7) Better harmonisation can prevent some countries from becoming havens from which international computer crime could be committed with impunity;
(8) Harmonisation facilitates law enforcement by the agencies of different countries because it provides a common understanding of what types of conduct constitute crime and, in particular, computer-related crime.
(9) The harmonisation of substantive law facilitates the extradition of alleged or fugitive offenders.
(10) Harmonisation facilitates mutual legal assistance, that is, the use of legally controlled investigatory powers, such as search and seizure, examination of witnesses, electronic surveillance etc., by one country for the benefit of another country. Even where dual criminality is not a prerequisite, a common conceptualisation of what constitutes a crime assists the law-enforcement and judicial authorities of the country in undertaking
(11) The harmonisation of offences facilitates the harmonisation of procedural law with respect to investigatory powers[170].

Items (2) to (6) are aimed at enhancing the world economy, and items (8) to (11) are aimed at facilitating international legal transactions. The item to attract attention is (7): it is aimed at preventing the creation of "havens" — places where computer crime can be committed without penalisation. Such "havens" still exist, for example, in Japan where it is problematic to penalise a computer criminal who has done unauthorized private work (i.e., time theft) because of a lack of clear consensus in the Japanese judicial circle. The significance of promoting harmonised legislation internationally is, therefore, indisputable. To fulfil the UN advantages of international harmonisation, the UN manual recommends:

[170] Items 1 and 4 are omitted due to their irrelevance. 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.

(1) Within regional groups or associations, [to conduct] comparative analyses of substantive and procedural law relating to computer crime;
(2) [To attempt] to harmonise substantive and procedural law among the States of a region by developing guidelines, model law or agreements;
(3) When negotiating or reviewing treaties on extradition, mutual assistance or transfer of proceedings, whether bilateral or multilateral, addressing the following issues, [to take] into account human rights, including privacy rights, and the sovereignty of States:
(4) [To ensure] a jurisdictional base for the prosecution of transborder, computer-related crime and enacting mechanisms for resolving jurisdictional conflicts [by];
    i. Imposing obligations to extradite or prosecute offenders;
    ii. Facilitating mutual assistance, particularly regarding synchronised law enforcement, transborder search and seizure and the interception of communications[171].

It is imperative to reform sentencing at a national level before dealing with the international level. As aforementioned, it would be easy to utilise international recommendations, such as those of the Council of Europe and of the UN[172]. Archiving long-standing efforts, the Council of Europe published the Convention on Cybercrime in 2001 as briefly mentioned earlier. It placed great importance on cybercrime (over computer crime) in consideration of its seriousness. However, it is too early to celebrate victory. First of all, this Convention has not been adopted worldwide. Secondly, some countries have just started the preparations for their existing criminal law to fulfil the requirement of the Convention[173]. Indeed, international harmonisation is not yet accomplished. In other words, half-finished international co-operation between nations is likely to allow for the existence of "computer crime havens" or "data paradises" where the computer criminal takes refuge[174].

3. The Methods of Cyber Risk Management

In the previous section, computer crime as a portion of cyber risk has been well examined. In reality, cybercrime is the centre of attention compared to computer crime according to the rapid development of computer technology. However, it is concluded that cybercrime *is* a part of computer crime. Some types of traditional computer crime, which do

[171] *Ibid.*
[172] Drug trafficking and money laundering have already been recognised as transnational crimes. Because they are in the similar crime range with computer crime, both being concerned with the economy, the process used to make the existing legislation for drug trafficking and money laundering, may prove useful in the computer crime legislation. Carter & Katz, *supra* n.145.
[173] Fuller discussion on this Convention will be presented in the following chapter.
[174] 'International review of criminal policy - the United Nations Manual on the prevention and control of computer-related crime', *supra* n.15.

not have any cyber factor, such as simple theft or time theft, do not have much impact on a victim company. Nevertheless, it runs contrary to the purpose of this thesis to exclude a potential risk simply because it is minor.

As previously mentioned in Chapter I, cyber risk is suggested to include computer crime, employees' operational errors or computer system failure, which fall within the definition of operational risk[175]. Even if a certain behaviour is not defined as an offence or error in reality, it may cost a company a tremendous amount of money: Websense Inc. reported that approximately 15 million employees are able to use the Internet at work in Japan, and their average monthly income is 355,000 yen (equivalent to £2,088 [176]). Considering those conditions, the Japanese loss of productivity reached 1.77 trillion yen (equivalent to £10.41 billion[177]). It has been proven that employee Internet abuse is taken seriously in some companies[178].

Considering financial service businesses in particular, computers and networks are utilised in all of their phases. It is critical for financial institutions to acknowledge all types of cyber risk to fulfil the sound management of businesses. Hence, this thesis attempts to address all cyber risks within financial service businesses. Towards the accomplishment of this purpose, other indigenous risks in financial service businesses, such as trading risk, market risk and the like, will be exempted from this thesis.

The first step has been taken towards avoiding cyber risk: financial institutions' vigilant awareness. However, there are some other steps which must be taken before moving to the actual risk management methods. Mere awareness of cyber risk differs from acknowledging what types of potential cyber risk exists in one's own company. Then, the next step is to grasp clearly what protection is necessary. Otherwise, it is impossible to either assume the potential extent of damage or choose the appropriate countermeasures. Indeed, it is essential to determine all cyber risks within all the business processes as well as within the entire company. Nevertheless, there are also risks in this course of action, such as:

A risk of
* receiving inconsistent quality of information;
* information being interrupted or intercepted;
* failing to take notice of information, and;
* information unable to be analysed.

---

[175] Operational risk will be discussed in Chapter VI.
[176] The exchange rate: £1 equivalent to approximately 170 yen.
[177] According to the survey conducted in 2000, an average 96 minutes per week per head was spent for browsing websites, which were irrelevant to one's business. See '18 September 2002, Websense Japan Inc.', <http://www.websense.com/company/news/pr/02/japan/091802.cfm> (print out on file with author).
[178] The Xerox's case, see Introduction.

To avoid these risks, it is critical to implement the transparent information superhighway. For example, while a particular piece of information is not important at a department, but it will be useful for others. Establishing a centralised information database will be helpful for knowledge management.

The final step is to choose the appropriate types of risk management methods. Traditionally, the responses to risks are divided into six categories: avoidance, prevention, protection, distribution, transfer and retention.

* Avoidance — not to involve any factor (activity, project, human resources) which associates with a risk in businesses;
* Prevention — to reduce or decrease the size of potential loss or its frequency;
* Mitigation[179] — to remove or minimise the impact of the incident being Mitigation realised;
* Distribution — to minimise the size of potential loss by distributing the risk burden;
* Transfer — to shift the risk burden to another party, and;
* Retention — to possess the risk burden[180].

In general, the first four responses work to control risks and the last two responses finance risks at one's own expense. A decision depends upon how each company combines the said responses. Indeed, the countermeasures against cyber risk that will be examined in the following chapters fall in one of those categories.

[179] It also appears to be identified as "Protection".
[180] See 'Risk Management Strategies', <http://www.c-risk.com/Construction_Risk/RM_Strategies_01.htm>. '*Dai 4 suteppu risuku syori* (The 4th step: risk disposal)', <http://www.hyuga.or.jp/hoken/rskmng/r14.html> (print out on file with author).

Chapter III: An Analysis of the Scope of Criminal Law

1. International harmonization

The international harmonisation movement to combat computer crime was initiated by the OECD. The OECD began their research in 1983, and published a report "Computer-Related Crime: Analysis of Legal Policy" in 1986. Following the OECD, the Council of Europe started discussions about the legal problems of computer crime in 1985, and published "Recommendation N° R (89) 9" in 1989 and Recommendation N° R (95) 13", concerning problems of criminal procedural law connected with Information Technology. Subsequently, the United Nations (hereinafter "UN"), at the thirteenth plenary meeting of the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders, adopted a Resolution to combat computer crime in 1990.

According to the Council of Europe, there are three approaches towards the international control of computer crime:

(1) Stipulating what acts constitute offences by amendments and supplements to substantive criminal law;
(2) Effective prosecution, *inter alia*, by possibly, adapting domestic criminal procedural law;
(3) Improving international collaboration[181].

These approaches appear very basic. The first and the second relate to the domestic dimension of computer crime, and the third, the international dimension. In its contract, the Eighth UN Congress adopted a more precise outlook[182]:

(1) Modernisation of national criminal laws and procedures, including measures to ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes;

(2) In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity;

(3) Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes;

(4) Improvement of computer security and prevention measures, taking into account the problems related to the protection of privacy, the respect for human rights and fundamental freedoms and any regulatory mechanisms pertaining to computer usage;

---

[181] J. Backhouse & G. Dhillon, *supra* n.123, at 647-648.
[182] See '8th United Nations Congress Resolution on computer-related crimes', <http://www.io.com/~asrcs/un.html> (print out on file with author).

(5) Adoption of measures to sensitise the public, the judiciary and law enforcement agencies to the problem and the importance of preventing computer-related crimes;

(6) Adoption of adequate training measures for judges, officials and agencies responsible for the prevention, investigation, prosecution and adjudication of economic and computer-related crimes;

(7) Elaboration, in collaboration with interested organisations, of rules of ethics in the use of computers and the teaching of these rules as part of the curriculum and training in informatics;

(8) Adoption of policies for the victims of computer-related crimes which are consistent with the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, including the restitution of illegally obtained assets, and measures to encourage victims to report such crimes to the appropriate authorities.

Its eight measures are similar to Parker's eight advantages of having a law specifically for computer crime[183], because both provide suggestions

---

[183] Parker explained eight advantages of having a law as:
Introducing new legislation combating computer crime
(1) makes people recognise such an abuse or offence is seriously harmful against a community, government or an individual, socially and ethically. The fact that potential losses are likely to be huge, is substantially noteworthy when focusing on combating computer crime;
(2) encourages companies to regulate company self-governance policy, and inform employees as to what activity is legal or illegal, and thus be effective to deter employees from committing computer crime;
(3) should restrain anyone who is in a confidentially high position or has high technology, from committing computer crime;
(4) makes a prosecution easy, so that the period of a criminal suit and the amount in controversy should reduce dramatically;
(5) can work effectively on criminal proceedings;
(6) The people involved in a suit need not divert to other types of laws combating computer crime, so they can convict directly;
(7) It is possible to correct any kind of precise statistics of computer crime. Those statistics will be effective in knowing the reality of computer crime and its characteristics; and
(8) Introducing new federal legislation combating computer works effectively to get rid of differences among states.
These advantages can be expected when new legislation on combating computer crime is introduced. The first three advantages are not directly related to legislation itself: the first aims at attracting people's attention, the second stimulates self-governance. They do not have an active effect on legislation, thus they would seem solely to be passive advantages. Only the third aims at restraining a person committing computer crime, thus is likely to be an advantage which develops outside the legislative process. The fourth to sixth aims consider three advantages of how legislation effectively deals with computer crime. In particular, the fourth is an essential advantage for the judicial circle, mainly for prosecutors. This is because it is said that it normally takes 65 days to prosecute an ordinary white-collar criminal: it is possible to prosecute a murder, two rapists, and three robberies within the same period. (See 'Prosecutors, Police and Judges', <http://www.edu.tuis.ac.jp/~b97049/climinal2.html> (print out on file with author).)

for combating the problem. However, the third and the eighth measures stated below, are not included in the advantages Parker suggested. The third and eighth aim at providing a type of relief measure for victims of computer crime. It is very important to consider legislation, not only for criminals, but also for victims. Regarding the sixth, as Bender also mentioned, providing computer-training opportunities seems to be becoming more of a necessity for anyone in the judicial circle[184]. The Council of Europe also suggested, at the very least, a minimum list and an optional list of offences to make an effective and a unified criminal policy on legislation is necessary[185]. This suggestion seems to be a very effective one. This is because all member countries will share the same basis on a national legislation as a result of adopting the suggestion.

As Kaspersen stated, national legislation is likely to have a role in both encouraging the harmonising of countries toward an international recognition of computer crime, and in stimulating the adoption of international conventions to tackle such crime[186]. But some questions should be raised:

(1) The adequacy of police powers performing criminal investigations in automated data processing devices for both computer crime and computer-related crime (a traditional crime committed by the use of computer technology);

(2) The jurisdiction for national police authorities executing investigations outside the national territory using these networks to access to data files (not physically present in the home country), and the necessity of new international conventions and regulations in the field of procedural criminal law; and,

(3) The necessity of an international harmonisation of those powers to prevent failure of international co-operation if police powers are not equally levelled[187].

As has already been mentioned, the Council of Europe has been addressing computer crime since the 1980's. The committee of experts on crime in cyberspace (PC-CY) began to work on a draft convention on cyber-crime in 1997, and then made the final Convention on Cybercrime in public in 2001. It was adopted by the Committee of Ministers of the

---

The seventh can provide empirical support for this aim. Only the last point is mainly for the USA, not in general. See Parker (1984), *supra* n.*42*, at 323.

[184] Bender mentioned that a panel of the Association for Computing Machinery recommended providing educational opportunities for new users to deal with criminal activity in 1985. See D. Bender, 'Computer law vol.4' (1997) Matthew Bender, New York at 4B-122.

[185] See European Committee on Crime Problems, Council of Europe (1990), *supra* n.112, at 33.

[186] Kaspersen, *supra* n.64, at 44.

[187] *Ibid.*

Council of Europe at its 109th Session on 8 November 2001 and was signed by its member countries as well as four non-member States: Canada, Japan, South Africa and the United States of America[188]. The said committee has worked actively. Its work consists of four chapters; terminology is explained first, harmonisation of the national procedural law second, international mutual assistance third, then final provisions in the end. Under the Convention there are four offence categories:

(1) Offences against the confidentiality, integrity and availability of computer data and systems, which includes illegal access, illegal interception, data interference, system interference and misuse of devices (Articles 2 to 6);

(2) Computer-related offences, which include computer-related forgery, and computer-related fraud (Articles 7 to 8);

(3) Content-related offences, meaning offences related to child pornography (Article 9); and

(4) Offences related to infringements of copyright and related rights (Article 10).

Any attempt in aiding or abetting of those offences aforementioned is also a crime under Article 11. The essential aim of concluding this convention is to let member countries implement a standardised national law combating cybercrime[189]. Any past guidelines or legal analyses carried out by any international organisation has lacked strong obligation. However, this Convention obliges a ratified country to implement counter measures against cybercrime[190]. In fact, those obligations require many changes mainly to an existing law, regulation or system of the ratified countries. Moreover, it is rigid and covers more than the majority of national law; no country would be able to ratify the Convention without legal change to a greater or lesser extent. However, the Convention promises a great deal, once its terms are agreed upon. Any offence which is described in the Convention, is criminalized on a national level at first (in its chapter II). Then it promises international mutual assistance if it is a transnational cybercrime based on the territorial jurisdiction (in its chapter III)[191]. However, it does not mean that an offender can be

---

[188] See 'Convention on Cybercrime (ETS no. 185): Explanatory Report', <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm> (print out on file with author).

[189] Not only the member countries of Council of Europe but also the United States, Canada, Japan and South Africa are involved in the drafting process. See 'Draft Convention on Cybercrime', <http://conventions.coe.int/treaty/EN/cadreprojets.htm> and 'Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime', <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41en.htm> (print out on file with author).

[190] This obligation is nevertheless no legal force in view of lack of an execute organ in case a member country does not accomplish as it describes.

[191] Article 22 of section 3 (Jurisdiction) urges appropriate legal counter measures

extradited amongst any ratified countries of the Convention; all ratified countries do not agree on the same reciprocal extradition treaty, such as the European Convention on Extradition. It is of importance to recognise the dual criminality held upon extraditing an offender from one to the other, as well as the treaty between two countries. If no mutual assistance treaty or arrangement exists between the two countries concerned, it is still possible to request mutual assistance by applying to the Convention itself under Article 27[192]. In case of a dispute amongst ratified countries, it suggests referring to the European Committee on Crime Problems (CDPC) or the International Court of Justice.

There are problematic issues in this Convention. Firstly, this convention would be ratified by a small number of countries. Most of them are developed countries; while cybercrime is not a specific problem for them, they are very likely to be target countries of cybercrime. Cybercrime is technically an offence anybody can commit from anywhere in the world with a networked computer. It is not exclusively an urban type offence. In fact, the "Love Bug Virus", which was called "the most destructive cyberspace attack yet" in early 2000, causing billions of dollars in damage, originated from the Philippines[193]. Therefore, this Convention is more likely to cover only the tip of the iceberg. Secondly it requires preserving, disclosing and accessing computer data and traffic data, collecting traffic data in real-time, intercepting communications and so on — a series of operations (themselves a heavy financial burden) which cannot be done without the assistance of the industries concerned[194]. Thirdly, it is an issue relating to privacy and human rights. In relation to the second issue, some requirements under the Convention may be in danger of infringement of privacy. The Convention, however, clearly expressed in its Preamble:

> "...Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and

---

against any offence described between articles 2 to eleven of the Convention being committed within a party's territory, on board a ship flying its flag, or by one of its nationals if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. See 'Draft Convention on Cybercrime', *supra* n.180.

[192] Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements. *Ibid.*

[193] See 'Waiting for 'Love' Suspect', <http://abcnews.go.com/sections/tech/DailyNews/virus_000508.html> and 'Love Bug probe widened at BBC News Online: Sci/Tech', <http://news.bbc.co.uk/1/low/sci/tech/749664.stm> (print out on file with author).

[194] See 'Opinion 4/2001 on the Council of Europe's Draft Convention', *supra* n.180.

impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy[195]..."

Although it does not intend to infringe upon human rights, it surely provides the potential for infringement. In fact, some online privacy support groups made a protest against the Council of Europe[196]. It is a critical issue. On the one hand, one could argue that the Convention on Cybercrime is minute and well made. On the other, it contains some critical problems, which must be resolved before the draft is ratified.

The efforts by major industrialised democracies (and others) to combat cybercrime are continuous. The first initiative was sketched in the Lyon Summit in June 1996. In the Lyon Summit, the importance of global cooperation to tackle international organised crime was emphasised, and 40 recommendations to combat transnational organised crime were adopted[197]. In regard to the following Denver Summit of the Heads of State of Government of the eight major industrialised democracies (hereinafter "G8") in 1997, the Communiqué clearly declared the importance of intensifying the cooperation on combating computer-related crime and high-tech crime in paragraph 40[198]. In Birmingham in May 1998

---

[195] 'Draft Convention on Cybercrime', *supra* n.180.

[196] '*Ohsyû online hanzai jouyaku ni soshikiteki-na-kougikoudou* (An organisational protest against the draft European Convention on Cybercrime)', <http://www.zdnet.co.jp/e-businenn_topb4f5b96f> (print out on file with author).

[197] See '*P-8 Kokusai-soshiki-hanzai jôkyû senmonka kaigou no 40 kankoku* (P-8 Forty recommendations against international organised crime prepared by the Senior Specialists Meeting)', <http://www.mofa.go.jp/mofaj/gaiko/summit/birmin98/bun_40.html> (print out on file with author).

[198] Since the Lyon Summit of the Seven in 1996, importance has been placed on issues on market globalisation and international organised crime. In regard to the Denver Summit of the Eight in 1997, the Communiqué declared 'we must intensify our efforts to implement the Lyon recommendations. In the coming year we will focus on two areas of critical concern: First, the investigation, prosecution, and punishment of high-tech criminals, such as those tampering with computer and telecommunications technology, across national borders. Second, a system to provide all governments the technical and legal capabilities to respond to high-tech crimes, regardless of where the criminals may be located.' See 'Communiqué: The Denver Summit of the Eight', <http://www.state.gov/www/issues/economic/summit/communique97.html> (print out on file with author). To reach this target, combating international organised crime, including high-tech crimes, was chosen as one of main issues at the Birmingham Summit of Eight in 1998: 'We agree to implement rapidly the ten principles and ten point action plan agreed by our Ministers on high tech crime. We call for close cooperation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic data as evidence, while maintaining appropriate privacy protection, and agreements on sharing evidence of those crimes with international partners. This will help us combat a wide range of crime, including abuse of the Internet and other new technologies'. See 'THE BIRMINGHAM SUMMIT: FINAL COMMUNIQUE - Sunday 17 May 1998', <http://birmingham.g8summit.gov.uk/docs/final.shtml> (print out on file with author). It is no exaggeration to say that this Summit was a milestone in exposing these issues to the limelight. In addition, the participants for these three Summits were, basically, Presidents, Prime Ministers and Chancellor from Canada, France, Germany, Italy, Japan, UK and USA, and President of European Commission. Russian President has joined the Summit at Denver. See 'G7 Lyon Summit Information',

the G8 Heads and the President of the European Commission held a summit and agreed on combating high-tech crime[199]. They recognised a dramatic increase in transnational crime caused by globalisation, and the necessity of international co-operation in combating this menace. The initiative since Lyon has aimed mainly at money laundering and transnational crime, such as terrorism, narcotics; issues on computer-related crime or high-tech crime were a related issue rather than an exact target. However cybercrime has become one of the central issues of transnational crime since 1997. The G8 Heads approved the ten principles and a ten-point action plan on high tech crime[200], to be implemented rapidly, was agreed upon: through co-operation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic data as evidence, while maintaining appropriate privacy protection. Furthermore, it would appear significant that they mentioned combating abuse of the Internet and other technologies. They recognised that the consequence of crime, generally using high technology, is nationally harmful enough to be combated under their leadership. In their declaration, they mentioned the fear of Internet crime, which might be committed in the near future, and pose a major threat. By this time, many countries had already prepared to combat computer crime, including unauthorized computer access[201]. The ministerial Conference of the G-8 Countries was held in Moscow in October 1999 after being welcomed by the Koln Summit. It specialised in issues of combating transnational organised crime, and its Communiqué expressed the importance of combating high-tech crime[202]. The Communiqués of both the Okinawa Summit in 2000[203] and the Genoa Summit in 2001[204] reaffirmed the

---

<http://www.mofa.go.jp/mofaj/gaiko/economy/summit/lyon/index.html> (print out on file with author).

[199] See 'The Birmingham Summit: Final Communiqué - Sunday 17 May 1998', *ibid.*

[200] It was agreed in Washington in December 1997 then approved by G8 countries in Birmingham in 1998. See 'Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, (Moscow, October 19-20, 1999), COMMUNIQUE', <http://www.moj.go.jp/PRESS/991020-1-1.html> (print out on file with author).

[201] See '*Dai-ni-syô Angou seisaku ni kanrensuru sonota no jouhou sekyurityi shisaku* (Chapter II Another security policy in relation to cryptography)', <http://www.npa.go.jp/hightech/secv_repo/2-2.htm> (print out on file with author).

[202] The Communiqué contained a specific section in regard to high-tech crime. It emphasized that there be no haven in the world for such criminals. To accomplish this aim it is necessary to intensify some points:

Clause 16. Strengthen legal systems;
Clause 17. Cooperation on transnational access to stored computer data;
Clause 18. Ability for locating and identifying high-tech criminals;
Clause 19. International network of 24-hour contacts;
Clause 22. Assistance from Industries.
(The numbers shown refer to paragraphs in the Communiqué.)

As the Communiqué mentioned, it is indispensable for law enforcement authorities to have appropriate technical ability as well as a sufficient legal framework to deal with such a crime. See 'Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, (Moscow, October 19-20, 1999), COMMUNIQUE', *supra* n.191.

[203] The Okinawa Communiqué

Clause 44. We must take a concerted approach to high-tech crime, such as cyber-crime, which could seriously threaten security and confidence in the global

importance of combating cybercrime as well as international organised crime.

2. Legislative approaches in the world

An action called a "crime" or an "offence" is a breach of others' freedom and/or profit. Although, criminalisation of an action usually demands three fundamental elements: a fact, substantial evidence of harm being done to others, and rationally visible losses[205]. Without these, it is impossible to judge economic crime as an illegitimate action. Even though an action is possibly recognised as illegal, punishment is not immediate; it takes time to decide on an adequate punishment.

It would appear that there are roughly two types of law to deal with economic interests. One is pro-social welfare and the other is anti-crime. A good example of the former is tax law. This type of economic law has long been an essential implement for government in the area of tax collection. However, antiquated economic laws (pertaining to government tax collection throughout the ages) existed almost for the regime itself. In the case of economic crime the latter type of law is necessary, the examples being criminal law and its related acts. A victim of economic crime can be an individual, or regime. The role of criminal procedure is to control crime, to punish a criminal and to keep public order through a disclosure, an apprehension, an investigation, a prosecution and so on[206]. These are also effective in keeping social justice in general.

However nothing is available for regulating or prosecuting a crime when it is committed for the first time in countries which implement

---

information society. Our approach is set out in the Okinawa Charter on Global Information Society. Taking this forward, we will promote dialogue with industry, including at the joint Berlin meeting in October. We welcome the results and the momentum created by the Government/Industry Dialogue on Safety and Confidence in Cyberspace in Paris, and look forward to the second High-level Meeting on High-tech Crime with industry to be held in Japan.

Information and Communications Technology (IT) was the key factor in the Okinawa Summit. Although the said paragraph declared to fight against high-tech crime, it appeared to place importance rather on developing IT technology (paragraph 10-12) See 'G8 COMMUNIQUÉ OKINAWA 2000', <http://www.g7.utoronto.ca/g7/summit/2000okinawa/finalcom.htm>. (print out on file with author).

[204] The Genoa Communiqué

Clause 33.We reaffirm our commitment to combat transnational organised crime. To this end, we strongly endorse the outcome of the G8 Justice and Interior Ministers Conference held in Milano this year. We encourage further progress in the field of judicial co-operation and law enforcement, and in fighting corruption, cyber-crime, online child pornography, as well as trafficking in human beings.

See 'COMMUNIQUÉ', <http://www.g8italia.it/_en/docs/XGKPT170.htm>. (print out on file with author).

[205] See R. Matsufuji, '*Secrets of a Super Hacker: Anata no computer mo nerawareteiru* (The Nightmare. Secrets of a Super Hacker)' (1995) Noritsu Management Centre, Tokyo, at 326.

[206] See Y. Nakanome, '*Keiji Sosyô Hoû no kaisetsu* (An commentary to Japanese Criminal Procedure Code)' (1997) Hitotsubashi Syuppan, Tokyo, at 1-3.

statutory law[207]. To be precise, if the principle of legality of crime and punishment[208] is expressed in the law, and in a constitution, it is hardly possible to indict a person for any crime that has not yet been criminalized. There are clearly two legislative approaches to deal with the situation: introducing new legislation or modifying existing legislation. Both approaches have advantages and disadvantages. The advantages for introducing new legislation are that, firstly it is a simple and intensive countermeasure only for certain crimes. Secondly it has more impact upon the general public than in modifying an existing legislation. However, new legislation is not always introduced promptly. On the other hand, modifying existing legislation takes less time but is without the said advantages of introducing brand-new legislation. Taking the time element point into consideration, introducing new legislation is likely to cost more than modifying existing legislation. Therefore it is difficult to decide which approach is better. It is important for a legislative body to judge which approach is suitable by conducting ample surveillance in advance. It is not always suitable to introduce new legislation — modifying legislation is sometimes more appropriate. One of the decisive factors in choosing either legislative approach is the urgency of a countermeasure's necessity toward combating a brand-new crime. If the crime has a transnational aspect, external pressure from abroad can expedite a smooth action against that crime no matter which legislative approach is taken. To a greater or lesser extent individual laws are linked legislatively through the nucleus of the constitution at the centre. Criminal law or any other specific act combating a certain crime refers to the constitution and no law can be beyond that, or be inconsistent or contradictory.

In regard to legislative approach against cybercrime, no law was expected to combat any one type. Cybercrime involves both traditional

---

[207] Law has two systems; common law and statutory law. Common law is unwritten, mainly based on judicial precedents and particular custom whereas statutory law is written, established by a legislature. The former system is, for instance, applied to England and Wales and in the United States at state level. The latter system is applied to Japan and European countries. However, it does not mean that a country unifies its law into either system entirely. Both systems of law are generally seen in a country. For instance, the Japanese constitution is statutory law but commercial law includes particular custom. There is no statutory constitution in the UK although other types of statutory law exist, such as Computer Misuse Act of 1990 or English Copyright Law (1709). See '*Keihou-souron 1. Resume No.7* (An introduction to Criminal Law *1. Resume No.7*)', <http://www.h2.dion.ne.jp/~tabu/01lec-cg1-e-7.htm> and '*Hougaku Dai-ichi-bu* (Jurisprudence Part 1)', <http://www5a.biglobe.ne.jp/~kaisunao/ho-kogi/05hogen.htm> (print out on file with author).

[208] The principle of legality of crimes and punishment is widely believed to be one of the aspects of "due process of law". It prohibits an administrative agency from prosecuting or punishing a person who commits a crime unless it has been criminalized in law and its corresponding punishment is also clearly described. It refers to human rights. See '*Daini Tokyo Bar Association, Q28 Du purosesu toha nandesuka?* (Daini Tokyo Bar Association, Q28 What is 'due process'?)', <http://www.dntba.ab.psiweb.com/qna/qna28.htm> and '*Keihou Souron Kougi Nouto* (Criminal Law lecture Note)', <http://web11.freecom.ne.jp/~aimon/kei/kei_n1.html> (print out on file with author).

types of crime, such as fraud and forgery, and brand-new types of crime, such as a computer virus and hacking. Even though computer fraud could be roughly categorised as a traditional fraud, it would be difficult to penalise it by an existing law. Not only because the principle of legality of crimes and punishment does not allow penalising it, but also that the use of a computer and/or the network differs from a traditional fraud on many levels. In regard to Parker's eight advantages, with them all as a basis, an attempt will be made to extend the observation into the legislative approach. Kaspersen showed how computer crime could be approached legislatively. He categorised two ways to distinguish a legislative an attempt will be made to extend the observation into the legislative approach. Kaspersen showed how computer crime approach: "crime-category-based" and "legislative amendment technique based". A "crime-category-based" approach is the method based on criminality, which has four approaches[209]:

(1) Property Approach
It defines computer data and software as property. Computer crime statues in many US states have adopted this approach;

(2) Forgery Approach
It focuses on the integrity of computer data. The UK adopted this approach in the Forgery and Counterfeiting Act 1981;

(3) Information Approach
This approach is based on the legal protection of privacy. This was adopted by Federal legislation in the USA, in Europe, in the Nordic countries, especially Norway and Finland; and

(4) Mixed Approach
It is possible to mix two or more of the approaches above. The mixed approach is sometimes effective to combat computer crime, due to its increased aspects.

On the contrary, the "legislative amendment technique based" approach is a completely different idea from the "crime-category-based" approach. Some countries recognise that existing provisions can be made applicable to computer crime. This approach can be categorised into four types[210]:

(1) Supplementation
This technique is the way to amend some countries' provisions to suit a real situation. The UK has adopted this approach;

(2) Extension
To focus on analogy of existing provisions, wherein the criminal code is

[209] Kaspersen, *supra* n.64, at 48.
[210] *Ibid.*

enlarged by enacting new provisions. Most countries use this technique;

(3) One-for-all
One main provision is used with a special subdivision of the criminal code or a special statute;

(4) Mixed;
A combination of the above three techniques can be effective.

The list below is a comparison among fourteen countries of how they approach combating computer crime. Unfortunately, only half of these countries had enforced the legislation by 1987. (Table 2.1)

Table 2.1: Legislative Approach

Country	Approach	Technique	in Force
USA(Federal)	I	O	Y
USA(States)	P	S	Y
Austria	P	E	N
Belgium	M	O	N
Canada	M	E	Y
Denmark	I	E	Y
Finland	I	E	N
France	M	O	N
Netherlands	M	M	N
Norway	I	E	N
Sweden	M	M	Y
Switzerland	P	E	N
UK	F	O	Y
W-Germany	M	M	Y

(Reference: Kaspersen as of October, 1987 [211])

P: property approach F: forgery approach
I : Information approach M: mixed approach
E: extension technique O: one-for all technique

Eight European countries, Austria, Denmark, France, Germany, Greece, Liechtenstein, Norway and Sweden, amended their existing legislation extensively by 1990[212]. Four European countries: Portugal, Switzerland, Spain, the UK, introduced legislation, with Italy remaining yet follow suit. Other countries, such as Australia, Canada, Japan and the USA have also introduced new statutes. The problem when comparing

[211] The data is offered by Kaspersen (1989), *supra* n.64, at 44.
[212] J. Backhouse & G. Dhillon, *supra* n.123.

and extracting an international consensus is that all countries should (or might) have a focal point: for example, computer systems, and software piracy. Therefore, it is very difficult to establish a unified consensus[213].

An attempt to extend the range of comparison of penalties has been suggested. It is worth mentioning how Australian law works in combating computer crime, especially from the viewpoint of the penalty. This is because some countries, for instance Japan, have been attempting to sophisticate legislation in terms of cyberspace and, as each state in the USA has its own penalty, it makes the issue too complex to focus on. Below is an extract from a report of the Attorney-General's Department in Australia.

> "A person who:
> (1) with intent to defraud any person, obtains, without authority and by means of a facility operated or provided by the Commonwealth, by the Australian Telecommunications Commission [(hereinafter "ATC")] or by another public authority under the Commonwealth, access to data stored in a computer (not being a Commonwealth computer); or
> (2) without authority, intentionally obtains, by means of such a facility, access to data stored in such a computer, being data that the person knows or ought reasonably to know relates to:
> (i) the security, defence or international relations of Australia;
> (ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;
> (iii) the enforcement of a law of the Commonwealth or of a State or Territory or the protection of public safety;
> (iv) the personal affairs of any person;
> (v) trade secrets;
> (vi) records of a financial institution; or
> (vii) commercial information the disclosure of which could cause advantage or disadvantage to any person;
> is guilty of an offence. Penalty is $12,000 or imprisonment for 2 years, or both."

To damage information on a computer carries a far stricter penalty than the above offences:

> "A person who, intentionally or without authority or lawful excuse, by means of a facility operated or provided by the Commonwealth, by the [ATC] or by another public authority under the Commonwealth:
> (a) destroys, erases or alters data stored in, or inserts data into, a computer (not being a Commonwealth computer); or
> (b) interferes with, or interruptions or obstructs the lawful use of, such a computer;

[213] OECD (1986), *supra* n.47, at 7-8.

is guilty of an offence. The penalty is $48,000 or imprisonment for 10 years, or both[214]."

Although these penalties seems to be sufficiently stringent to deter criminals, there were 123 cases of computer abuse between 1975 to 1980 (reported to the police only), and those losses were about $5.6 billion[215]. Based on Table 2.2, in comparison with the USA, Australia has only one penalty more severe (Intent to damage).

Table 2.2: Computer Crimes and Maximum Penalties[216]

Country	Pure Trespass	Intent to Damage	Intent to Defraud	Computer Stalking
Australia	6 months	10 years	2 years	1 year
Canada	not a crime	10 years	10 years	**
Finland	1 year	1 year	2 years	**
Germany	not a crime	2 years	**	**
Japan	not a crime	5 years	10 years	**
Netherlands	6 months	4 years	4 years	**
Sweden	2 years	2 years	2 years	**
UK	6 months	6 months	**	**
USA	1 year	5 years	5 years	2 years, 5 years, 20 years

(Reference: Harvard Journal on Legislation[217])

A comparison of legislation in two countries (JAPAN and the UK) will now be discussed to gain a deeper understanding of the existing legislation relating to cybercrime in a narrower sense than computer crime.

3. Japan

Japan fundamentally adopts statutory legislation [218]. The greatest authority is the constitution and no other law can interfere with it. It is broadly recognised that the principle of legality of crimes and punishment is made in an interpretation in article 31 of the constitution[219]. It secures

[214] Attorney General's Department, 'Review of Commonwealth Criminal Law: Interim Report on Computer Crime' (1988) Australia Government Publishing Service, Canberra, at 69-70.
[215] *Ibid.*
[216] Heymann, *supra* n.152, at 370.
[217] Harvard Journal on Legislation, *supra* n.152.
[218] Historically Japanese law and jurisprudence had been influenced by the continental European countries, mainly Germany.
[219] The article 31 of the Constitution of Japan.
Article 31 [*Seitou tetsuduki no hosyo* (Secured fair legal proceedings)]
No person shall be deprived of life or liberty, nor shall any other criminal penalty be imposed, except according to procedure established by law.
See T. Kobayashi, '*Kenpô* (the Constitution)' (1989) Nihon Hyouron, Tokyo, at 111 and 259-260, and also 'The Constitution of Japan',

fair legal proceedings and prohibits an application of analogical interference in the law, such as stretch of the law.

The Japanese had very few cases of computer crime to address until 1990's. There were only 30 cases between 1971 and 1982; 22 of these were unauthorized access of data. Cash dispenser crimes [220] had increased from 64 in 1977 to 472 in 1982[221]. It increased by about 14 percent in five years, and the majority of computer-related crime cases were cash dispenser crimes. Hence, computer crime did not become the centre of public attention. In 1986, the OECD published its report on computer-related crime [222], and it recommended member countries particularly to seriously address such crime. Keeping pace with the OECD member countries, the Japanese Government came to the decision to amend existing provisions in Criminal Law to combat computer-related crime in 1987[223]. There were four amendments:

(1) Illegal use of electromagnetic records (Article 161, 2);
(2) Interference with a duty by destroying a computer and the like (Article 234, 2);
(3) Computer-related fraud (Article 246, 2); and
(4) Damage on a private and public document (Articles 258 and 259)[224].

They were mainly categorised into two examples: fraud by computer manipulation and computer sabotage[225]. Then the provisions, specifically relevant to combating computer crime, were revised again in 1992 [226].

<http://list.room.ne.jp/~lawtext/1946C-English.html> (print out on file with author).

[220] It is a crime using others' ATM card to withdraw money and deposits it in a doer's bank account. See '*Wagakuni niokeru jûyou-infura bouei notameno houseibi no mondaiten memo* (The issues on introducing law for protecting important infrastructure in Japan)', <http://www1.sphere.ne.jp/netlaw/sec/cipj.htm> (print out on file with author).

[221] OECD (1986), *supra* n.47, at 10.

[222] *Ibid.*

[223] '*Dai-ni-syô Angou seisaku ni kanrensuru sonota no jouhou sekyurityi shisaku* (Chapter II Another security policy in relation to cryptography)', *supra* n.192.

[224] See '*Keihoû* (Criminal law)', <http://www.lec-jp.com/law/houritsu/k_33.html> and '*Keihoû, Syouwa 62nen-kaisei no fusei-akusesu kanrenbubun wo bassui* (Criminal law, the relevant articles to unauthorized access amended in 1987)', <http://www.ipa.go.jp/security/ciadr/law1987.html> (print out on file with author).

[225] ILC-Internet Lawyers Committee, *supra* n.38, at 92-94. 'Computer sabotage is defined by the Audit Commission as 'interfering with the computer process by causing deliberate damage to the processing cycle or to equipment.' See Audit Commission for Local Authorities in England and Wales, *supra* n.66.

[226] The article 161, 234, 246, 258 and 259 of Criminal Law of Japan.

Article 161 [*Gizou sibunsyo nado koushi* (Forgery of a private document)]
Article 161, 2 [*Denjiteki-kiroku fuseisakusyuku oyobi kyôyoû* (Illegal use of Electromagnetic records)]
A person who illegally draws up an electromagnetic record to misguide one's right, obligation or identification for a purpose of mishandling a business shall be punished with penal servitude for not more than five years or a fine of not more than 500,000 yen.

Clause 2

Under the current criminal law, traditional type of crimes, such as fraud, forgery and their related crimes, which cause any damage, are punishable[227]. This is simply because revised provisions were made up from specific words into the two existing provisions; "an electromagnetic record" and "a computer". It is possible to say that the concept of criminal law had not been changed. The 1987 revision took notice of tools being used to commit a crime. It did not pay much attention to targets of a crime. Thus crimes with damage, such as, "computer-related forgery", "computer-related fraud", and "manipulation by computer", are technically able to incriminate the perpetrators. On the other hand, crime with no damage, such as "unauthorized computer access", "computer espionage" or

---

A person who has infringed the provision of clause 2 is an official or the misguided electromagnetic record regards to any public business shall be punished with penal servitude for not more than ten years or a fine of not more than a million yen.

Clause 3
A person who employs an electromagnetic record which has been illegally drawn up for misguiding one's right, obligation or identification for the purpose being prescribed in clause 1 shall be punished the same as the person who has drawn up the illegal electromagnetic record.

Clause 4
A person who attempts the provision of clause 2 shall be punished.

Article 234 [*Iryoku gyôumubougai* (Interference with a duty by power)]
Article 234, 2 [*Denshi-keisanki sonkai nado gyoumubougai* (Interference with a duty by destroying a computer and the like)]
A person who deliberately damages a clerical computer or its electromagnetic record, alters an electromagnetic record, inputs false information, imposes improper instructions, or any other means to interfere or disturb others' computers workings shall be punished with penal servitude for not more than five years or a fine of not more than a million yen.

Article 246 [*Sagi* (Fraud)]
Article 246, 2 [*Denshi-keisanki shiyou sagi* (Computer-related fraud)]
In addition to the preceding clause, a person who inputs false information or imposes improper instructions in a clerical computer and draws up a false electromagnetic record in regard to procuring, losing or altering property rights for making profits illegally, or make a person beneficiary shall be punished with penal servitude for not more than ten years.

Article 258 [*Kouyou-bunsyo nado kiki* (Damage on a public document)]
A person who deliberately damages a public document or an electromagnetic record in any public business shall be punished with penal servitude for more than three months and not more than seven years.

Article 259 [*Shibunsyo nado kiki* (Damage on a private document)]
A person who deliberately damages a private document in regard to a right or an obligation shall be punished with penal servitude for not more than five years.

[227] Under relevant articles in Criminal Law of Japan, such as A charge of damaging (article 261) and Larceny (article 235). See '*Fusei-akusesu-taisakuhousei ni kansuru Keisatsuchou-an oyobi Yûseisyou-an heno paburikku komento bosyû henotaiou nitsuite* (The correspondence to the public comment advertisement on Unauthorized Computer Access Bills by the NPA version and the Ministry of Posts and Telecommunications version'), <http://www.jisa.or.jp/activity/opnion/990107-i.html> (print out on file with author). Due to the nature of this thesis, 'any damage' in this context excludes physical damage.

"invasion of privacy", are unable to be criminalised under this law. "Hacking" and "sending computer virus" can go either way depending on whether there was damage as a result of it. There is proof that some issues, for instance a ban on unauthorized computer access or privacy, had been postponed or been exempt from the subject of the amendment in 1987 or 1992. This was because, firstly, combating a cash dispenser crime was the principal target in revising Criminal Law[228]. Secondly, the difference in the information value between computers and on paper was not clearly defined[229]. Since, previously, it was not punishable for a person to steal a paper containing information, new provisions needed to strike a balance. Thirdly, information, obtained by unauthorized computer access, was not always considered valuable, nor any unauthorized computer access illegal where data had not been kept secure[230]. These reasons prompted the legislation council to continue pursuing a penalty against unauthorized computer access and related offences[231]. Although the possibility of hacking being committed or having computer virus problems was not denied, the Japanese government was still more likely to underestimate the risks.

Until the early 1990's, the number of Internet users had increased rapidly, and with cyberspace expanding even faster. Words such as "hacking", "hacker" and "computer virus" became very familiar all over the world due to the increasing rate of incidents. Unlike other participating G8 countries in the 1998 Birmingham Summit, Japan had not made preparations for combating computer crime (including unauthorized computer access to a computer) and had left it to be improved[232]. It was the only one of the G8 countries that had not, at that time, implemented a plan against unauthorized access to computers or networks, although the Japanese government had been under the pressure to rush through a brand-new law.

In fact many public websites in Japan had suffered intensive attacks by hackers in early 2000. The absence of an appropriate law against

---

[228] It was laborious to incriminate a cash dispenser crime as fraud by criminal law whereas it had increased as well as a cash card use was widespread rapidly. See '*Wagakuni niokeru jûyou-infura bouei notameno houseibi no mondaiten memo* (The issues on introducing law for protecting important infrastructure in Japan)', *supra* n.210.

[229] See 'Dai-ni-syô Angou seisaku ni kanrensuru sonota no jouhou sekyurityi shisaku (Chapter II Another security policy in relation to cryptography)', *supra* n.192 and *infra* n.222.

[230] See '*Cyber security no kokusaiteki houritsu mondai* (International Legal Issues on Cyber Security by Ikuo Takahashi)', <http://www.isc.meiji.ac.jp/~sumwel_h/junc/cmp_crime/cmp_crime-1998-4.htm> (print out on file with author).

[231] See '*Fusei-akusesu taisaku-hou no yukue* (The future of Unauthorized Computer Access Law)', <http://members.tripod.co.jp/hatzemi/resume/zemirepo/1999-2kcss/05.htm> (print out on file with author).

[232] See 'Dai-ni-syô Angou seisaku ni kanrensuru sonota no jouhou sekyurityi shisaku (Chapter II Another security policy in relation to cryptography)', *supra* nn.192 and 219.

unauthorized computer access encouraged the hacking. Apart from Criminal Law there is another related legislation: Unfair Competition Prevention Law[233]. Under these laws, it is not totally impossible to hold criminal responsibility against unauthorized access to computers, or hacking. However, there are two inherent weaknesses: the first problem relates to the conditions in application, such as the existence of major damage or disturbance to any business as a result of hacking. A "hacker" is defined in Japan as "a maniac or a genius on computing technology", though it is believed, in general, that a "hacker" is a person who invades without authorisation and damages other people's computer or networks by the hacker's computing knowledge and technologies[234]. However hackers do not always cause damage. They are, sometimes, enthusiasts who just enjoy demonstrating their technological skill by exploring others' computers or networks without causing any damage. If a hacker gets access to one's computer or a network without any intention to cause damage, or if he does not damage anything as a result of his invasion, the condition mentioned above would never be established. The second problem relates to hacking activity itself. It is very difficult to discover whether a computer has been hacked. Furthermore, another possible danger exists as one may not realise one's own computer has been hacked. These two

---

[233] Unfair Competition Prevention Law is, potentially, applicable to prosecute hackers if they make profits from trade secrets, which they get as a result of hacking. However neither there is a case to be prosecuted according to Unfair Competition Prevention Law nor to be claimed damages in Japan at present. See '*Fusei-akusesu boushi-hô ni kansuru chôsa* (Research on Unauthorized Computer Access Law)', <http://www.ipa.go.jp/SECURITY/pub/contents/crack/research/law/Criminal-3.html> (print out on file with author).

[234] In reality there are two terminologies: a 'hacker' and a 'cracker'. Not only NTT (Nippon Telegraph and Telephone Corporation) but also many institutions recognise nowadays that a person who performs wrong activities such as causing damages on others' computers or a network should be called a 'cracker'. It is said that a 'hacker' has higher knowledge and technology than a 'cracker' has. This is why the hackers differentiate themselves from crackers. See '*Pasokon shittaka jiten* (PC dictionary)', <http://www.nttpub.co.jp/paso/index.html> and 'e-words', <http://www.e-words.ne.jp/frame.asp?body=view.asp&word=%83n%83b%83J%81%5B> (print out on file with author). In addition, there are two examples of definition on hacking in the UK. According to Nildram, Internet service provider in the UK, the definition of hacker is 'anyone [attempting] to gain unauthorized access to your machine or network.' See 'Security Online', <http://www.nildram.co.uk/primers/security.shtml> (print out on file with author). On the other hand, the Department of Trade and Industry (hereinafter 'DTI') in the UK shows 'computer hackers are usually self-motivated, and view security as a challenge. Some may hack into computer systems with intent to disclose company information or to disrupt business, for example by spreading computer viruses.... Some hackers work for organisations engaged in industrial or economic espionage....' See 'DTI - Protecting business information - Understanding the risks', <http://www.dti.gov.uk/PROTECT/risks/risks.htm> (print out on file with author). It seems that a private company, Nildram, defines hacking very broadly without mentioning anything about criminal or economic damage. Besides this DTI places much more importance on economic damage than a private sector. But it is obvious that hackers have a peculiar ethics according to a book from Raymond as '...The belief that system-cracking for fun and exploration is ethically OK as long as the cracker commits no theft, vandalism, or breach of confidentiality'. See 'The New Hacker's Dictionary', <http://www.tuxedo.org/~esr/jargon/jargon.html#hacker> (print out on file with author).

difficulties show that there is no particular regulatory framework or sanction against hackers, either in Criminal Law or in Unfair Competition Prevention Law in Japan.

A brand-new law named the "Unauthorized Computer Access Law" (hereinafter "UCAL") was introduced on 13 February 2000[235]. However, it is impossible to prosecute hackers, who attacked Japanese websites before the said law was in force. Even though their activities were known, "no person shall be deprived of life or liberty, nor shall any other criminal penalty be imposed, except according to procedure established by law[236]." The UCAL consists of nine articles[237]: it contains the aim of the law, definitions of relating terminologies, prohibited matters and punishment. It prohibits two main acts: unauthorized computer access itself and the aggravation of it, such as selling an identification code[238]. It entails three constructive policies[239]:

1. It requires the system administrators to take protective measures, if necessary, including upgrading an access control function[240]. (Article 5)
2. In cases of unauthorized computer access being committed, assistance, such as providing relevant materials, advice or guidance, will be given by the district Public Safety Commission on a request basis from the access administrators. (Article 6)
3. The National Public Safety Commission, the Ministers of International Trade and Industry and of Posts and Telecommunications[241] are obliged to publish the incident report on unauthorized computer access at least once a year as well as the R&D situation of the access control

---

[235] The Millennium in Japan was expected to be called, very proudly, the memorial first year for a reliable security. This is because the Japanese government was about to introduce a brand-new law against unauthorized access to computers, and furthermore it also had tackled preparing public countermeasures against hackers. Ironically, the reality seemed to have revealed Japan as 'the hacking haven'. See 'Interactive News', <http://www.mainichi.co.jp/> (print out on file with author).

[236] See The principle of legality of crimes and punishment, *supra* n.199.

[237] See 'Unauthorized Computer Access Law (Law No. 128 of 1999) (provisional translation)', <http://www.npa.go.jp/hightech/fusei_ac2/UCAlaw.html> (print out on file with author).

[238] See '*Fusei-akusesu taisaku-hou no yukue* (The future of Unauthorized Computer Access Law)', *supra* n.221.

[239] See 'Unauthorized Computer Access Law (Law No. 128 of 1999) (provisional translation)', *supra* n.227.

[240] In Unauthorized Computer Access Law, 'the access administrators' is defined as 'a person who administers the operations of a computer which is connected to a telecommunication line, with regard to its use (limited to such use as is conducted through the telecommunication line concerned)', and 'access control function' is as 'a function that is [controlled] by the access administrator [for] a specific use [to a specific computer or the other,] which is connected [...] through a telecommunication line[,] in order to [control the said use of the computer automatically], and that removes all or part of restrictions on [the said use] after confirming [a code inputted into a specific computer as the identification code for that said use]'. *Ibid.*

[241] The restructuring of the central government of Japan had done in 2000. Ministry of International Trade and Industry has changed into Ministry of Economy, Trade and Industry. Ministry of Posts and Telecommunications was incorporated into Ministry of Public Management, Home Affairs, Posts and Telecommunications.

function-related technology. Furthermore, the State is obliged to enlighten and spread knowledge concerning unauthorized computer access. (Article 7)

As has been confirmed, criminal law covers illegal activity with visible, present damage — defamation[242] is also within its confines. The new law has criminalised unauthorized access to a computer: it prohibits unauthorized access itself, and damage. Many cybercrimes involve unauthorized access to a computer. It is the critical condition to constituting a crime which allows most cybercrimes to be penalised successfully. Apparently, these two laws can cover cybercrime being committed against both tangible assets and intangible information. This brand-new law, however, involves some arguments. Firstly, it confines its subject to computers, which have an "access control function". This indicates that any domestic use or a stand-alone[243] computer is exempt. Secondly how to prove a computer is being accessed without authorisation? Furthermore, it is not impossible to destroy evidence of unauthorized access to computers. If evidence is destroyed, it would be very difficult to prosecute a suspect even if the suspect is found. Thirdly, a penalty for aggravating unauthorized access to a computer is simplified[244]. Moreover, cybercriminals, especially hackers or crackers, are most likely to be minors — a factor that can hamper prosecution. Fourthly there is obviously no application to the infringement of privacy or the use of another's computer without permission. The most crucial argument is in regard to where this new law holds up. The fundamental role of law is to protect social benefits, and the majority of legislation consists of preserving them.

Contrary to this trend, the UCAL adds the act of accessing a computer without authority. This approach, that centres upon prohibiting unauthorized access to a computer, seemingly gives flexibility to penalise or prosecute a crime. Any illegal activity being committed as a result of unauthorized access to a computer is largely considered by the UCAL to be (in the first place) a crime even though the final form of the crime is different from computer access without authority. Under this law, the social benefits to be protected involve both tangible assets, for instance computers, and intangible assets, for example information, data or computer software. Judging by the nature of the law and of relevant

---

[242] To discredit someone by putting rumour or false information to a Bulletin Board System (so called 'BBS') is one of the examples. Even if a statement at BBS is utmost true, it can bring discredit upon an opposite. However it is hardly possible to prosecute a case if no intention for defamation is admitted. See '*Tôshbia no after service, homepage no iryoku 700 mankai* (The power of the homepage, seven million hits for the Toshiba After-service problem)', <http://www.acc.ne.jp/~h-kyoko13/kakokizi/tosibamondai.htm> (print out on file with author.

[243] A computer in use without connecting to a network. See website a relevant issue is discussed, '*Fusei-akusesu taisaku-hou no yukue* (The future of Unauthorized Computer Access Law)', *supra* n.221 and *infra* n.235.

[244] *Ibid.*

crimes, it is most likely to deal largely with intangible assets. However, the legal position of intangible assets is left vague due to lack of applicable law or regulation to provide definition[245]. In reality, it is not easy to generalise or judge the value of information. The type of information varies; client lists, company financial information etc. The value of information changes depending on each individual. For instance, an insurance company's client list is very valuable to the proprietor and its rival companies, but not for staff from a coffee shop. Though likely to be inconsistent and unbalanced if an illegal act is punished, the social value benefit (which is damaged or infringed by the act) is uncertain. It would give the same sentence to two different criminals, each of whom has realised different scales of impact as a result of committing a crime.

Information, in this context, has two approaches for classification: one approach is to concentrate on Confidentiality, and the other approach is to focus on Integrity. If the former approach is taken, the Copyright Law or the Unfair Competition Prevention Law is available for reference. Computer software is, for example, protected by the Copyright Law[246]. Under the Unfair Competition Prevention Law, information or data, which is accepted as a "Trade Secret" is protected, although Patent Law is the mainstream method for trade secrets' protection[247]. To date, those are at risk of being spied upon or stolen through computer networks. Although this risk is not yet readily recognised in Japan, it has already been widely acknowledged in the USA: Computer intrusion cases have already been committed. (Table 2.3). However, they are not designed for combating cybercrime. Copyrights Law actually works to criminalise a perpetrator who makes a copy of data or programmes, but not for unauthorized computer access. If there is no proof of the infringement of copyrights or patent (e.g., just peeking at trade secrets and data), it is hardly possible to apply those legislations. For the latter approach, there is no exact, applicable law. This is because "Integrity" is a state of data or information, not even an intangible asset. Still, it is the most critical factor of any information and, although it is more difficult to protect "Integrity" by law, this will be necessary for combating cybercrime.

---

[245] See '*Fusei-akusesu taisakuhoū ni taisuru kihonnteki-kenkai* (A fundamental opinion to Unauthorized Computer Access Law)', <http://www.asahi-net.or.jp/~vr5j-mkn/fuseiakusesu.htm> (print out on file with author) and also '*Fusei-akusesu taisaku-hou no yukue* (The future of Unauthorized Computer Access Law)', *supra* nn.221 and 233.

[246] Under No. 9 clause 1, article 10, the Copyright Act. See '*Jōhō kanren hō Dai 4 kou Computer programme no houtekihogo* (Law related to information, Part 4 Legal protection on Computer Programme)', <http://www.mars.dti.ne.jp/~kos/law/lives/infolaw/info-04.html> (print out on file with author).

[247] Unfair Competition Prevention Law was revised in 1990 and 1993. For reference see '*Jōhō kanren hō Dai 6 kou Eigyō-himitsu no houtekihogo* (Law related to information, Part 6 Legal protection on trade secret)', <http://www.mars.dti.ne.jp/~kos/law/lives/infolaw/info-06.html> (print out on file with author).

Table 2.3: Computer Intrusion cases in the USA

Economic Espionage Act Cases	Violations	Method of Theft	Type of Information Stolen	Punishment	
				Incarceration or Probation in Months	Fine Forfeiture Restitution ($)
U.S. v. Daddona (D. Conn) March 12, 2002	EEA **CI**	Insider	Engineering plans	5 home detention 36 prob.	Fine: 4K Rest: 10K
U.S. v. Rector (M.D. Fla.) January 25, 2002	**EEA CI**	Insider Ex-employee	Drug delivery system formulas	14	
U.S. v. Estrada (S.D.N.Y.) March 21, 2001	EEA **CI** ITSP	Outsider	Confidential documents		
U.S. v. Dai (W.D.N.Y.) August 23, 2001 (sentencing)	**Other**	Ex-employee	Computer source code	24 prob.	50K
U.S. v. Morch (N.D. Cal.) March 21, 2001	**EEA CI**	Ex-employee	Software design documents	36 prob.	
U.S. v. Kern (E.D. Cal.) April 4, 2000 (sentencing)	**EEA CI**	Ex-employee	Radiological machines servicing info	12	

Economic Espionage Act Cases:
Colloquial Case Name (District), Press Release Date or Date of Most Recent Court Activity
Violations:
EEA
The Economic Espionage Act prohibits foreign economic espionage and the theft of trade secrets, 18 U.S.C. §§ 1831-1839.
CI (=Computer Intrusion)
The Computer Fraud and Abuse Act protects the confidentiality, integrity, and availability of electronically stored data, 18 U.S.C. § 1030.
ITSP
Interstate Transportation of Stolen Property, 18 U.S.C. § 2314.
Method of Theft:
Insider, Ex-employee, Competitor or Outsider
(Resource: See "Computer Crime and Intellectual Property Section (CCIPS): Economic Espionage Act (EEA) Cases",
<http://www.usdoj.gov/criminal/cybercrime/eeapub.htm> (print out on file with author).

Eavesdropping on a computer is banned by Telecommunication Business Law[248]. Furthermore, the Ministry of Justice (hereinafter "MoJ") has

[248] There is another law called the wiretapping law, which is one of three law passed by the Diet in August 1999 combating organised crime. That allows law enforcement to intercept telecommunications and so on if a certain offence is concerned. Therefore, its nature is different from a law to ban eavesdropping in this context. See 'New crime measures have cops all ears', <http://www12.mainichi.co.jp/news/mdn/search-news/837080/DoCoMo-0-3.html>

announced the revision or establishment of a new law to regulate producing or distributing computer virus without resulting damage. Any related activity, such as selling, placing an order for, importing tools or materials with the intention of producing a computer virus, including producing a password for illegal purpose are within the scope of MoJ[249]. There is other legislation being amended or newly established in relation to cyberspace, such as the Copyright Act and Law Concerning Electronic Signatures and Certification Services[250]. However, they are mostly irrelevant to crimes being targeted in this thesis, thus rendering unnecessary further discussion on this point.

Apart from a legislative approach combating cybercrime, other efforts have been made. For instance, the Ministry of Economy, Trade and Industry (hereinafter "METI") published guidelines; Computer Virus Prevention Guidelines and Unauthorized Computer Access Countermeasure Guidelines. The former guideline shows the effective preventive controls against computer viruses, and it targets industries concerned, such as system administrators or network service providers. The latter provides avertable measures against unauthorized computer access, and its target includes both companies and individuals[251]. They are guidelines (thus no legal force) although some affiliated organisations concerned with the said Ministry endeavour to influence related industries by providing those guidelines.

4. The United Kingdom

Bill Hughes, the Director General of Britain's National Crime Squad, has stated "Great Britain is the No. 1 target in the western world for computer criminals, but too many British businesses are in denial about the existence of computer crime[252]." There is, unfortunately, no reference to the authority of this statement. Whether or not having a law acts as a deterrent on preliminary computer criminals, the UK has introduced the

---

(print out on file with author). Moreover, the Criminal Law was revised and promulgated in July 2001 to prevent credit card fraud, forgery and related offences. Under the revised Criminal Law possessing a forged credit card or obtaining a credit card details without authority and so on are offences. See *Nihonkeizai Shimbum* dated 1st June 2001, at 5.

[249] See *Nihonkeizai Shimbum* dated 1st April 2001, at 1.

[250] For reference, see 'Links to Laws of Japan, Codes, Statutes, Regulations of Japan',<http://www.isc.meiji.ac.jp/~sumwel_h/links/linkJ04.htm> (print out on file with author).

[251] See 'Computer Virus Prevention Guidelines', <http://www.ipa.go.jp/security/english/virus/virus-guidelin-e.html> and 'Unauthorized Computer Access Countermeasure Guidelines', <http://www.ipa.go.jp/security/english/access-guideline-e.html> (print out on file with author).

[252] See 'Brit Cops Tackle E-Thievery', <http://www.wired.com/news/business/0,1367,43171,00.html> (print out on file with author). The article stamped the date on April 19, 2001.

Computer Misuse Act of 1990 (hereinafter "CMA") in the last decade[253].

Until the said Act came into force in 1990, the UK had combated computer-related crime by means of existing law, such as the Criminal Justice Act 1994 and Criminal Damage Act. While the Parliament[254] became aware of the limit of current existing law to combat computer-related crime in the 1980's, the Scottish Law Commission started an investigation on its own crime problems in 1984, published in the Memorandum in 1986, followed by another report entitled "Report on Computer Crime" in 1987[255]. The Scottish Law Commission categorised eight computer misuses, with each category explained in detail, plus a discussion regarding the possibilities of addressing them through existing law. Furthermore the Commission contemplated both minimal and wider law reforms[256]. In succession to this, the Law Commission (in England and Wales) published "Computer Misuse working paper No.110" in 1988.

---

[253] Prior to the British government, the former West German government revised its Criminal Law and Unfair Competition Prevention Law in 1986 to combat unauthorized access and French introduced a new law called '*la loi Loi No 88-19 du 5 janvier 1988 relative à la fraude informatique* (dite 'Loi Godfrain' (Act No.88-19 dated January 5, 1988 on Computer Fraud (said 'Godfrain Act'))' to control an illegal access to data processing and related matters in 1988. In the USA many an individual state amended their existed Criminal Law and the Federal Law was revised in 1986. Compared to a series of international pace, the British government was said to be relatively unhurried. See '*6-9tuke Jôhô-tsûshin network no anzen/sinraisei ni kansuru kenkyûkai-houkokusyo dai-1-hen dai-2-syô* (A report on a society for safety and confidentiality of information communication network dated June 9th)', <http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/denki/970609j602_3.html > (print out on file with author). For French law, see '*Sécurité Informatique : la loi* ', <http://cri.univ-tlse1.fr/documentations/securite/loi_penetration.html> (print out on file with author).

[254] The United Kingdom of Great Britain and Northern Ireland consists of four countries (England, Wales, Scotland, and Northern Ireland) and three individual jurisdictions (England & Wales, Scotland, and Northern Ireland). Since the Labour Government raised the flag in 1997, it has devolved legislative powers of certain areas to Scottish Parliament, a Welsh and an Irish Assembly, therefore they enact any legislation within their limits. Legislation established by the Parliament applies to the whole country. Unlike Japan, which mainly has its origin in continental law system, English law originated in the UK, which relies mostly on case law. So instead of having a written Constitution, it is regarded as consisting of both statute law on the one hand and case law in the UK. See 'Update to A Guide to the UK Legal System by Sarah Carter', <http://www.llrx.com/features/uk2.htm> (print out on file with author).

[255] Scottish Law Commission, 'Report on Computer Crime (Scot Law Com No.106)', (1987) Edinburgh. Also for reference, See the Scottish Law Commission's website, <http://www.scotlawcom.gov.uk/index-1.htm>. See also 'The Computer Misuse Act 1990: 5 years on', <http://csrc.lse.ac.uk/people/kelmana/CMA1990_Page3.htm> (print out on file with author).

[256] The minimal reform suggested that obtaining unauthorized access to a computer would be created as a new offence. The wider reform of some property related activities were accepted to be covered by the existing law. On the other hand, making all related activities the subject of specific computer-related offences might increase the deterrent effect of the law in the interests of clarity and certainty. *Ibid.*, at 10-13. Moreover recommendation one in the said report was implemented by section 1 of the Computer Misuse Act 1990.
Recommendation 1. (Unauthorized access to a computer)
Provision should be made for it to be an offence to obtain unauthorized access to a computer. *Ibid.*, at 9.

It classified computer misuse into five categories, then a published a report based on this working paper (Criminal Law Computer Misuse No.186). The role of these papers published by the Law Commission was the same as the Scottish Law Commission's report[257]. However, it argued that computer related conduct might not constitute an offence under existing criminal law[258]. Although there were other reports published in the Commonwealth, they are not discussed here, with, instead, a concentration on the development of law within the four countries in the UK[259]. While law enforcement had been struggling, there were some cases that highlighted the weakness of existing law[260]. In *R v. Gold* (1988) AC 1063, existing law was unable to penalise the defendant for hacking. In *Cox* v. *Riley* (1986)[261], the defendant was almost declared not guilty under the Criminal Damage Act of 1971[262]. Applying Section One of the Criminal Damage Act of 1971 was also inadequate for the earlier case because the word "damage" in Section One did not apply to a computer programme[263].

---

[257] See 'The Computer Misuse Act 1990: 5 years on', *supra* n.245.

[258] See 'Chapter One Crime and the Computer', <http://www.strath.ac.uk/Departments/Law/dept/diglib/book/criminal/crim16.html> (print out on file with author).

[259] For reference, (1) Queensland Department of Justice, Green Paper on Computer-related Crime 1987, (2) Interim Report Computer Crime 1988 (Gibbs Report) and (3)Tasmanian Law Reform Commission Report No. 47 of 1986, Computer Misuse. See 'Computer Crime Reports', <http://www.underground-book.com/chapters/ccm/10.html> (print out on file with author).

[260] Some concrete examples of computer crime between late 1980's to early 1990's under three categories:
[Criminal damage case]
Cox v. Riley (1986) 83 Cr. App. Rep. 54.
R v. Whiteley (1991) 93 Cr.App.Rep.25
[Theft and related offences]
R v. Thompson (1984) 3 All ER 565 (1 WLR 962)
[Hacking]
R v. Gold (1988) AC 1063.
See 'Regulating Cyberspace', <http://www.bileta.ac.uk/00papers/teichner.html>, 'IT Law LLM Reading List: Computer Crime', <http://www.qmw.ac.uk/~ccls/itlaw/reading/crime.htm> (print out on file with author), and 'Chapter One Crime and the Computer', *supra* n.248.

[261] *Cox v. Riley* (1986) 83 Cr App Rep 54.

[262] In *Cox v. Riley* (1986), the defendant erased computer programme which was kept in a plastic card. The computer programme was intangible property and it was not applicable to the breach of the Criminal Damage Act of 1971, because section 10 of the said Act of 1971defined 'property' as 'a tangible nature':
(Section 1)
A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property...shall be guilty of an offence.
The said programme was kept in the IC card, which was recognised as a tangible property, therefore the defendant was declared guilty. See 'Electronic Frontier, Crime and the Computer', <http://www.strath.ac.uk/Departments/Law/dept/diglib/book/criminal/crim11.html>, 'Case: Cox vs. Riley (1986)', <http://www.cs.mdx.ac.uk/courses/foundation/modules/bis0015/lectures/bis0015_week11/tsld017.htm> and '*Dai-5-syô Eikoku* (Chapter 5 England)', <http://www.ipa.go.jp/security/fy11/report/contents/virus/report5.pdf> (print out on file with author).

[263] Section 1 of the Criminal Damage Act 197:

The Computer Misuse Act of 1990 received Royal Assent in June and was approved as a form of a Private Members Bill addressed by Michael Colvin MP[264]. It came into effect on 1st September in 1990. It starts with explanations on penalising certain activities as computer misuse offences (section 1 to 3). Then, the exposition on jurisdiction is illustrated (Sections 4 to 9), followed by miscellaneous and general information (Sections 10 to 18). The three offences penalised by the CMA are:

- Unauthorized access to computer material;
- Unauthorized access with intent to commit or facilitate commission of further offences, and
- Unauthorized modification of computer material[265].

It is possible to say that unauthorized access to a computer, in the first place, is a central offence. From there, any further offences with such unauthorized access (theft, fraud, modification, and so on) follow. Like the Japanese UCAL, it could have penalised only unauthorized access to a computer comprehensively. But the difference to the Japanese legislation is that committing further offences with unauthorized access imposes a more severe penalty compared to mere unauthorized access to a computer[266]. Constituting an offence, subsection 1 of Section 1 explains this as a person knowingly accessing a computer, without authorisation, with the intention of getting access to any programme or data in the computer. At the same time, that access to a computer must be technically unauthorized. In this respect, it is not important to penalise an outside hacker (outsiders[267]): it is taken for granted that outsiders do not

---

'a person is guilty of an offence if, without lawful excuse, he destroys or damages any property belonging to another.'
See 'Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!', <http://webicli.ncl.ac.uk/1996/issue3/akdeniz3.html> (print out on file with author) and also '*Dai-5-syô Eikoku* (Chapter 5 England)', *ibid*.

[264] See 'House of Commons, Friday 9 February 1990', <http://www.parliament.the-stationery-office.co.uk/pa/cm198990/cmhansrd/1990-02-09/Debate-1.html> (print out on file with author). As Colvin MP stated, there was no draft bill attached by Law Commission, which published its report.

[265] See 'Computer Misuse Act 1990 (c. 18)', <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_2.htm> (print out on file with author).

[266] Computer Misuse Act 1990, *ibid*.
(Subsection 3 of section 1) Penalty for unauthorized access to a computer
A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

(Subsection 5 of section 2 and subsection 7 of section 3) Penalty for any further offence with unauthorized access to a computer
A person guilty of an offence under this section shall be liable—
(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

[267] 'Insider' in this context is explained by using the definition in the said report as;

have authorisation to access to a computer. However, in the case of an inside hacker there is the problem of proving that his intention to secure access was unauthorized — although the Law Commission report No.186 explained that unauthorized insider access is established whether or not a computer-owner invested in sufficient safety measures. Furthermore, the report clearly explained that an outside attack does not constitute an offence if a hacker has been invited — for example, to check security vulnerability[268].

Subsection 2 of Section 1 has, rather than narrowing it down, taken a wide scope of the objective resulting from an offence under this law[269]. Therefore, the objective is not the main factor in constituting an offence; and, any future form of data or devices are also protected under this law. Due to this background, for instance, the combination of Section 1 and 3[270] apply to the offence of attacking computer data by computer viruses.

In regard to the implementation of the principle of legality of crimes and punishment, there is an interpretation in subsection 2 (a) of section 2. As previously stated, the offence "unauthorized access with intent to commit or facilitate commission of further offences" is described in subsection 1 of Section 2. This does not mean that it is necessary for a further offence (committed on the basis of unauthorized access to a computer (stated in Section 1)) being assisted by a computer[271]. Any offence, where the sentence is fixed by law, is a crime. This can be seen as a basic approach to the principle of legality of crimes and punishment.

The CMA is obviously an individual law specially targeting computer-related crime. However it is, in fact, not an individual law; subsections 1 and 2 of Section 7 were prepared for insertion after subsection (1) of Section 1 of the Criminal Law Act 1977. Subsection 3 of Section 7 follows 1(1) of the Criminal Attempts Act of 1981[272]. It also refers to other laws, such as the Magistrates' Courts Act of 1980, the

---

"Insider' ... include not only employees of the owner or operator of the computer but also persons with authorised access to another system to which that computer is connected, and persons providing software or maintenance services to the system.' Therefore, 'outsider' is all types of hackers except perpetrators as stated in the above. 'Outsider' is more likely to be a typical hacker. See The Law Commission, 'Criminal Law Computer Misuse Law Commission report No.186' (1989) H.M.S.O., London, at 4.

[268] *Ibid.*, at 12

[269] Computer Misuse Act 1990, *supra* nn.255 and 256, and *infra* n.260. Subsection 2 of section 1 shows an object of an offence as:
(2) The intent a person has to have to commit an offence under this Section need not be directed at—
(a) any particular programme or data;
(b) a programme or data of any particular kind; or
(c) a programme or data held in any particular computer.

[270] Section 3 is established to ban unauthorized modification of computer material. See Computer Misuse Act 1990, *supra* nn.255, 256, and 260.

[271] See '*Dai-5-syô Eikoku* (Chapter 5 England)' *supra* n.252.

[272] The scope of section 7 is Jurisdiction. See Computer Misuse Act 1990, *supra* n.255.

Police and Criminal Evidence Act of 1984, the Extradition Act of 1870 and so on[273].

It is also possible to deal with a specific cybercrime with another type of law. Sending and spreading computer viruses is regulated by section 43 of the Telecommunications Act of 1984[274]. Furthermore, hackers are dealt with as "cyber terrorists" under section 19 of the Terrorism Act of 2000[275]. However, an offence in this context is categorized as an act of terrorism; not as a cyber crime. Section 19 of the said law is cited from Sections 1 to 3 of the CMA, wherefore any offence committed under its provisions is defined as terrorism.

Changing direction now, towards the customers of financial institutions, there are two different laws which are designed to allow individuals to check personal data held appropriately by organisations in the UK[276]: the Consumer Credit Act of 1974 and the Data Protection Act of 1984. The former Act refers directly to credit reference agencies, defined as "carrying on a business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected by the agency for that purpose". Two main factors of this Act are that:

(1) The data is concerned with individuals, not companies (i.e. an agency that restricted its activities to the creditworthiness of companies is not subject to the Act);
(2) Unlike the Data Protection Act of 1984, the Act covers data held in manual files as well as computer data[277].

The latter Act covers any organisation, which maintains personal data on behalf of the data user by imposing an obligation to ensure adequate security measures. The Data Protection Act of 1984 was formulated using the Council of Europe Convention principles. There is also some legislation existing in the UK: The UK Wireless Telegraphy Act can be effective on illegal interference with telephone lines, for example, eavesdropping. The Copyright Designs and Patents Act of 1988

---

[273] *Ibid.* Three legislation mentioned above refer Section 2, 14 and 15 of Computer Misuse Act of 1990 each.
[274] See '*Computer virus nado yûgai-puroguramu no houtekikisei nikansuru kokusai-doûkoû-chôsa* (The world trend of the legal approach towards injurious computer programme including computer virus)' <http://www.ipa.go.jp/security/fy11/report/contents/virus/law243.html> (print out on file with author).
[275] See 'Terrorism Act 2000', <http://www.hmso.gov.uk/cgi-bin/htm_hl3?URL=http://www.hmso.gov.uk/acts/acts2000/00011--x.htm&STEMMER=en&WORDS=comput+misus+&COLOUR=Red&STYLE=s>. and '*Hacker wo teroristo toshite atsukau eikoku no sinpou* (The new British Law against cyber terrorists dated 20th February 2001)', <http://www.idg.co.jp/report/security/backnumber/us_topics/200102/sec20010220_01_us.html> (print out on file with author).
[276] See Longley, *supra* n.41, at 289-290.
[277] *Ibid.*

(hereinafter "CDPA") is also effective for the legal protection of computer programmes. Although it is impossible to enjoy legal protection under the Patents Act, whose primary objective is to protect inventions, the CDPA does not restrict its subject to inventions only. The CDPA gives legal protection to a wide range of materials: literary works, dramatic works, musical works, artistic works, and sound recordings, cinematography films and radio and sound broadcasts. Computer programmes are categorised with literary works.

It is worth mentioning a consultation paper on the Conspiracy to Defraud in 1987. This recognised the potentially serious consequences of computer crime[278]. The most significant piece of legislation in this respect is the Computer Misuse Act of 1990[279]. It is divided into three offence types; "unauthorized access to a computer with intent to commit or facilitate the commission of a serious crime", "unauthorized modification of computer material", and "unauthorized access to computer". The Metropolitan Police's Computer Crime Unit resulted was set up under this Act and has sole responsibility for policing and enforcing it[280].

5. Comparative analysis of Japanese and the British legislation

According to the review published by the Department of Trade and Industry (hereinafter the "DTI"), the overall cost of computer misuse in the UK may amount to between £400 million and £2 billion[281]. The DTI also comments, regarding these figures, that careful interpretation is necessary as they represent the cost of all crime, including both computer misuse and crime using computer. There is obviously a huge gap between the two figures. Judging from the characteristics of cybercrime, these figures can be inflated easily. Similar figures, which are the estimated damage of cybercrime, are published all over the world but they are likely to be very different. This is because it is hardly possible to estimate the reality of cybercrime for three main reasons. Firstly, it is due to the difficulty of detecting a crime[282]. Secondly, it is easy to destroy evidence of a crime in cyberspace, as the majority of evidence exists in cyberspace. Also, a great many cybercrimals are skilful in using computers and mostly have experience of working with computer technology[283]. In cyberspace committing a perfect crime is not a dream. These two are particularities of cybercrime as well as obstacles to prosecution. Thirdly, it is due to a lack of awareness about the risks of being a victim of cybercrime. Even if

---

[278] Other relevant legislation to the issues are Civil Evidence Act 1955, Criminal Justice Act 1994, Theft Act 1968 and 1978, and Trade Descriptions Act 1968.
[279] Duff & Gardiner, *supra* n.20 and *infra* n.270 at 218-219.
[280] Duff & Gardiner, *supra* nn.20 and 270 at 221-222.
[281] Department of Trade and Industry, 'Dealing with computer misuse: review of the application of the Computer Misuse Act and the associated market for information and expert advice', (1992) Department of Trade and Industry, London, at 4.
[282] This has already been mentioned in Chapter I, therefore it is not discusses here.
[283] The Law Commissions report describes that many hackers have a background of software development or systems engineering. The Law Commission (1989), *supra* n.257, at 5.

a firm is damaged by a cybercriminal, it is more likely to be reluctant to inform the police and rather takes internal actions to solve the problem[284]. Legislation discussed in this chapter is mostly an aspect of criminal, rather than civil, law. Compensation is not covered by criminal law. Although compensation may be afforded under civil law, it is not always enough to cover the total damage of cybercrime or indeed worth the trouble from as it is time consuming. Pursuing a criminal case may reflect upon a firm's reputation. In that case the points at issue exist far beyond "a dearth of the awareness". Therefore, it is necessary to consider at least three figures to discover the real figure of the cost of cybercrime; a real figure of cybercrime being prosecuted, a real figure of undetected cybercrime, and a figure of cybercrime which was detected by a victim firm but has not been reported to the police. Any offence is likely to have similar problems to a greater or lesser extent. However, the number of undetected and unreported cybercrime cases is numerous, compared to the number of actual prosecutions. Moreover, there are some cases in cybercrime that do not incur any damage[285]. Nevertheless, it is contrary to the reason for excluding those cases from crime category, and those offenders are at least morally responsible. If there is no real figure available to show the damage as a result of cybercrime being committed, if there are some offences, which, though not damaging, still count as cybercrime, what remains to persuade the general public of the vulnerability of cyberspace?

The DTI described the pattern of computer misuse in the 1980's, shown in the Audit Commission's survey of computer fraud and abuse, as:

"It indicates increasing direct costs to computer users and ultimately to the economy as a whole; and

It may diminish potential users' confidence in computer systems and therefore reduce their willingness to introduce and extend the use of such systems[286]."

This analysis was partly realised. The former is completely true; as a familiar example, anti-virus and related computer software has increased its share of the market. In the latter case, Internet users, unlike the prediction, expanded rapidly. By early 2001, 13.6 million home online population had got themselves connected[287]. By September 2002, the total number of people with Internet access in the UK reached 34.3 million[288]. This figure obviously does not involve office online population.

---

[284] Department of Trade and Industry (1992), *supra* n.271 and *infra* n.276, at 4-11.
[285] Hacking is a paragon of non-damage-making cybercrime although it has been criminalized. Characteristics of cybercrime has been analysed in depth in Chapter I.
[286] Department of Trade and Industry (1992), *supra* nn.271 and 274, at 4.
[287] See 'UK Surfers Are Not Limited to Big Earners', <http://www.internetnews.com/bus-news/article.php/772461> (print out on file with author).
[288] See '*Heisei 15 nen Jouhou Tsuushin Hakusyo* (2003 White paper on

Nonetheless e-commerce has not rapidly spread, compared to the expansion of Internet users. Only 15% of the total online population frequently conducts e-commerce[289]. While it has been a year since electronic signatures received legal grounds in the USA as a result of the enactment of the Global and National Commerce Act[290], firms are nevertheless reluctant to introduce electronic signatures into their businesses[291]. This could, of course, be interpreted that firms are sceptical about using electronic signatures in businesses because of distinctive American characteristics[292]. There is a case for arguing that firms and individuals tend to be unwilling to take one further step into cyberspace. It is still too early to see the effect of the Global and National Commerce Act, which encourages the expansion of e-commerce.

It seems that both firms and individuals understand the vulnerability of cyberspace. The question is to what extent a firm or an individual realises their risk of incurring any offence. Until one faces real risk, for example, a firm receives a computer virus through emails and then computer data is erased or destroyed, feasibility would be lacking. This attitude is likely to apply to any type of crime. If the situation is so, and the impact of cybercrime is more likely to be massive, it is not necessary to prove the vulnerability of cyberspace.

The trend in Ministries in both Japan and the UK is apparently to promote strengthened computer security among the industries concerned. As was introduced earlier, METI in Japan published guidelines to reinforce computer security. Furthermore, there are some affiliated organisations associated with it. The DTI rather takes the view of improving business attitudes towards computer security as well as promoting awareness of the CMA[293]. In regard to affiliated organisations in Japan, there is an issue. Similar organisations existing under different Ministries, for instance METI

---

telecommunications)',
<http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h15/html/F1101300.html> (print out on file with author).

289 See '*Internet de syouhi ga hirogaru?* (Can Internet expand the number of online consumers?)',
<http://www.ntt-ad.co.jp/core_value/origin_s/dotocon2002_s/main_04_1.html> (print out on file with author).

290 The formal name is 'A Bill to facilitate the use of electronic records and signatures in interstate or foreign commerce'. See 'A Bill to facilitate the use of electronic records and signatures in interstate or foreign commerce',
<http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/bill-1999-k.htm> (print out on file with author).

291 See '*Beikoku denshisyomeihô sikoukara 1 nen, fukyû-kakudai wo habamu mondaiga sanseki* (A year has passed since Signatures in Global and National Commerce Act came into effect in the USA, innumerable problems to avoid popularised dated 1 November 2001)',
<http://www.idg.co.jp/report/itreport/backnumber/200111/20011101_01_ebiz_report.html> (print out on file with author).

292 It is expressed that firms are confused and reluctant to implement electronic signatures especially in trans-states businesses. *Ibid.*

293 Department of Trade and Industry (1992), *supra* n.271, at 3.

and the Ministry of Finance, are unlikely to cooperate with each other. It is of course true that they have different roles and areas for which they are responsible. Each organisation has different activities but they have common parts to share. If so, it may contribute greatly to promoting computer security when all organisations share their resources and experiences beyond the boundary[294].

Comparing the two pieces of legislations, in Japan and the UK, is difficult. The reason for this is not only because they apply to different legal systems. The critical difference is in the time the two laws were promulgated. The Japanese UCAL was introduced in 2000 whereas the Computer Misuse Act of 1990 already had ten years' history by then. The last decade was extremely crucial in technological developments. The more technical innovation, the more issues and brand-new types of crime arose. It is inevitable to regard the old legislation as "out of date". In this regard, the Japanese UCAL must be superior to the British CMA in covering new issues, which have arisen in the last decade. Still it is not that straightforward, and requires closer examination.

First of all, both the Japanese UCAL and the British CMA are individual laws to criminalize a certain offence. Both laws refer to other legislation, such as the Constitution or Criminal Law Act, with technically different meanings. The British CMA refers to other legislation to complement it; especially in the sections for Jurisdiction (Sections 4 to 9) and for miscellaneous and general (Sections 10-18), an interpretation in a section in the CMA is read as a reference to a section of other legislation in another jurisdiction. This is due to the formation of the UK's three jurisdictions within the territory. In other cases, the CMA declares it is without prejudice to others. Though Section 7 was prepared to insert in the 1977 Criminal Law Act in relevance to external law, the 1977 Criminal Law Act does not replace it to restrict the effect of the CMA. However, the Japanese UCAL is tacitly controlled under the Constitution. Furthermore, the UCAL cannot crack down on all types of cybercrime despite its preparation as a special law attached to the Criminal Law[295]. A certain offence is penalised under the Criminal Law (revised prior to the UCAL) in Japan. Four offences penalised under the Criminal Law are: illegal use of electromagnetic records, interference with duty by computer destruction and the like, computer-related fraud, or damage on a private and public document, whether authorized or unauthorized. If any offence is done by authorized computer access, the Criminal Law is the ultimate legal solution. The Criminal Law gives a more severe penalty than the UCAL. From this point of view, it is possible to say that the UCAL is

[294] The Centre for Financial Industry Information Systems is established under the Ministry of Finance. Information-technology Promotion Agency (IPA), Japan Information Processing Development Corporation (JIPDEC) and Japan Computer Emergency Response Team Coordination Centre (JPCERT/CC) are under METI. Each one of them surely has a specific role and activities.

[295] A special law mostly takes precedence over general law, such as the Criminal Law or the Civil Law.

designed to complement the Criminal Law. In other words, the UCAL has appurtenances to cover a certain offence, which cannot be penalized by the Criminal Law. Therefore it tends to apply to only a limited range of offences, and is very likely to be insufficient for further offences with unauthorized computer access, such as money laundering in cyberspace.

Returning to an offence under authorized computer access, the British CMA resembles the Japanese UCAL in that any offence with authorized computer access cannot be penalized under the CMA. It is appropriate to recognize an offence committed by using a computer in both cases. After taking everything into consideration, what is the advantage of having a specific law against cybercrime? It would be unnecessary to establish a specific law if it covers only limited offences, especially in statutory countries; revising an existing law would be adequate to address this. That is to say that two primary factors make cybercrime different from any other offence: the crime's difficulty of detection and the ease of destroying evidence of a crime in cyberspace. Do those factors particularly need to be emphasised in regard to legislative proceedings? It was hardly possible to find a particular reason to have a specific law to combat unauthorized computer access in the Japanese case. As far as examining articles 1 to 4 and 8, it would have been unnecessary to consider establishing a brand-new law. However, the nature of articles 5 to 7 is hardly suitable for insertion into the Criminal Law [296]. Those articles are more likely to be constructive measures to avoid unauthorized computer access, in response to the two difficulties already mentioned. Another possible reason for establishing the Japanese UCAL is of necessity; establishing a brand-new law has more political impact on the general public than revising an existing law [297]. This impact can be paraphrased as a short-term deterrent against unauthorized computer access.

In regard to the British CMA, the approach is completely different. Throughout all reports and papers published by the Law Commission and the Scottish Law Commission, both Commissions had discussed whether or not new offences should be defined. In addition to this, it was agreed that any crime (except unauthorized access to a computer) could be subject to sanction under the existing legislation. The British legislative approach was, compared to the Japanese approach, innovative. That is to say that

---

[296] Articles 5 to 7 of the Japanese UCAL have been mentioned earlier in this chapter. Article 1 is for purpose of this law, article 2 shows definitions of terms, article 3 prohibits acts of unauthorized computer access, and article 4 prohibits acts of facilitating unauthorized computer access. See 'Unauthorized Computer Access Law (Law No. 128 of 1999) (provisional translation)', *supra* n.227.

[297] Another possible reason for the UCAL of Japan is that Unauthorized Computer Access Bills were prepared by both the NPA and the Ministry of Posts and Telecommunications. Both of them took their position to establish an individual law. See '*Fusei-akusesu-taisakuhousei ni kansuru Keisatsuchou-an oyobi Yûseisyou-an heno paburikku komento bosyû henotaiou nitsuite* (The correspondence to the public comment advertisement on Unauthorized Computer Access Bills by the NPA version and the Ministry of Posts and Telecommunications version'), *supra* n.217.

creating a new offence leads to establishing a new individual law without considering revising the existing law. The Japanese legislation takes a rather more cautious approach; taking the choice of either inserting a new offence into an existing law or establishing a new law. This is a crucial difference based on their legal systems[298].

Considering the application of jurisdiction, the principle of territorial jurisdiction is widely accepted, but not always successful. The principle of universal jurisdiction will now be examined. This applies to the protection of universal values, for instance, piracy and genocide. The UN manual interpretation explains, "...the universality principle, based on the protection of universal values". It is usually effective on the basis of express treaty provisions but is otherwise rarely used. It is generally held that this principle should apply only in cases where the crime is serious, where the State that would have jurisdiction over the offence, based on the usual jurisdictional principles, is unable or unwilling to prosecute. The territorial jurisdiction successfully works if a certain country has primarily criminalised a certain offence, and further, if that country has a will to prosecute. It would be unsuccessful if a country has not criminalised the offence or is unwilling to prosecute. Of course, it is possible to prosecute such a case in conjunction with other jurisdictions, that is, the active or passive nationality principle and the protective principle. However, applying universal jurisdiction is more applicable when combating computer crime. This is based on the following reasons: firstly, the damage/loss of computer crime is huge in many cases compared with that of national/transnational crime. Secondly, that damage can lead to serious confusion in the economy in the national market, and resultantly it will cause serious confusion in the international market. Thirdly, computer crime has already become a worldwide phenomenon and has become recognised as a transnational crime at an international level. Fourthly, because of the advent of the Internet and digital cash, international co-operation has become an imperative factor in combating such crimes. In fact, the UN reported that, in formulating a computer crime strategy, it would be helpful to create universal criminalisation. Therefore, it would be possible to apply a universal jurisdiction. A universal jurisdiction would eliminate the need for extradition. The computer criminal could be prosecuted in the country where the crime was committed. The other four

---

[298] The Law Commission clearly mentioned that creating new criminal offences pertaining to computer misuse as the most appropriate approach to the reform of the criminal law. It analysed three specific issues: computer fraud, the threat presented by hacking, and unauthorized destruction or alteration of information held in a computer. Regarding computer fraud, it stated that the general criminal law was adequate to meet most cases. A specific case, which does not meet the criminal law, still did not give a good reason to suggest the urgent reform. Concerning unauthorized destruction or alteration of information, the crucial argument was the interpretation of 'property'. The Commission explained the disadvantages of applying the existing law and recommended creating a new offence directly. Referring to hacking, it evidently assented that privacy is not generally protected under the criminal law, and placed the importance on criminalising it. See the Law Commission (1989), *supra* n.257, at 9-15.

jurisdictions are aimed at protecting national interest more than international cooperation, thus, using any of these is likely to prove unjust to one party.

In effect, the initiatives of international organisations, including working groups, are needed to offer recommendations based on extensive research. It may be necessary to establish an organisation to arbitrate in computer crime disputes. This implies that an international criminal court may not always be needed, because computer crime is concerned with the economy. An international arbitration, even in the private sector, will be invited to participate in a computer crime dispute providing it can prove its ability to work effectively. Whether applying a territorial jurisdiction or a universal jurisdiction, the essential factor is which one works more effectively at persuading people to comply. The crucial point concerning this problem is the ability to adapt the most effective jurisdiction, case by case, under international consensus.

As was mentioned, it is recognised that the existing legislation in the UK is adequate to deal with any computerised crime except one: unauthorized access to a computer. It is a similar conclusion to that which the Japanese UCAL came to. The CMA is prepared to penalise only for unauthorized access to a computer and further offences based on the groundings of unauthorized access. It is essential to examine the difference in illegal offences designated by law. Under the CMA, unauthorized access to computer material is a core offence; from there, an intentional offence and unauthorized modifying computer material follow. The UCAL of Japan criminalizes unauthorized computer access itself in the first place and then, an offence to aggravate unauthorized computer access to others. The CMA unquestionably covers many more offences than the UCAL. Neither a further offence with unauthorized computer access nor unauthorized modifying of computer material are independently dealt with under the UCAL. Due to the nature of the UCAL as a special law, it is prioritized over the Criminal Law. In the case of forgery on the basis of unauthorized access to a computer, this offence is decided on by both the UCAL and the Criminal Law. However, only the CMA covers such an offence in the UK. Applying more than two laws seems to cause unnecessary confusion. Moreover, it is very likely to involve technical issues or terms, especially for cybercrime cases, and those would be an obstacle to standing trial — particularly for judicial officers. It would be more effective to apply for one single law only against an offence/offences. In the case of forgery on the basis of unauthorized access to a computer in the UK, the offence is penalised under section 2 of the CMA (if the offence was indicted under the CMA). The penalty for a person who commits the offence would be mostly the same under the 1981 Forgery and Counterfeiting Act[299].

[299] Section 2 of the Computer Misuse Act of 1990 prepares imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both for an offender. Section 6 of Forgery and Counterfeiting Act 1981 prepares the

On the other hand, a broad interpretation of offences tends to lose the efficiency of the law itself. The essence of having any law is to deter the general public from committing a crime. If the interpretation of an offence covers a wide range, the focus of the law falls into vague ambiguity; therefore, the perception of the general public is likely to be vague and uncertain. This in turn reduces the law's effectiveness as a deterrent. There may be a view that the existence of law itself deters offences although it would not deter careless offences committed without understanding the aim of the law. The CMA covers a wider range of computerised offences than the UCAL. Furthermore, the name of the law itself is indistinct; it is hardly possible to know what exactly "computer misuse" could be. Conversely, there may exist a view that a wider interpretation of offences, and unclear wording, make the general public aware and (suspicious of each other's activities) so that it provides more deterrence than the narrower interpretation of offences with its precise wording. Unfortunately from the characteristics of cybercrime mentioned in the previous chapter, many cybercriminals are individuals whose purpose of committing a crime is to enjoy people's response to their deeds. For those criminals the deterrent efficiency of law hardly works on their knowledge and ability to manipulate computer technology. But the deterrence surely works on the rest of the cybercriminals. Therefore it is of importance to make the general public well aware of the law.

The victims of any cybercrime are supposed to be either an individual or a firm. In this thesis, the emphasis is on firms (more precisely in the financial sector) for the economic stability point of view. Firms in both Japan and the UK have been, in reality, aware of the laws combating cybercrime. However, a critical problem lies in firms. As the DTI review stated earlier in this chapter, firms are very likely to be reluctant or even avoid reporting incidents to an administrative agency concerned. The reasons have been stated: pursuing a case can be time-consuming as well as unattractive to firms due to the lack of monetary recovery functions such as compensation in civil cases. The other reason is a firm's reputation. It is easy to see how a firm would prefer silence over advertising itself as a crime victim. In reality, it is sometimes

---

same penalty but more precise. However the Law Commission stated in its report that,
'...if computer records are altered by an authorised user in order to create a false impression ...that is plainly forgery.'
If an offence is considered as forgery, Forgery and Counterfeiting Act is applied for it. On the contrary, in *R v. Gold and Schifreen,* the respondents were acquitted after the appeal owing to the lack of appropriate legislation at the time the offences were committed in 1984. The CMA would prove to be applicable to such a case.
See 'Computer Misuse Act 1990 (c. 18)', *supra* n.255, and 'Forgery and Counterfeiting Act 1981',
<http://www.butterworths.co.uk/academic/lloyd/Statutes/forgery.htm> and the Law Commission (1989), *supra* n.257. For the case, see 'R v. Gold and Schifreen [1988] 2 WLR 984', <http://www.underground-book.com/chapters/ccm/Gold.html> (print out on files with author)

discrediting for it to become known that a firm was hacked. It shows that the firm was without a sufficient security measure to protect itself, or had a security hole to make it easy for offenders to attack — making itself vulnerable to more offenders. It has been mentioned repeatedly that the difficulties of cybercrime are detection and destroying evidence. Firms as victims, are the ones who find a crime scene. If victims do not report incidents, it is impossible either to prosecute for an offence or indeed to know an offence has been committed. This is the same as a victim concealing an offence, and thereby sheltering an ill-intentioned offender. But in fact, the firms take internal measures[300] to reduce, minimise or avoid the damages suffered, and thus avoid sheltering an offender even if he is an insider. Still it is a vicious circle; firms do not report the incidents, and criminal prosecutions are not pursued. The low ratio of prosecutions against cybercrime does not lead firms to believe that it is less frequently committed compared to their expectations, due to so much information to the contrary[301]. This impresses on firms that criminal prosecutions against cybercrime are mostly unsuccessful, and this too prevents them from reporting incidents. Even if a new offence to incriminate any firm or individual who does not report an incident is established, this attitude will not change easily, and the situation could worsen. One possible method to encourage firms to report incidents is permitting them to apply to civil courts and requesting compensation to cover the damage of cybercrime. However, if the damage were substantial, it would be impractical to pronounce a sentence on a cybercrime offender to compensate for the total damage. The offender is unlikely to be unable to pay huge damages unless he/she was a billionaire. In criminal cases, it is much less attractive for firms to report incidents since there is no compensation they can claim.

Taking financial institutions into consideration, the critical issue is the integrity of information and its availability for market stability. Losing integrity and availability in the financial market could cause market disorder. Nonetheless, these are not defined even if "intangible property" is the result; they are notions. Thus, it is so far impossible to protect "integrity" or "availability" by laws yet. Law extends protection only to tangible property. The idea of protecting these notions exists far beyond it. Protecting the value of intangible property comprehends roughly the meaning of protecting "integrity" and "availability" of information. Nevertheless it is not the same thing. The problem is that ruining "integrity" and "availability" without damaging either tangible or intangible property is likely to happen in cyberspace. The typical example is hacking. Hacking is said to be likely a harmless crime [302]. A hacker may

[300] Asking compensations, dismissal of an offender and so on.

[301] Warnings and incidents reports of computer virus and hacking published by research organisations or computer software companies are always available. Reporting those incidents is automatically done through Internet when an incident is found, and there is no legal obligation to accompany with.

[302] Scottish Law Commission, 'Report on Computer Crime (Scot Law Com No.106)', (1987), *supra* n.245.

get unauthorized access into a computer without altering or damaging information. However it means that information is always in danger of being altered or damaged; in short, information integrity and availability is infringed. It is possible to say that therefore the Japanese UCAL and the British CMA have aspired to criminalise unauthorized access to a computer. But the point is that the penalty of the said offence is very likely to be minor compared to the possible impact of infringement of information integrity and availability. This is still the limit of legislation for both countries at present.

The more computer technology develops, the more types of cybercrime emerge. In addition to this tendency, many financial institutions in Japan find more significance in having a law to define whether offence could be illegal, rather than being protected under the law in general[303]; the general criminal laws provide a certain framework. Any legitimate business activity within the framework is legally protected; by the same token, any offence being committed against the framework is punished and the damage occurring as a result of an offence is compensated to a certain extent.

However, financial institutions are likely to be interested in new legitimate business outside the framework. Using e-cash for business can be useful although it is also likely to be abused. Moreover, money laundering in cyberspace is not yet a major problem although it could happen much more easily than in the "real world". In case of any new type of cybercrime being committed, it is critical to consider whether or not any existing legislation addresses it. For instance in regular money laundering cases, the Law for Punishment of Organized Crimes, Control of Crime Proceeds is generally applied in Japan and the Money Laundering Regulations of 1993 and the Financial Services and Market Act of 2000 in the UK[304]. It is critical whether or not any existing legislation, including the UCAL and the CMA, is sufficient to criminalise where e-money laundering happens under the present conditions. Both in Japan and the UK is whether it is committed contingent upon unauthorized access to a computer. If an insider or any authorised person commits e-money laundering, there is no chance to meet the UCAL or CMA. E-money laundering would be dealt with as money laundering accompanied by a computerised factor or simply computer manipulation or fraud, so the said existing legislation in both Japan and the UK would play an important role. In reality any cybercrime is not listed as a conditional crime of money laundering in Japan at present[305]. Combating money laundering is, in

---

[303] The author is grateful to financial institutions, where the author visited in 1999-2001, for their invaluable comments and advice.

[304] See 'Regulations at the Financial Services Agency', <http://www.fsa.go.jp/fiu/fiue/fhe001.html> (print out on file with author). The Financial Services and Market Act 2000 has come into effect on 1 December 2001.

[305] Illegal use of electromagnetic records (Article 161, 2) and computer-related fraud (Article 246, 2) under the Criminal Law are listed as a conditional crime of money laundering. See 'Conditional crime list on money laundering',

plain words, to prevent and forestall a further crime being committed, which affects the public welfare and damages the economy. From the viewpoint of protecting information integrity and availability, if e-money laundering is very likely to endanger financial stability, financial institutions ought not to leave the matter until e-money laundering is actually committed. At the very least, e-money laundering against a financial institution would easily cost it its reputation. For practical purposes, it may be unnecessary to establish a brand-new law, especially against e-money laundering, as long as information integrity and availability is impeccably maintained, and legal remedies are available in case of any threats. It is doubtful whether existing legislation fully covers cyberspace issues in both countries, whereas stretching new legal boundaries too far may restrict further business development. Therefore, it is crucial to concentrate on protecting a specific issue such as information integrity and availability. In this viewpoint it has to be said that legal protection in cyberspace still leave much to be desired.

It is crucial to involve a specific institution for financial services to combat not only e-money laundering but also other cybercrime against the financial institutions; the Financial Services Authority of the UK (hereinafter the "FSA") and the Financial Services Agency of Japan (hereinafter the "JFSA"). They must play a central role in assisting financial institutions as well as combating financial crime. If financial institutions are less cooperative in combating cybercrime, appropriate guidance needs to be provided. If the financial sector needs any legal assistance to maintain its stability, it ought to approach the authorities. Mutual cooperation between the financial institutions and the FSA/JFSA would be effective in deterring cybercrime.

<http://www.fsa.go.jp/fiu/fiu.html> (print out on file with author).

Chapter IV: An Analysis of Civil Law

1. Introduction

Whether consciously or unconsciously, all humankind is involved in contracts everyday: for instance, one purchases a loaf of bread by paying its price to a bakery. This commercial transaction is legally defined as a contract. As is obvious, it is unnecessary to sign a contract form to complete this transaction. If the bread is found to be mouldy after the purchase, the purchaser would ask to exchange it for a new loaf or for a refund of the money paid and the seller (= the bakery) would agree to the demand. If the seller does not agree on either exchanging the product or making a refund, the purchaser could sue the seller for negligence. If the purchaser has food poisoning after eating the mouldy bread without noticing the mould, and he/she could prove that the cause is the mouldy bread, he/she could seek compensation. Those simple assumptions happen without the signed contract form between the two parties, because the purchase itself is considered to be a sales contract. Even if there is no sales contract, there are cases where one could seek compensation for injury, damage and losses. Suppose one has a dog and it bites a leg of a passer-by while being taken for a walk in a park. There is no contract between the dog's owner and the passer-by: they are perfect strangers to each other. However, the owner is liable for the injury of the passer-by: the passer-by is able to claim a fee for medical treatment.

The cases above are disputes between private individuals. The former example proves how contracts are familiar to daily life without our realizing it. In the first case, a contract is considered to be a primary factor. Contrary to this, there exists no contract between the two parties in the latter example. If the passer-by demands from the dog's owner the right to claim compensation for his injury, tort theory of civil law comes into effect. Indeed, contracts are one part of business transactions that civil law deals with. Tort theory basically works if there is no contract behind the parties involved in an incident. Both cases are dealt with in civil law in Japan; continental countries, such as Germany and France, have similar civil law systems. In the UK, common law and statues correspond to take care of such cases. This is merely a difference of legal systems between continental law and common law[306]. It is not too much to say that civil law is, in a certain sense, the most familiar law worldwide. The dividing line between contracts and torts is sometimes not clear. For example, there was a case in Japan where a member of the Self-Defence Force died in a car accident on the premises. The bereaved family brought a lawsuit against the State more than three years after the accident. The plaintiff's complaint was based on the State's default on an obligation based on the principle of faith and trust. That is to say that the State neglected to ensure a safe work place. This is because legal prescription on tort is

[306] Thus, the generic term 'civil law' is used in this thesis to refer to law dealing with interests amongst private individuals.

three years whereas suing the State by default gave the bereaved family 10 years' legal prescription. Hence, it is possible to say that there are flexibilities in civil law.

In general, civil law is applicable when a private individual seeks monetary (or other) resolutions for one's loss or injury. If the passer-by in the latter example is dead as a result of the dog's attack, criminal law would be called upon. It is no wonder that civil relief is acquired with criminal punishment. Civil actions are normally brought after the criminal suit. Criminal law imposes punishment (such as imprisonment or a fine) on a perpetrator to compensate for the death of the injured party of an incident. Needless to say, the nature of a fine is entirely different from that of compensation. If an incident results in both a criminal and a civil action, it is possible that the two courts judge differently on the extent of negligence. For instance, even if it is judged in the civil court that compensation to be paid is suitable, it is possible that a criminal court judges the same case and does not reach the decision that criminal punishment is necessary to be imposed. Criminal liability is very likely to be more serious than civil liability in the vast majority of cases. Hence, being judged the other way around would be less likely to happen[307].

Due to the nature of the law, relief measures under civil law are basically sought within the domain of domestic law. That is to say that there is no international cooperation, such as a convention or treaty, on civil law. As is mentioned in Chapter II, it is very likely to establish conventions and treaties in relation to criminal law to criminalise a certain offence at the global level. However, seeking civil resolutions deals with entirely individual matters and is unlikely to arouse the necessity of international mutual understandings or cooperation. It is, of course, likely to involve two parties in different jurisdictions. In this case, the dispute should be settled in either jurisdiction by mutual consent.

In the event of losses or damage occurring in cyberspace, are victims able to seek civil resolutions as simple as in the case of mouldy bread? In this chapter, this delicate proposition will be discussed in depth with explanations from three major standpoints: how an incident happens, which parties are involved, and what legal interests are involved.

2. Preliminary Knowledge on Three Major Standpoints

Here are three standpoints to be considered in the context of cyber loss:

(1) How does an incident happen?
(2) Which parties are involved?

---

[307] See M. Kato, '*Jimukanri, Futouritoku, Fuhoukoui* (Misconduct of business, Unjust enrichment, and Tort)' (2002) Yūhikaku, Tokyo at 411-412.

(3) What legal interests are involved?

In regard to the first standpoint, it explores what could cause an incident. An incident is sometimes likely to be caused by accident or carelessness. Other times it is perpetrated. In other words, an incident happens as a consequence of professional negligence or intentional/malicious interference to businesses. Intentional or malicious interference can be paraphrased as an offence. Those two grounds of legal obligation almost suffice to answer the first question. However, are these all? The actual situations should not be so simple to judge each case by two of them. Considering the characteristics of cyberspace, what if the computer systems of a company (X) is accessed by an individual (Y) without authority, and Y abused X's computer system as a stepping-stone to commit further offences against a third party (Z)? Can X defend itself against a lawsuit brought by Z?

In the second place, it is important to judge who an injured party/ perpetrator would be. Financial institutions can be both injured parties and perpetrators even at the same time. Take the assumption raised earlier: an original perpetrator Y hijacked the computer networks of financial institution X. Y abused the networks as a stepping-stone to cause damage upon a third party Z. There are three parties involved: a perpetrator Y, and two injured parties Z and X; however X's position (a perpetrator or a victim) is not clear. Z is, without doubt, an injured party and Y is a direct perpetrator of the incident. From Z's point of view, both X and Y are defined as perpetrators. However, X is also an injured party of the incident whereby losses are caused by Y. As an injured party, X may/may not suffer any direct losses from Y if Y's motive to abuse X's computer system is to damage Z. Thus, X remains as an indirect injured party. This works conversely: as a perpetrator, Y is a substantial perpetrator. However, X could be defined as an indirect perpetrator for Z.

Keeping these in mind, who could be X (both an indirect perpetrator and an indirect injured party), Y (a direct perpetrator) or Z (a direct injured party) in the event of a cyber incident? Considering the principal object of this thesis, X is to be financial institutions: they are likely to be both an indirect perpetrators and an indirect injured parties at the same time. Moreover, financial institutions are potentially to take a position of Y or Z: Y could be an employee or ex-employee of X, or anyone unconnected to X. If an employee of a financial institution causes losses to a customer, this institution is likely to be blamed for negligence in employee supervision — that is to say that the institution officially plays the role of a direct perpetrator. In this case, the institution becomes an injured party when it files a suit against its perpetrator (= an employee). If a hacker intentionally causes losses to a financial institution, that hacker is the direct perpetrator and the institution is the direct injured party. This can be more simply explained by categorising into groups. (Table 3.1)

Table 3.1: Who plays what role in incidents of cyber crime?

An injured party	Perpetrators			
	Direct			Indirect (causing losses through FIs' computer networks)
	FIs (an employee)	A 3rd party	A hacker	A hacker
FIs (a corporate body)	(1) Negligence or (2) Intentional	(5) Negligence	(6) Intentional	(7) Intentional
A 3rd party	(3) Negligence or (4) Intentional			

FIs= Financial Institutions
ISP= Internet Service Providers
The shaded portions are irrelevant cases in this thesis.

In the type of cases highlighted in the table, injured parties are either financial institutions (as a corporate body) or a third party. A perpetrator causes losses directly or indirectly. A common party in both cases is hackers. A hacker can be an employee or an outsider. However, in this context, it is easy to define hackers as outsiders who do not have authority to access computer networks of financial institutions. This means that ex-employees of financial institutions are included in this definition of hackers. In general, it is not necessary for hackers to commit offences with the intention to damage others. However, hackers in this special context are very likely to have the intention to cause damage, as they naturally do not have any authority to access others' computer networks. It is possible to consider a case that someone might have authority of computer access but is not employed by a company. If there is such a person, he/she must be an interested party to the company to some degree. So, such a person should be judged to have a similar position to employees. Employees causing losses to any party could be acting with negligence or with intention. A third party as a perpetrator is different from a hacker; that is to say that he/she causes losses by negligence or with intention. If losses are caused with wilful intention, the person should be defined as a hacker. Hence, there are seven cases to be examined.

Finally, the essential standpoint is the legal interests. What could be damaged as a result of negligence or cyber crime being committed? The possibilities at risk are: money, computer hardware, data and computer programmes, website contents, domain name, copyrights and intellectual property rights, good reputation, and privacy. Even in the absence of damage, if a firm is unable to offer online services, its economic losses or opportunity losses must be considered. Central to this question is which

rights would cover each legal interest.

3. Japanese Civil Law and Basic Issues

Looking at Japan, the applicable law for civil resolutions is mainly civil law. Depending on the legal interests being trespassed, other specific statutes become involved, such as Copyright Law, in protecting legitimate owners' rights in case of infringement. Still, civil law is the very centre for seeking resolutions. The Act concerning Prohibition of Private Monopoly and Maintenance of Fair Trade and the Product Liability Law also have specific Articles on right of compensation claim for losses (Article 25 of the former and Article 3 of the latter). However, they are most likely to be irrelevant to any legal interest to be discussed from this point.

Japanese Civil Law has its origin in both German and French civil law[308]. It consists of five chapters: general rules, property rights, claims (those three were promulgated in 1896), relatives and inheritance (the last two were promulgated in 1898). Japanese Civil Law as a whole came into force in 1898[309]. Chapter 5 Tort (*Fuhô kôi*) provides:

> Article 709
> A person who infringes upon others' rights by negligence or with intention shall be liable for compensating a loss (except an accidental fire);
>
> Article 710
> A person who is liable for damage, regardless that it was caused as a result of harming another's body; infringing another's freedom, discrediting others, or trespassing on others' property rights, shall be also liable for compensating a loss other than damages on property;
>
> Article 715
> A person who employs others for his/her businesses shall be liable for compensating a third party's loss that is caused by an employee while conducting the business(es). Providing an employer supplies appropriate attention on appointing an employee to a post, or supervising the businesses, and yet a loss occurs, it shall be exempted from the previous term.
>
> Clause 2
> A person who has supervised conducting the businesses as a substitute for an employer shall fall under the previous clause.

---

[308] See '*Minpô no manabikata* (How to learn Civil Law)', <http://www.nomolog.nagoya-u.ac.jp/~kagayama/howtostudy/howtociv.html> (print out on file with author).
[309] See '*Minpô* (Civil Law)', <http://www.houko.com/00/01/M29/089.HTM> (print out on file with author).

Clause 3
Provided clauses do not prevent the right of redemption for an employee and a supervisor of an employee.

As illustrated, Article 715 establishes an employer's liability for his/her employees' business conduct, unless one could prove suitable attention having been given to them. However, in reality, it is hardly possible to place this privilege on employers in court cases. This is called strict liability. There are some grounds on the strict liability rule: firstly, it is hardly possible to find sufficient financial resources for an employee in case of losses having been caused as a result of his/her business conduct. So it is reasonable to ask for compensation from his/her employer. Secondly, it is based on the theory that a loss should be taken by a profit-making party: that is to say, that an employer obtains profits from employees' business conduct. So, it is fair to turn losses into profits[310]. This strict liability rule has been developed in the USA where insurance products covering all varieties of liability are commonly purchased. Consequently, there exist opinions on this rule to assert that the rule could not easily adjust to Japan[311].

To acquire the right to make a claim for damages according to Article 709, there are four conditions to be satisfied:

(1) There was an act of negligence or with intention (hereinafter "J1");
(2) The act infringes other's rights (hereinafter "J2");
(3) As a result of 2, losses or injuries occur (hereinafter "J3");, and;
(4) There are proximate relationships between 1 and 2 as well as 2 and 3 (hereinafter "J4");[312].

On the contrary to the said four conditions to claim, the right cannot be acquired if any of the next three conditions is proved even if the said four conditions are satisfied:

(5) If a perpetrator is a distracted person (i.e., a juvenile, a person who is *non compos mentis*) (Article 712 and 713);
(6) If the conduct was done for lawful self-defence or an act out of necessity (Article 720), and;
(7) If there is any legitimate cause of non-imputability other than 5 and 6[313].

---

[310] M. Kato, *supra* n.294, at 361-362.
[311] See '*Network-jô no fuseikoui ni kansuru siyousyasekinin nokentou* (An analysis on employer's liability on online unlawful behaviour)', <http://www.kisc.meiji.ac.jp/~skondo/ethics/genko000920hp.pdf> (print out on file with author).
[312] M. Kato, *supra* n.294, at 143-145.
[313] *Ibid.* In regard to condition 7, it is not written in Japanese Civil Law. The possible cause of non-imputability is, for instance, a case if the conduct was done with an injured party's consent.

In regard to the methodology for civil remedy, it is basically accepted as monetary compensation under Article 722 in application of Article 417:

> Article 417
> In relation to redress of damages, monetary compensation is to be applied unless otherwise specified a declaration of intent.
>
> Article 722
> Article 417 is to be applied for the redress of damages based on wrongful conduct.
>
> (Clause 2)
> A court takes a fault or negligence of an injured party, if any, into consideration in deciding the sum of the redress of damages.
>
> Article 723
> At an injured party's request, a court is to order a perpetrator, who discredits others, to compensate damages or take appropriate measures to revive reputation as well as monetary compensation.

Article 417, however, does not restrict the measures of redress of damages. For instance, an injured party has a right to demand the injunction against an infringement or invasion of its right. If the object of damages is reputation, it is likely to be accepted to claim on publishing an apology in a newspaper[314].

When analysing an offence, it is necessary to judge the cause of the incident clearly. As Article 709 states, only an act through negligence or with intent obliges a perpetrator to compensate for damages. The Supreme Court in pre-war Japan in 1899 ruled negligence as the violation of one's legal duties as a result of one's defective act causing losses[315]. There are two main streams of theories of negligence: the objective or the objective negligence theories, and the actual or the abstract negligence theories. The objective negligence theory requires a careless state of mind at the time of perpetrating an act. The objective negligence theory means a perpetrator violates one's legal duties. Take a car accident as an example: if a perpetrator carelessly drives a car and hits a person. This is easier to be explained by the former theory. If a perpetrator pays as much attention as possible but is still breaking the speed limit, it falls better into the latter theory. On the other hand, the actual negligence theory means a perpetrator neglects duty of care on the basis of his/her own ability or knowledge. In this theory, the level of duty of care is not standardised and is always different as the case may be, due to the fact

---

[314] See '*Songai Baisyô - Kinsen Baisyô* (Redress of Damages, Monetary compensation)', <http://www02.u-page.so-net.ne.jp/rb3/tortslaw/3-3aDamages.HTM> (print out on file with author).

[315] See '*Fuhô Kôi* (Tort)', <http://cc.matsuyama-u.ac.jp/~tamura/minpo-709.html> (print out on file with author).

that each person has different ability or knowledge. The abstractive negligence theory means a perpetrator neglects duty of care on the basis of a general level which a reasonable person usually fulfils. A reasonable person is considered to be a person potentially in a similar situation: it does not mean the general public. The actual negligence theory is hard to be applied in practice compared to the latter theory, so the abstractive negligence theory is generally applied. But assume there are two persons in the scene: one is seriously injured or sick and he/she requires first aid. If another is a non-qualified person, the required duty of care of first aid is unlikely to be a professional level. If the injured person is deceased as a result of first aid being applied, it would not be a problem that the abstractive negligence theory were applied in this case. If that person is a medical professional, required duty of care cannot be on the same level as the former case. There is no doubt that the expected level of first aid should be of a professional level. In this case, the perpetrator would be judged against whether the treatment he/she gave to the deceased was legitimate and up to the level of his/her knowledge, skill or ability[316]. The pre-War Supreme Court adopted the abstractive negligence theory in 1911[317].

The other theory is based on foreseeabilitiy and the duty to avoid risk. If a reasonable person could foresee, but a perpetrator did not foresee a consequence when an incident occurred, it is judged that the perpetrator is to blame for negligence. If a risk is foreseen but a perpetrator did not try to avoid an incident happening, this is also judged as the perpetrator's fault[318].

However, a criterion of evaluating negligence might still be ambiguous. US Judge Learned Hand introduced the model finding of negligence in the case of *the United States v. Carroll Towing Co* in 1947. He proposed three key factors: P as probability, L as loss, and B as burden or cost of precautionary measures preventing losses, whereupon PL (probability X loss) represents the mean value of losses. If B is less than PL (B<PL), Hand's logic suggests that losses are inevitable results since the level of precautionary measures is not satisfied and negligence is to be admitted. If B is bigger than PL (B>PL), it suggests negligence cannot be admitted since the necessary level of precautionary measures is taken. However, there is a plain defect in this logic. It is most unlikely to be able to know or calculate exact damages or costs[319].

All the theories above-mentioned are merely criteria for a party to prove a perpetrator's negligence; it neither means only one of those

---

[316] See M. Kato, *supra* n. 294 and *infra* nn.305 and 306 at 154-159.
[317] See '*Fuhô Kôi* (Tort)', *supra* n.302.
[318] See M. Kato, *supra* nn. 294 and 303, and *infra* n.306, at 160-164.
[319] See M. Kato, *supra* nn. 180, 294, 303 and 305 and also see 'Liability for Computer Glitches and Online Security Lapses', <http://www.sidley.com/cyberlaw/features/liability.asp> (print out on file with author).

theories is right, nor that it applies to all cases. The burden of proof is carried by the party who claims for compensation. In other words, it is the duty of an injured party to prove negligence or intention with regard to a perpetrator's act. Hence, the injured party is practically required to look at the act in question from different angles in order to prove negligence.

An act with intention is rather simpler to consider than the negligence theories. If a perpetrator knowingly takes an action that would infringe upon another's rights, one's wilful intention (to interfere with an other) is to be identified. Against this background, it is unnecessary for the perpetrator to foresee the occurrence of any loss or injuries[320]. The Supreme Court of Japan ruled in 1957 that the requisite of wilful intention is the cognisance of a perpetrator to infringe upon proprietary privileges of others in general: it is not necessary to indicate the proprietary privileges of a specific person[321].

When the court comes to the decision of protecting an injured party, there is another issue to be considered: deciding the amount of compensation for losses. Depending on the legal interests being infringed, it is often difficult to estimate the factual value of losses. In the USA, a court has authority to give exemplary damages at its discretion if a perpetrator's act is judged to be based on immoderate *mala fide*. It was the fact that a subsidiary in the USA of a Japanese company was ordered to pay out US$ 1.125 million for its deceit on a rental contract as exemplary damages in the US court in 1997. In Japan, neither judicial precedents nor a common view is affirmative on this issue. On the contrary, an estimation of consolation money is at the judge's discretion according to a degree of relevant particulars, such as a perpetrator's *mala fide* and the emotion of an injured party[322]. Due to some complications, the Japanese court dismissed the case when a plaintiff of the said case brought a lawsuit in Japan claiming the payment of $ 1.125 million. At first, the Supreme Court gave the reason that the decision made by the US court was prejudicial to public order and morals provided in Article 118 of the Code of Civil Procedure. Secondly, the court translated that the Japanese system of indemnity promises an injured party restoration of losses as before; its implication is different from that of exemplary damages[323].

Finally, as was previously mentioned, contract issues are dealt with by Civil Law as a part of the law of obligations. If an injured party has a contract with a perpetrator, there may be possibilities to deal with a case under the law of obligations. However, it is dubious whether the terms of a contract include the clause on the services of providing, receiving and processing data. If that is the situation, there is hardly an opportunity to

---

320 M. Kato, *supra* n. 294 and *infra* nn.309 and 310, at 152-154.
321 See '*Fuhō Kōi* (Tort)', *supra* n.302.
322 M. Kato, *supra* nn. 294 and 307, and *infra* n. 310, at 311-312.
323 M. Kato, *supra* nn. 294, 307 and 309, at 410.

discuss a case under the law of obligations.

4. English Common Law and Statutes

Needless to say, English law observes the common law tradition: in other words, common law is case law. Hence, it collaborates with statutes, codes, statutory instruments and the like that are set up for protecting individual legal interest. EC materials and International conventions also have binding force. When seeking civil relief measures, contract and tort by virtue of law are mostly applicable. If two parties are in a specific commitment and one party fails to perform it, this falls within the scope of the law of contract and the other party can claim compensation for losses or injury as a consequence of the breach of contract. Beatson expressed that contract law is the child of commerce in a figurative sense: it has been developed along with the Britain itself from mainly agricultural into a commercial and industrial nation. The definition of "law of contract" is given as:

> "A contract is a promise or set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognises as a duty[324]."

Thus, if there is no contractual obligation between two parties established, any loss or injury occurred is outside of the objective of the law of contract. Such a case mostly falls within the scope of the law of tort. Tort is defined as civil wrongs in simple words[325]. Harpwood applied Winfield's definition to explain the law of tort as:

> "Tortious liability arises from the breach of a duty primarily fixed by law; this duty is towards person generally and its breach is redressable by an action for unliquidated damages[326]."

In this context, the possible injured parties are decided as financial institutions or a third party; it may be either a customer of a financial institution or an utter stranger. Taking some simple assumptions, if a customer suffers losses due to negligence of an employee, a financial institution is likely to be liable for the losses based on contract theory; if a financial institution itself suffers losses due to an act of its employee, this is also possible to deal with under contract theory. If an injured party has no contract with a financial institution, tort theory is applicable. As is mentioned earlier, it is for a plaintiff to decide whether a legal action is based on tort or contract; or, if it is possible to plead both[327].

---

[324] See J.Beatson, 'Anson's Law of Contract' (2002) Oxford University Press, Oxford at 1-2.
[325] See A.M., Dugdale (ed.) 'Clerk and Lindsell on Torts' (2000) Sweet & Maxwell, London at 1-01.
[326] See V. Harpwood, 'Principles of Tort Law' (1998) Cavendish Publishing Limited, London at 1.
[327] See V. Harpwood, *ibid.*, at 3

To acquire civil relief measures based on the law of contract, a contract must be made by deed or a simple contract: a bare promise or agreement does not have legal binding force[328]. It goes without saying that the parties involved are legally bound on the terms of a contract: in other words, they are not liable to each other outside the terms. Once a party breaches a term of the contract, it is legally liable for losses of the injured party. The remedies are;

(1) the losses the injured party has suffered;
(2) the right to enforce a perpetrator to complete the contract;
(3) the injunction to restrain the repetition of the breach;
(4) the payment of the sum due under the contract;
(5) a refund of the money being paid;
(6) recompensing for services offered or goods transferred; and
(7) money being awarded.

The first remedy is awarded for all cases, whereas the rest all depend on the case[329]. In this context, the nature of businesses is mostly based on financial transactions and the related business transactions. Considering this background, the major theory denies the possibility of the law of contract being applied. This is because the said law would not be applied unless two parties have an agreement on providing and receiving data storage as well as processing services. The contract theory is hardly applicable in cases of security breaches affecting individuals or other third parties[330].

A civil wrong is defined as a "breach of a legal duty which affects the interests of an individual to complain on his or her own account rather than as a representative of society as a whole[331]." In other words, it is unnecessary for applying the law of tort to have a contract. In reality, parties involved are unlikely to be bound to each other before an incident occurred. The difference between contract and tort is that duties in tort are imposed by law, whereas duties in contract are fixed amongst parties involved. The remedy for tort losses is normally an action for damages to restore an injured party to the situation before an incident occurred based on the aims of the law of tort. This is also different from the law of contract that aims to treat an injured party as if a contract has been performed. There are two remedies for torts: pecuniary and non-pecuniary methods. The pecuniary method is financial compensation. This is divided into five categories;

(1) nominal damages
If an injured party (=a plaintiff) has not suffered a loss as a result of a

[328] See J.Beatson, *supra* n.311, at 73-75.
[329] *Ibid.*, at 589.
[330] See 'Liability for Computer Glitches and Online Security Lapses', *supra* n.306.
[331] See A.M., Dugdale, *supra* n.321, at 1-01.

civil wrong of a perpetrator, the plaintiff receives a very small sum of money. This is mostly a demonstration to show that the plaintiff has won the case;

(2) compensatory damages
This intends to restore the losses or injury of an injured party suffered;

(3) contemptuous damages
It mainly applies to libel cases. An injured party has proved the case but the court wishes to express its disapproval. The amount of damages is normally to be the smallest coin of the realm;

(4) aggravated damages
This applies to a case if the court wishes to express its disapproval of the defendant's behaviour, and;

(5) punitive or exemplary damages
Non-pecuniary method is the injunction recognised as the most equitable remedy in tort. This works effectively in defamation cases in particular[332].

It is said that the majority of tort cases are for negligence. In some cases, it is not necessary to prove fault: it is called torts of strict liability. If it is possible to prove that a perpetrator commits a civil wrong, and an injured party suffers losses or injury as a consequence of the act, strict liability covers the case without imposing the burden to prove. It is very likely to be imposed in specific circumstances, such as a case on liability for defamation[333]. Turning again to negligence, there is a well-known case called *Donoghue v. Stevenson* (1932)[334]. This case involved two parties: a customer (an appellant) and a manufacturer of ginger beer (a defendant). An appellant drank ginger beer at the public house and she found a snail in her glass. The appellant suffered gastro-entities and nervous shock as a result of drinking the ginger beer in which a snail was decomposed. There was no contract between the parties. When the proceeded to the House of Lords, the decision was made in favour of the appellant since the defendant should have owed duty to its customers to offer harmless products. To establish this decision, the "neighbour principle" was introduced: this is based on the golden rule that "you are to love your neighbour", and this rule is developed as "therefore you must not injure your neighbour as a result of your acts or omissions". Lord Atkin explained who, in law, could be a neighbour as;

> "...Persons so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when directing my mind to the acts or omissions which are called in question[335]."

---

[332] *Ibid.*
[333] V. Harpwood, *supra* n.313, at 7-10.
[334] *Donoghue v. Stevenson* (1932) All ER Rep 1.
[335] V. Harpwood, *supra* n.313 and *infra* n.323 at 17-19.

This is a monumental decision, albeit this case could be easily settled by the Consumer Protection Act 1987 if it had happened after the implementation of this statute.

In order to seek civil relief measures in tort of negligence, it is necessary for an injured party to prove the existence of three factors: (1) duty of care, (2) breach of duty, and (3) damage.

(1) Duty of care (hereinafter "E1")
A perpetrator must owe duty of care to an injured party. The existence of duty of care is said to depend on foresight, proximity and other factors. The notion of foresight is explained, to find causation between the act or omission of a perpetrator and damage an injured party has suffered. The notion of proximity is similar to that of foresight. It is likely to be easy to prove this since there is no dispute on the existence of duty of care in the vast majority of negligence cases. The problems are in proving the following two issues.

(2) Breach of duty (hereinafter "E2")
It is the fact of whether a perpetrator breached duty of care or met a standard level of duty of care when undertaking an act in question. A standard level of duty of care varies depending on the circumstances.

(3) Damage (hereinafter "E3")
It is the fact of whether causation exists between the breach of duty and the damage. If the damage is too remote from the negligent act or omission, it fails to prove the existence of this factor[336].

The burden to proof is, as in Japanese Civil Law, on the plaintiff. It is critical to know which formula the courts employ to judge the standard of care in a specific case. The main formula is called the "reasonable man" test that is explained as "a device" for judges to make a decision on a case on the grounds of policy or expediency. If a perpetrator failed to act as a reasonable man would have done in the same circumstances, his act is to be judged as negligence[337].

Negligence is not the only one possibility for establishing the existence of torts. A criminal offence could be the object of the law of torts: there are circumstances when it is better to deal with the offence from different aspects other than negligence, such as wrongful interference, deceit, statutory misrepresentation and so on[338]. To date, a criminal conviction is recognised as a *prima facie* of a civil case although the criminal conviction was not able to be submitted as evidence for a civil

[336] V. Harpwood, *supra* nn.313 and 322, at 19-23, 27-28.
[337] There is no jury in negligence cases; so judges have to make a judgement alone. *Ibid.*, at 101-102.
[338] See D. Campbell, R. Halson and D. Harris, 'Remedies in contract and tort' (2002) Butterworths, London at 551-552.

case due to the strict rule of common law separating criminal and civil processes[339].

The constituent elements of torts in both countries are evident and there are some similarities and differences. In the first place, examining the similarities, it is satisfactory in English law to prove that an act violates the duty of care that a perpetrator owes to an injured party: this has mostly the same meaning as the Japanese second condition that it is necessary that the perpetrator's act infringes another's rights. Although there is no word "rights" in English conditions, another's right would be harmed as a consequence of breach of duty. So this understanding is not unreasonable. Secondly, the third conditions of both laws express the existence of losses. Furthermore, the third English condition fulfils half of the Japanese fourth condition. That is to say that the damage must have causation with breach of duty (in the English conditions) or the infringement of another's right (in the Japanese conditions). However, the other half of the Japanese fourth condition, requiring the causation between the infringement of another's right and the grounds of an act, is not mentioned in the English conditions. This is because, unlike Japanese Civil Law, it is not necessary to prove whether an act in question occurred through negligence or with intention. This should be noted as the biggest difference between the two countries for proving the existence of torts. However, in some cases, the existence of malice or wilful intention is required.

Having observed both the Japanese and the English law, it is now necessary to deal more carefully with the three questions above-mentioned and their connection.

5. Protecting Rights

5.1 Protecting Proprietary Privileges

As was previously mentioned, there are several legal interests that are vulnerable in cyberspace. Examining the possibilities of seeking civil remedy, it is further practical to focus on how each legal interest is protected by law rather than judging the type of offences. The first case to be examined is legal interests that are supposed to be protected by proprietary privileges.

Proprietary privileges are one of the central objects of Civil Law. There are some specific legal interests that have absolute protection of rights. They are, for instance, life, health, freedom, proprietary privileges and other property rights, and intangible property. In general, they are promised exclusive rights to an owner. Hence, judicial precedents seem to have been willing to agree with the claim of the compensation for losses

[339] See W.V.H. Rogers, 'The Law of Tort' (1994) Sweet & Maxwell, London at 5-7.

if negligence or intention of a perpetrator's act is proved[340].

Referring to incidents occurring in cyberspace, the potential objects of the proprietary privileges to be acquired are computer hardware and money.

5.1.1 Computer hardware and network computers

Excluding natural perils (such as earthquakes and tidal waves), accidental perils (such as fire) and any incident beyond control (such as war and terrorist attacks), there are still some possibilities of computer hardware and related equipment becoming physically out of order[341]. Scenario 1 is to assume an incident wherein an employee P may spill liquid on computers belonging to company X (employer) through negligence. This incident would also be caused intentionally by P; however it is hardly possible for a third party Z to damage computer hardware physically by negligence in particular, unless Z has access to X's premises. It is hardly possible to believe that financial institutions permit an unauthorized person to enter their premises; if it is necessary, a person should be attended by an employee. If P trespasses on X's premises and damages computers with intention, P is penalised for intrusion into a structure and destruction of property under both the Japanese and the English law. They are obviously not defined as computer crime or cybercrime, so they are irrelevant to the main object. In terms of a potential intentional case, a hacker Y can physically damage X's computer hardware and the like by sending computer viruses — malicious codes in particular — through computer networks[342]. It is a criminal offence in both countries: a hacker physically breaks X's property with malice (this fulfils the conditions J2) and the damage evidently exists (this fulfils the conditions J3 and E3). If considering a case in the English law of tort, the act is likely to be defined as wrongful interference with goods. This incident is judged as an intentional offence whether or not Y had expected ahead of time that X's computer would be physically broken by Y's act (this fulfils the conditions J1). This also applies to a case of P introducing malicious codes to destroy computers with intention. As this is an offence, it goes without saying that causations between J1 and J2 as well as J2 and J3 are proved. So, this incident falls in the scope of Japanese Civil Law. In regard to the English law, this offence falls in the scope of torts on account of a criminal conviction being a *prima facie* in a civil case.

---

[340] M. Kato, *supra* n.294, at 200.

[341] Mechanical failures and mere theft are also out of the thesis' scope since they are not defined as cybercrime.

[342] The author is grateful to Mr H Emura, Senior Researcher, Mr H Fujita, Senior Researcher, Mr H Ogura, Manager, Security & Audit Research Dept., Mr K Taniguchi, Senior Researcher, Mr M Tachikawa, Senior Researcher, Electronic Banking Research Dept., and Mr S Watai Senior Researcher, General Research Dept., of the Centre for Financial Industry Information Systems (Japan) for their invaluable comments and advice.

However, what if Z (=a third party) or P (=an X's employee) unknowingly introduces malicious codes through X's computer networks? Such problems are liable to happen frequently when P opens a contaminated email and malicious codes spread throughout the X's whole computer system. It is not important who initially sent the contaminated email in this context. When P opens the addressed email to read, it causes P to commit an error accidentally. However, it is unlikely for X to bring a lawsuit against P in both Japan and the UK. This is because it is a duty of employers to install computer security measures for all computers being used for daily business. To date, it is no exaggeration to say that installing anti-virus software is the minimum level of common practice when utilising computers and networks. Thus, if P receives a contaminated email by viruses through conducting business, it is no wonder that the incident is considered a result of X's negligence.

Such malicious codes can be infectious not only through opening emails but also by other channels involving a third party Z. It is not a rare case that newly purchased computer software, parts for upgrading (such as extended memory) or even a brand-new computer from Z has computer viruses standby. There are some examples: In 1994, Fujitsu announced that its shipped computers had contained computer viruses. In 2001, Compaq found a computer virus called "PE W95 CIH V1.2" (popularly known as "Chernobyl") in a compact disk attached to the shipped brand-new computers. In 2002, IBM published the statement that a part of shipped 32MB memory had contained a computer virus called '"wyx"[343]. Each company took suitable action as soon as they found the problems. If X purchases any product containing computer viruses from Z, Z owes X warranty against defects because of the defects of Z's products in both Japan and the UK. These types of incident are very likely to be well taken care of by a manufacturer. If it is necessary to seek legal action, this can be dealt with by either "torts" or "breach of contract" under the English law, and "torts" or "default on an obligation" under the Japanese law. When purchasing goods from Z, a contract is formed between X and Z.

As was mentioned earlier, proprietary privileges have absolute protection of rights. Therefore, it is difficult to consider that the process of claiming damages for losses would not progress smoothly in all cases mentioned above. In the latter cases, X needs to prove the fact that damages on computer hardware are caused by nothing but computer viruses in both laws (to fulfil the conditions J4 and E3). It would not be difficult as long as X has a department to deal with computer security and computer security policy for the whole company. For instance, in the case

[343] See '*Fuseipuroguramu no haifukeiro* (A distribution route of mal-computer programme)', <http://cherry.webdos.net/~blueskv/virii/haizen.html>, '*PRESARIO 229x sirîzu gokounyû no okyakusama he* (To whom purchased PRESARIO 229x computer series', <http://www.compaq.co.jp/support/presario/info/service/pre_v.html>, and '*IBM no USB memori ni uirusukonnyû no kanôsei* (A possibility of containing computer virus in IBM USB memory)', <http://www.zdnet.co.jp/news/bursts/0201/29/10.html> (print out on file with author).

of computer viruses' attack, even if negligence or intention of a perpetrator is obvious, if X has no defence measures, the relevant court would not simply give a favourable judgement for X. This is because judging from the actual circumstances of this computerised world, it is appropriate for any company using computers and networks to have a security policy or countermeasures to avoid risks to some degree.

In relation to the amount of damages, it is relatively easy to estimate the damages in cases of computer hardware losses. The value is simply found by multiplying the number of damaged equipment by the market price of a computer or equipment. As is shown, there are three types of perpetrators in this section: P (=an X's employee), Y (=a hacker, i.e., an intentional third party) and Z (=a third party). P and Y are very likely to be individuals although they may be part of a conspiracy. P can be either an individual or a corporate body. In general, it is almost impossible to seek a huge amount of monetary compensation from an individual. This applies to any case or any legal interests being harmed. Taking a hacker case, Raul, Volpe and Meyer explained that:

> "...any recovery collected would likely be small, as hackers often lack the financial resources to make an injured party whole in the wake of an attack[344]."

In July 2002, the American Internet service provider EarthLink won US $24 million in a claim against K.C. "Khan" Smith who spammed against EarthLink. However, it is very doubtful whether Smith has funds to pay out $24 million. EarthLink spokeswoman commented that,

> "While we don't know if we'll recover any monetary damages, for us, the victory is in being able to take steps that help stop spam[345]."

In reality, an injured party does not lose a right to claim for damages even if a suspect is unidentified. If that is the case, it is, without any doubt, impossible to exercise rights. So, it is technically necessary for a plaintiff (=an injured party) to know the postal address of a defendant (=a perpetrator) to send a petition[346].

If an injured party believes that suing a perpetrator works to deter further offences being committed, it would be worth trying to do so. Neither the Japanese Civil Law nor the English law of torts aims to deter a further offence being committed. It is true that the effect of deterrence exists in the said law in the process or as a consequence of the law. But,

---

[344] See 'Liability for Computer Glitches and Online Security Lapses', *supra* n.306.
[345] See 'Earthlink wins $24 million from spammer', <http://zdnet.com.com/2100-1106-945169.html> (print out on file with author).
[346] See '*5 syô. Hidaitodoke, Sosyô, Sousa* (Chapter 5. An incident report, a lawsuit and investigation)', <http://www.web110.com/roppou/roppou4.html> (print out on file with author).

their principal aim is to compensate the loss an injured party has suffered. In reality, it is not difficult to find a suspect in some cyber cases like the case of EarthLink. If a suspect is found, there is still a possibility of getting a part of compensation even though it is impossible to get the full amount. On the contrary, if it is a hacking case, it would not be worth suing hackers. In many cases, hackers cannot be identified. Even if a suspect hacker is identified, it is not necessary that he/she is in the same jurisdiction because of the nature of cyberspace. Unless an injured party is well prepared to bring a civil action against a suspect located in a foreign country, they are unlikely to succeed in the attempt.

As is mentioned earlier, the injuries against computer hardware and the like may be the easiest to estimate in terms of the size of damages. Therefore, in comparing the upcoming cases discussed later, it seems to be possible for a perpetrator to compensate for this type of damage as long as the size of damages does not reach astronomical figures. Of course, it depends on to what extent computer hardware is damaged; for instance, if computer viruses being introduced damage all computers in the intranet in a large company, it may not be possible to be compensated by an individual. However, computer viruses are, in many cases, very likely to damage computer software, data and the like rather than computer hardware. Thus far, it is unlikely to happen that computer viruses damage all computer hardware in the intranet in an instant.

5.1.2 Money and its equivalent

Before pursuing a further analysis of cases in relation to money, it is critical to confirm the form of money in this context. Due to the nature of cyberspace, money cannot be a physical substance in cyberspace. For instance, a traditional embezzlement is not within its scope, because there is no physical matter or mass in cyberspace. Money in cyberspace is mere digital signals that are handled in computers. However, such digital signals are based on actual money a client deposits in. Thus, other similar monetary legal interests, such as electronic money, are also equally vulnerable.

When analysing cases of money being abused in relation to cyberspace, if there is any case caused by negligence, it would be a data input error by an employee P of financial institutions. Otherwise, almost all cases involving money are committed intentionally (this fulfils the condition J1). That is to say that those cases are to be criminal offences committed by an employee P or a hacker Y against an employer X. Taking a company X (a financial institution) as a direct injured party, whether the perpetrator is P or Y, a third party Z, more precisely depositors in this context, is likely to be involved as an indirect injured party. Possible cases are that (1) P manipulates or alters computer data in order to transfer X's funds or its clients' deposits and savings into P's personal bank account, and (2) a hacker gains unauthorized access to X's computer

system and alters computer data in order to steal money from X.

In terms of possible cases caused by negligence — input error cases in particular — would mostly occur internally. Those cases remain manageable at a company's discretion in general. Unless the damage is huge, an injured party would be unlikely to file a lawsuit. In regard to criminal offences, they are far more serious than that. If P peculates X's company funds by altering internal computer data, P has to reimburse "ill-gotten gains" to X. X is very likely to dismiss P on disciplinary grounds. In this circumstance, X's company funds may consist of both X's business profits and client's deposits if X is, for instance, a bank. It is, however, not practical to identify whose money P actually peculated because there is no sign or seal on money. When an individual deposits money in a financial institution, both parties are in a contract. Depositors do not lose proprietary privileges on their own deposited money when depositing, whereas financial institutions have obliged depositors to earn interest by using the fund. The fund here means an aggregate of all clients' deposits and business profits. Even if P abuses computer data to steal money from the aggregate deposits, it is hardly possible to discriminate whose money is stolen. After all, the stolen money is the funds under the financial institution's control, not any individual's. Any client would not be refused to withdraw money from his or her own bank account after money is stolen. Hence, the said case hardly involves a third party as a direct or an indirect injured party. On the contrary to this, a third party Z would be involved in a case to some degree if an employee P manipulates a specific customer's bank account information in order to withdraw money. It goes without saying that a hacker Y could perpetrate the same act from outside the Intranet. An incident having characteristics of both cases happened in October 2001 in Japan.

A then employee of Citibank, K. Okada, got some ten clients' personal information, such as names, account numbers and birthdays, by dishonest means during his contract period from June to October 2001. Okada deduced passwords from the information he had got and gained unauthorized access to two customers Z as he impersonated them. Between October 2001 and January 2002, he withdrew approximately 3.7 million yen (equivalent to £21,764[347]). This case humiliated Citibank, who had expressly stated its tight computer security in offering Internet banking services to costumers. Those passwords revealed were said to have been based on birthdays. Okada obtained information internally while in contract but did not use the Intranet to practice fraud: to avoid the discovery of the offences, he used computers in Internet cafés. There are at least two problems disclosed by this case: firstly, the comprehensive computer security policy, including compliance and training for employees, was not enough to prevent such abuse. This incident could have been avoided if Citibank (company X) had introduced a more comprehensive

[347] The exchange rate: £1 equivalent to approximately 170 yen.

policy throughout the entire company. Secondly, Citibank should have warned customers against using birthdays as a password. Today, it is generally accepted as best to avoid using birthdays as passwords; at least financial institutions are in reasonable positions to propose that their customers change passwords if they are the same as birthdays. So, it is possible to bring a civil case against the said bank for negligence or breach of duty of care[348].

In such cases, a victim would notice fraud being committed against their bank account before company X discovers unauthorized access to the services through the Internet. It is no wonder that X does not (to keep up its good reputation) want a fraud case to become public. In this circumstance, X is no longer able to conceal the fact, at least not from the injured customers. However, the final consequence would not be different from a negligent case above-mentioned. X is fully responsible for any monetary damages under its control. Thus, in the Citibank case, customers Z's monetary losses technically would be recovered by Citibank. It would be possible for Z to claim compensation for interests while 3.7 million yen was out of their bank accounts. Finally, as has been previously mentioned, Z is in a good position to bring a lawsuit against Citibank for the reason that it neglected proper duty of care. Z would obtain consolation money if a court accepts Z's complaint. When Okada was prosecuted in May 2002, the contract between Okada and Citibank had already expired. So Citibank could not dismiss him; however Citibank was supposed to claim compensation for damages against him. It was not disclosed whether Citibank claimed consolation money against Okada himself or a mediate company that intermediated between him and Citibank, if any.

If the same offence is committed by a hacker Y, a total stranger to a company X or a third party Z, nothing would be different from the said cases for Z: as Z's money was kept under X's control, X realistically would compensate Z for the losses. On the other hand, the situations seem to be harder for X. No action could be practically taken until Y's identity was revealed. It is impossible to say that all hackers are apprehended for various reasons after their offences are discovered. It is sometimes due to technical difficulties, territorial barriers (as was previously mentioned), or other problems. Hence, the losses caused by hackers are, for financial institutions that are in the position of company X, more at risk than any other cases as they are unlikely to be compensated.

Considering the position of the English law on the same cases,

---

[348] See '*Netbanking akuyou, Beiôtegin de sagi, Anzentaisaku saigo ha hito* (The abuse of Internet banking, a fraud in a major US bank, the last resort of safety measures is 'human beings')', <http://www.yomiuri.co.jp/bitbybit/bbb07/261701.htm> and '*Netbanking de hakensyain ga yaku 370 manen sasyu, Keisichô* (A temporary staff obtained 3.7 million yen by abusing Internet banking, The Metropolitan Police stated)', <http://www.mainichi.co.jp/digital/netfile/archive/200205/10-2.html> (print out on file with author).

employers incur vicarious liability for the torts of their employees. If an employee P is the perpetrator and P commits an offence in the course of employment, a financial institution X is liable to the third party Z who suffered damage. On the other hand, it is possible for X to seek compensation from P based on the *Lister v. Romford Ice* principle[349]. Although there is a grey area whether an independent contractor is defined as an employee, each statute gives a different approach[350]. If a perpetrator is a hacker Y, Z would sue X in relation to breach of duty of care: X neglected implementing a sufficient/reasonable level of computer security, thereby Y succeeded in abusing the system and the outcome is Z suffering the damage. X and Z are unquestionably bounded by a contract. So there is an alternative for Z to sue X in breach of contract.

5.2 Protecting Intangible Property

Intangible property is sometimes understood as equivalent to intellectual property. In this context, intellectual property is more in the realm of exact words. As was mentioned earlier, intangible property rights also enjoy absolute protection of rights. Above all, intellectual property in Japan is protected under Copyright Law, Design Law, Trade Mark Law, Patent Law, Utility Model Law and so on. All of them establish the right to demand injunction: in Japan, Article 112 of Copyright Law, Article 37 of Design Law, Article 36 of Trade Mark Law, Article 100 of Patent Law and Article 27 of Utility Model Law are available. The construction of those laws in general is very similar. After the article on establishing the right to demand injunction, there normally follows the article on conducts regarded as trespass and the article on the estimation of the amount of losses. They do not have an exact stipulation of promising the right to claim damages, however — this is because Article 709 of Civil Law is the authority for the said right[351]. For protecting English intellectual property rights, statutes such as the CDPA , the Patents Act 1977 and the Trade Marks Act 1994 have been established. For instance, Section 96 of the CDPA, Section 61 of the Patents Act 1977 and Section 14 of the Trade Marks Act 1994 are established as rights for owners of intellectual property rights[352].

Both the Japanese Civil Law and the English tort law establish the burden of proof on an injured party. However, it is very unlikely to be easy finding out the factual amount of damage compared to the cases of

---

[349] *Lister v Romford Ice and Cold Storage Ltd* [1957] AC 555. V. Harpwood, *supra* n.313, at 281-291.

[350] Tax law considers the employment status of an individual based on for the purpose of collecting tax. The law of tort considers other aspects, such as moral issues and loss distribution for the sake of a victim in case of an incident occurs. *Ibid.*

[351] M. Kato, *supra* n.294, at 320-321.

[352] See 'Patents Act 1977', <http://www.jenkins-ip.com/patlaw/pa77.htm#s1> and 'Copyright, Designs and Patents Act 1988 (c. 48)', <http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_7.htm> (print out on file with author).

tangible property being damaged. Assume a case of infringement of copyright; the object that the copyright being infringed is supposed to be made use of by many people simultaneously. But it is not necessary to mean that a rightful claimant cannot exercise his/her own rights[353]. Thus, Copyright Law establishes a relief measure for an injured party estimating the amount of the damages. In Japan, Clause 1 of Article 114 agrees that an injured party is able to judge a profit of a perpetrator out of the invasion as a result of his/her copyright being infringed.

If this Clause is not applicable to a case, Clause 2 of Article 114 provides another measure to estimate the damages. It allows an injured party to claim from a perpetrator the appropriate amount the owner is supposed to obtain from executing the copyrights as the same as the losses. English law sounds very complicated compared to this. Instead of sections being established in the statutes, the estimation of losses and injuries depends on common law. Causation, remoteness and foreseeabilitiy are the keys to solving this issue. There are mainly two different types of relief being given: compensatory or exemplary damages. It is said that seeking compensatory damages is common, compared to exemplary damages[354].

The potential legal interests being protected as intangible property rights are copyrights of websites' contents and computer data and the like.

5.2.1 Copyrights of contents of websites

In the first place, there are some hypothetical examples of Copyright Law protection. Nowadays, it is easy to download software online: some of them sometimes are so-called freeware, in other words, the original copyright owner of specific software does not require fees. Although it is free, it is problematic to consider that the owner has renounced the copyright. Some software asks for payment voluntarily. If a financial institution, as a perpetrator, installs certain computer software without paying royalty to an owner of copyrights, it would end up paying compensation for overdue royalties. In 1996, a company in Osaka was sued for illegal software copy into considerable numbers of computers. It paid 140 million yen for compensation, as well as making an apology to a purchaser, to arrive at a compromise (equivalent to £823,529[355]). This is, however, a very primitive issue to discuss. Software administration

---

[353] See '*Chosakuken-singai ni taisuru songaibaisyô ya sasitomeseikyû* (Claims for damages and rights to demand the injunction on the infringement of copyrights)', <http://www.kyoto-archives.gr.jp/copyright/KOZA/koza08.html> (print out on file with author).

[354] The author is grateful to Mr A. Trenton, Solicitor, Taylor Wessing, for his invaluable comments and advice.

[355] The exchange rate: £1 equivalent to approximately 170 yen.
See 'Microsoft Industry Solutions Review: Public Services for Local Government vol.2', <http://www.microsoft.com/japan/PARTNERS/industry/misr/pub2xso2.htm> (print out on file with author).

should centrally be managed without any doubt.

The contents of websites literally mean items on a website: documents, links to other websites, graphics and photos, online software and the like. It is not necessary for the said items to be covered by Copyright Law; for instance, a brand-new model of business (by utilising information technology and the like) presented on a website is also included in websites' contents. When inventing a new model of business, it is to be protected under Patent Law in Japan and the Patents Act 1977 in England[356]. Apart from business models, the Japanese Copyright Law and the CDPA cover the majority of websites' contents. Clause 1 Article 2 of the Japanese Copyright Law gives the definition of the objects of the law: the matter of representing ideas or feelings creatively within the scope of literature, arts and science, the fine arts or music. Hence, there is a theory that it is possible to protect website contents by Copyright Law as long as a website is the matter of representing one's ideas or feelings[357]. In regard to the English CDPA, copyright works are largely classified into three within Section 1:

"(a) Original literary, dramatic, musical or artistic works,
(b) Sound recordings, films, broadcasts or cable programmes, and
(c) The typographical arrangement of published editions. "

The descriptions of Section 1 are prepared in Section 3 to 8. Section 3 explains "literary work" as "any work, other than a dramatic or musical work, which is written..." This literary work includes a table or compilation and a computer programme[358]. Considering the contents of websites, they are within the scope of the CDPA.

However, it sounds awkward to apply this theory for protecting corporate websites in both Japanese and English law. Corporate websites are mostly set up for business purposes. They contain a company name, the logo, the financial report, the online services offered for customers and the like. The issue is whether or not they are to be defined as the object of copyrights. First, considering Japanese Copyright Law, Clause 10-3 of Article 2 gives the definition of database as a structured matter of the aggregate of essays, numerical values, figures and other information being retrievable from a specific data by using an electronic computer. Articles 10 to 13 illustrate with examples of the objects of Copyright Law: Clause 2 of

---

[356] Inventions which are supposed to be protected under Clause 1 Article 2 of Japanese Patent Law means 'An advanced creative work by using the law of nature'. Business models and computer software are technically excluded from this definition. However, it is possible to protect by Patent Law if such business models and computer software are combined with other means, such as Information Technology. See '*Dai-7-kou, IT to business moderu* (Chapter7, IT and Business models)', <http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd> (print out on file with author).

[357] *Ibid.*

[358] See 'Copyright, Designs and Patents Act 1988 (c. 48)', *supra* n.339.

Article 12 defines a database as the object under the law that database which is able to retrieve data and/or has a formulated structure is acknowledged to have creativity, whereby it is to be protected as the object of Copyright Law. Considering these Articles, it is very likely to be able to protect corporate websites with an application of database theory. It goes without saying that a company name is to be protected by the Trade Marks Act 1994, if it is registered. Under the English CDPA, it is possible to acknowledge corporate information published online as literary work; the majority of information or data are likely to fall in 'compilation'. However, the definition of the CDPA has been altered by Statutory Instrument 1997 No. 3032 (the Copyright and Rights in Databases Regulations 1997) (hereinafter "CRDR") in 1998. It suggests changing Section 3 of the CDPA as:

" (a) a table or compilation <u>other than a database</u>;
(b) a computer programme;
(c) (not exist in the CDPA);
<u>(d) a database</u>[359]"

It also gives the definition of database (to insert after Section 6 of the CDPA);

" Databases
3A. -(1) In this Part 'database' means a collection of independent works, data or other materials which -
(a) are arranged in a systematic or methodical way, and
(b) are individually accessible by electronic or other means.
(2) For the purposes of this Part a literary work consisting of a database is original if, and only if, by reason of the selection or arrangement of the contents of the database the database constitutes the author's own intellectual creation[360]."

Under this definition, a corporate website may well be classified as database. So Copyright Law in both countries surely works to protect from being infringed. What about a financial institution X if X's website contents are infringed by a hacker Y? Y is able to get unauthorized access to X's website and abuse the contents, such as deleting or altering them. This is a criminal offence as long as a hacker is involved. So, the legal proceedings are identical to the case previously mentioned in 5.1.1. Technically, to demand the injunction would be the first action for such a case. However, it is very unusual to identify a suspect while the hacker is actually abusing the website contents. Thus, even if X is eager to claim compensation for damages against Y, it is hardly possible to take any civil

[359] The underlined parts are the suggested amendments. Although Statutory Instrument 1997 No. 3032 suggested the existence of (c), there is no section in the original the CDPA 1988. See 'Statutory Instrument 1997 No. 3032', <http://www.hmso.gov.uk/si/si1997/73032--b.htm> (print out on file with author).
[360] *Ibid.*

action against the hacker until the identity is revealed.

In the websites of financial institutions, the services are introduced by using brand-new business models; for example, the Internet banking service and aggregation service[361]. The number of business models or technology being used in such services is likely to be more than one: the services consist of several or a great many business models and technologies. One of them may infringe someone's rights. Assume a financial institution X offers the Internet banking services to its customers and is claimed by a third party Z asserting that one of the technologies being used in X's services is officially registered under the name of Z. If that is the case, not only does X have to compensate for damages but also it is likely to lose the usage of certain technology. This would terminate the whole Internet banking service. The potential losses, including the losses as a result of business interruption, for X would be tremendous. There is no way to continue offering services for X's customers unless X arrives at a compromise with Z (generally paying a sufficient amount of money) or redevelops the Internet banking services without using Z's technology. The latter case definitely takes huge costs and consumes considerable time until the final form of the service is to be ready again. Under this circumstance, X is the weakest link in both the Japanese Patent Law and the English Patents Act 1977. Under this circumstance, X is the weakest link in both the Japanese Patent Law and the English Patents Act 1977: to establish the infringement of the Patent Law, it is unnecessary to prove whether an act occurred by negligence or with intention under both laws. Since a patent is registered and the ownership is evident, it is generally not difficult to prove the infringement of the patents right. Some patents and business models could be the goose that lays the golden egg: that is to say that X is likely to be obliged to pay a huge compensation in case of infringing such intellectual property rights. However, this risk is avoidable, unlike the risks of committing an offence. Before offering new online services to customers, it is surely necessary for X to check the registered patents and business models to know the services are free from infringing upon another's rights.

To protect intellectual property rights, the existing statutes work effectively. The law of torts is unlikely to be the mainstream in this type of case; however, it assists and backs up the statutes at some points. In relation to the infringement of personal rights on websites, the issue will be discussed in depth later in this chapter.

5.2.2 Computer data and the like

"Computer data and the like" are not limited to online materials. In this context, computer data and the like basically mean tangible matters (including computer data and programmes) that are not intended for the

[361] In relation to aggregation service, see Chapter VII.

public. They usually run internally on computers for ordinary business transactions in a company. On the other hand, information that is supposed to be in public, usually data kept in servers, should be defined as "the contents of websites". Thus, even if one can access data online, if it is for individual use or confidential information, it is to be the subject of this section. That is to say that one's personal bank information that one can access through the Internet is to be defined, due to its nature, as computer data.

A possible negligence case would be simple. Suppose there is a financial institution X, its employee P and the customer Z. P deletes or alters Z's financial information by mistake. The restoration must be done promptly. In case Z suffers any loss or injuries as a result of P's mistake, X is liable to respond to the claim. As long as Z is suffering losses as a result of P's breach of duty of care, this type of case would not be difficult to prove a tort by establishing both the Japanese four conditions and the English three conditions. In practice, this type of error is very likely to happen in daily business transactions. Indeed, it is possible to discover an error before the situation becomes more critical (or before Z would notice the error) by having a checking system throughout all internal transactions.

Another example is that, supposing there is a financial institution X and a third party Z, and Z deletes X's data. For instance, there was the case in 1993-1994 in Japan that X made a contract on leasing computers from Z, a supplier of office automation machinery. Z1, the employee of Z, visited X's office to migrate computer data from the old computers to the new ones. While working on it, Z deleted all data from the computers by mistake (this fulfils the conditions J1 and J2). The deleted data was about sales administration (this fulfils the condition J3). Since it is a fact that Z1 deleted the data by mistake, the causations between J1 and J2 as well as J2 and J3 were evident. Thus, X claimed damages based on Article 709 and 715 of the Japanese Civil Law. In contrast, Z brought a rule of contract and maintained that it was not liable for the accident since X was liable to make a backup of data[362]. This is because it is common to have an exemption clause in regard to a backup of data in the majority of contract forms. There was, however, no such clause in the contract between X and Z. Throughout the process of investigating the cause at the court, the evidence that Z mistakenly deleted the data was found in the computer. Both parties arrived at a compromise and Z paid damages to X. Any contract form has exemption clauses to some degree. A contract is generally advantageous to a party who has flamed clauses. In some cases, even if there are exemption clauses, the court is likely to make a decision in favour of a plaintiff if the act in question is judged to be gross

[362] See '*Data-hason no songai-baisyô-sekinin, backup ha user no sekinin?* (The liability for damaging data, is a user liable for making backup?)', <http://www.asahi-net.or.jp/~zi3h-kwrz/law2backup.html> (print out on file with author).

negligence or malpractice[363].

The most serious case is likely to be the abuse of financial information. It would be simple to perform a case analogous to the Citibank incident. P is in a good position to alter Z's data kept in X's computer system to obtain illegal profits intentionally. As long as such personal financial data is accessible to P, it is not necessary for P to have special knowledge on computer security to hack. This is a criminal offence and it is not a brand-new type of offence: on the contrary, it is well known as a fraud or an embezzlement case but using a computer rather than altering an account book. Just letting a computer join with a crime scene for a while, it is thus easy for a perpetrator not only to commit an offence but also to erase all traces of it. A hacker Y could commit the same crime even more perfectly by his/her computer knowledge and skills. So far, there have been no reports of an IT related fraud case that has caused a company to incur astronomical loss. If the losses are within the remit of X's capacity, X is unlikely to look for a civil relief let alone criminal punishment: keeping good reputation is far more important for X. So, if a perpetrator is an employee at the time of the offence, X is very likely to settle the case internally as well as X can, by demanding P to compensate damages as well as to dismiss P on disciplinary grounds. This would be more or less the same reaction in both Japan and the UK.

If a perpetrator is Y, X may have to face the impossibility of having any type of contact with Y. If the identity of Y is revealed, X is able to claim compensation for damages: compensation that Y is supposed to award includes the restoration cost of the computer with the illegal profits Y gained from X. If the offence was to harm X's reputation, the court would also impose compensation on Y. It is easier to establish both the Japanese four and the English three conditions to prove a tort than any other cases when a wrong behaviour is to be a criminal offence. If only it was so easy to identify and arrest a hacker! However, the bigger the losses are, the less likely the hacker, as an individual, could pay compensation.

What if a perpetrator does not damage any intangible or tangible property of X? For instance, it is possible that a perpetrator makes a digital copy of X's computer data without damaging anything. Whether a perpetrator is P or Y, this type of offence is very likely to be committed for the purpose of selling X's confidential information to a competitor Z. In such a case, it is questionable whether X could possibly discover such an unlawful behaviour promptly until X gathers from Z having X's confidential information. P or Y could work as an industrial spy for Z. Otherwise, there is no relation between a perpetrator and Z until the perpetrator approaches Z to sell the information. If a perpetrator is P, X is able to bring a lawsuit as well as dismiss P on disciplinary grounds. Even if it is

[363] *Ibid.*

Y, it would not be impossible to trace Y through the connection between Y and Z. Z is, without any doubt, guilty if Z sends a perpetrator for the purpose of stealing information from X. Even if Z asserts his innocence, it is hardly possible to be judged innocent since Z has been in the position of knowing the perpetrator obtained information illegally from X. This type of unlawful behaviour infringes patents right or copyrights in both Japan and the UK; if a perpetrator makes a copy of data other than patent rights, he/she infringes copyrights of the database.

Although X's property is not damaged directly from the unlawful behaviour, X would lose profits and/or business opportunities that are supposed to be gained by using the stolen confidential information. A perpetrator who actually makes a copy of confidential information would obtain a huge ill-gotten gain by selling it. X has the right to claim damages to P (or Y) and Z on the grounds of Article 112 of Copyright Law and Article 709 of Civil Law (in Japan) and Section 96 of the CDPA (in England).

In Japan, there are some parties who suggest incorporating this treble damages rule into the Japanese existing Law, although it remains to be seen. However, Tokyo district court made the decision in favour of an injured party in regard to the infringement of its patent rights and ordered compensation of approximately 74 hundred million yen (equivalent to approximately £43 million[364]) in February 2002. This is the highest compensation regarding the infringement of patent rights. This court decision underlines the fact that the court showed its initiative to protect patent rights, attaching greater importance to the current of pro-patent[365].

It is useful to use the available US cases to explain "treble damages". In the USA, four out of ten cases granting the highest compensation are the infringement of intellectual property rights. In regard to the case of the misappropriation of trade secrets, it is $114 million for a perpetrator to grant compensation. (Table 3.2) As was previously mentioned, it is possible to impose exemplary damages in the USA, depending on the malice of an offence. In case of the infringement of patent rights, if it is intentional invasion, compensation trebles. This is called "Treble damages" (or triple damages)[366].

---

[364] The exchange rate: £1 equivalent to approximately 170 yen.

[365] See '*Jitsurei ni miru chiteki-zaisanken mondai 33* (The issues in actual cases of Intellectual Property Rights 33)', <http://www.ngb.co.jp/jitsureichizai/jitsureichizai_34.htm> (print out on file with author).

[366] See '*Eiwa tokkyo yougo jiten* (English-Japanese dictionary for the Patents terminology', <http://www.patro.co.jp/EJPatDic/T.html> (print out on file with author).

Table 3.2: Top 10 Verdict of 2002 in the USA		
No	A size of Compensation	Type of offence
1	$ **505** million	Breach of licensing agreement; MD (Jan. 10)
2	$ **500** million	Breach of contract; CA (June 24)
3	$ **276** million	Fraud; MD (March 26)
4	$ **170** million	Fraud; CA (April 16)
5	$ **150** million	Product liability; OR (March 22)
6	$ **135.8** million	Breach of warranty; MN (Feb. 14)
7	$ **122** million	Products liability; AL (May 2)
8	$ **118** million	Breach of contract; MO (March. 15)
9	$ **114** million	Trade secrets; CA (Feb. 1)
10	$ **100.36** million	Wrongful death; NY (Feb. 15)
(Resources: See 'The National Law Journal (web edition) as of August 2002', <http://www.nlj.com/> (print out on file with author).		

In the UK, as was previously mentioned, exemplary (or punitive) damages is one of the types of damages. However, *Rookes v. Barnard* (1964)[367] showed the basic concept of imposing exemplary damages i.e., that it would be awarded in specific and exceptional cases. There are three categories that exemplary damages potentially would be awarded:

(1) If a perpetrator is a "servant of the government" behaving in an unconstitutional way;
(2) If compensation payable for an injured party is less than the profit a perpetrator has made from the tort, and;
(3) If some statutes permit imposing exemplary damages[368].

In practice, it is likely to impose exemplary damages in case the police are involved under the category (1). Compared with the American cases, it is less common in the UK.

5.3 Protecting Domain Name System

Domain name system (hereinafter "DNS") is usually explained as an online address. After getting access to the Internet, it enables browsing any website by typing the domain name in the Internet browser software (such as Internet Explorer or Netscape). Assume there is an example, <http://www.ABC.co.uk/>. Technically speaking, domain name is "ABC.co.uk" in this case, and "www" is called sub-domain. Three pieces of of information are surmised from it at least: This is an Internet address for a company called ABC registered in the UK. There are obviously three parts: "ABC" as third level domain, "co" as second level domain and "uk" as top level domain. The top level domain has two different types (gTLD, such as ".com" or ".org" and ccTLD, such as ".jp" or ".uk") and it is basically arranged, depending on the state of an applicant, so that there is

[367] *Rookes v Barnard* [1964] AC 1129.

no right of choice. The second level domain normally shows a type of institution, such as "co" for corporate bodies or "ac" for academic institutions. The third level domain is free of choice for an applicant[369].

DNS is an address used to reach to a website online. An individual wants to have his/her preferable domain name when publishing a website. A corporate domain name is far more serious to choose: a domain name must be very similar to a corporate name so that it is easy for the general public to remember. It eventually helps its businesses to thrive in many ways. A domain name is unique without exception and registering it is based on a "first come, first served" rule. For the purpose of DNS, abuse, a new offence has been established that is called cybersquatting: it means an act to register a certain domain name, which is similar or identical to trademarks of a famous enterprise or institution, for the purpose of a resale or harassment. As it is unique, if a company ABC wants to register its website as <http://www.ABC.co.uk/>, it is unable to do so if someone else has already registered it. This has been one of the frequent problems online.

Without knowing the exact website address of a specific company, it is possible to find it out by using search engines. There was a dispute in the USA between Playboy Enterprises Inc (hereinafter "Playboy") and Calvin Designer Label (hereinafter "CDL"). Playboy has registered "PLAYMATE" and "PLAYBOY" as trademarks and CDL deliberately registered domain names as "playboyxxx.com" and "playmatealive.com". Moreover, CDL used the said words in meta-tags, which brings the general public to CDL websites when conducting searches by the words "playboy" or "playmate" in search engines[370]. To avoid leading customers to a wrong website, well-known companies often bring a lawsuit to confiscate a domain name from some other owners. Technically speaking, the majority of big financial institutions must have their own websites by now. No one could bring a lawsuit against those who have already registered; those financial institutions are legitimate entities. However, a fraudster could register a similar domain name. In relation to disputes over domain name, a perpetrator could be anyone. Some of them are ill-intentioned people, but some would be innocent people. In Japan, the Unfair Competition Prevention Law was revised in 2001 and Clause 1(12) and 7 of Article 2 rule that it falls on unfair competition if a domain name is registered to obtain illegal profits or for the purpose of causing losses to others[371].

---

[368] V. Harpwood, *supra* n.313, at 344-346.

[369] See 'What's Domain?', <http://www.uma.nu/domain.htm> and '*Domain no kisochisiki* (The basic knowledge on domain name system', <http://www.solid.ad.jp/solidweb/domain/domain_01.html> (print out on file with author).

[370] CDL also sounds similar to Calvin Klein clothing. It was said to be nothing to do with Calvin Klein. See 'Domain Name Regulation', <http://www.hamiltons-solicitors.co.uk/Domain.htm> (print out on file with author).

[371] See 'Yahoo! Domain'. <http://domains1.yahoo.co.jp/help/13.html> (print out on file with author).

Article 3 establishes a right to claim an injunction, Article 4 for damages and Article 5 for an estimation of the size of losses. So, if the court judges a perpetrator's act to have been based on malice, the perpetrator not only loses the domain name but also must pay compensation. If the court judges that one is innocent and there was no intention to damage others, a company cannot take any further action. There is an institution called the Japan Intellectual Property Arbitration Centre (hereinafter "JIPAC") that has a role to arbitrate two parties in a dispute on domain name. For example, an attorney of Christian Dior, the well-known French fashion industry raised an objection in Japan against a beauty salon called Cut Salon Dior in 2002. JIPAC judged in favour of Christian Dior and ordered the other party to give up the domain name. An attorney of Montres Rolex S.A., a world famous watchmaker, also raised an objection in Japan against a company called Pro-lex. JIPAC judged in favour of Montres Rolex S.A. since there was no adequate cause for the other party. To facilitate JIPAC, a complainant has to pay a fee for seeking arbitration. In the former case, Christian Dior paid 189,000 yen (equivalent to £1,111) and in the latter case, Montres Rolex S.A. paid 378,000 yen (equivalent to £2,223)[372]. The fee depends on the number of panellists working for a case as well as the number of domain names to be discussed[373]. Prior to these cases, J-Phone Higasi-Nippon, a mobile phone company, won its case, and also compensation, in April 2001. A defendant called *Daikô Tûsyô* registered "j-phone.co.jp" in 1997 and made a linkage to J-Phone Higasi-Nippon's website as well as sold mobile phones parts online. The plaintiff claimed the defendant acted in violation of the Unfair Competition Prevention Law. The Tokyo District Court ordered the defendant not to use the said domain name and to pay 2 million yen (equivalent to £11,764) for damages of credibility and 1 million yen (equivalent to £5,882) for the cost of the court costs[374]. Although the amount of compensation in this case was not huge, this is the milestone for such disputes.

In the UK, the Trade Marks Act 1994 provides the two grounds: the infringement of trademarks and an element of unfair competition[375]. It goes without saying that it is required of a trademark to have been registered in the event of suing a defendant party. In *Harrods Ltd v. UK Network Services Ltd* (1997)[376], the plaintiff sued the defendant, who had registered "Harrods" as a domain name, for the infringement of trademarks. The court made a decision in favour of the plaintiff as the defendant was judged to have infringed a trademark of the plaintiff under Section 10 of Trade Marks Act 1994. The most remarkable point in this case was that the court made a decision for protecting the registered trademark without

---

[372] The exchange rate: £1 equivalent to approximately 170 yen.
[373] See '*Nihon chiteki-zaisan chûsai sentâ* (Japan Intellectual Property Arbitration Centre), <http://www.ip-adr.gr.jp/> (print out on file with author).
[374] The exchange rate: £1 equivalent to approximately 170 yen.
[375] See '"Suck sites" and Trademark Infringement', <http://www.kaltons.co.uk/TMandhyperlinking.htm> (print out on file with author).
[376] *Harrods Ltd v UK Network Services Ltd and Others* (High Court, Ch D December 9, 1996), EIPR D-106.

evidence of the domain name being abused[377]. However, *1-800 Flowers Inc v. Phonenames Ltd* (2001)[378] showed a twist. The plaintiff, a US company called 1-800 Flowers Inc runs flower telemarketing businesses worldwide by employing the website as well as a toll free number "1-800-FLOWERS" and the trademark was registered in the USA. The defendant, Phonenames Ltd, had "0800 FLOWERS" in the UK. The plaintiff claimed that it tried to register the trademark in the UK under the old 1938 Trade Marks Act. To explain the details of the services, orders were placed via the regional agents in each country when an order was placed outside the USA. But the actual services were offered in New York after a foreign resident placed an order online. Thus, the English High Court rejected the plaintiff's complaint and commented that:

> "...the mere fact that websites can be accessed anywhere in the world does not mean, for trademark purposes, that the law should regard them as being used everywhere in the world[379]."

The case was proceeded in the Court of Appeal but the decision entirely supported the High Court's decision.

The outcome shows that it is insufficient to judge a domain name, being used worldwide, as applicable in all jurisdictions for accomplishing the purpose of the Trade Marks Act 1994. On these grounds, there is the basic principle that the vast majority of the trademark law is territorial. In other words, the use of registered trademarks is effective in the jurisdiction within the range that the legislation applies, i.e., within the UK[380]. If the plaintiff were to provide goods and services in the UK, it could have successfully registered the domain name as trademark and the court decision could have been different.

Having statutes, such as the Japanese Unfair Competition Prevention Law and the English Trade Marks Act 1994, makes it easy to claim damages or an injunction as long as the existence of the infringement is able to prove what the appropriate section/article explains. To date, it is possible to seek arbitration resolutions by some international supervisory authorities, such as the World Intellectual Property Organisation (hereinafter "WIPO"). WIPO is the organisation that the Internet Corporation for Assigned Names and Numbers (hereinafter "ICANN") acknowledge as an organisation offering standing dispute resolution. They have adopted Uniform Domain Name Dispute Resolution Policy and there are three conditions to meet for making a complaint. The merits are that the cost could be less than bringing a lawsuit and the

---

[377] See 'Disputes & Litigation Over Domain Names', <http://www.kaltons.co.uk/DNdisputes.htm> (print out on file with author).
[378] *800-FLOWERS Trade Mark Application, 1-800 Flowers Inc v Phonenames Ltd* [Case No A3 2000 0052 Chancf, 17 May 2001] IP & T 839.
[379] See 'Domain Names as Trade Mark Usage in the UK', <http://www.kaltons.co.uk/DNasTM.htm> (print out on file with author).
[380] See 'Disputes & Litigation Over Domain Names', *supra* n.364.

decision is made quicker (normally within three months)[381]. In this issue, the biggest concern for companies is, however, to maintain good reputation rather than to maintain an actual domain name. In reality, a dispute hardly costs money. Companies do not want other parties to use domain names that the public might associate with their corporate name. Perhaps this is a matter of pride. In the circumstances, seeking a dispute resolution would be more useful than lawsuits from the enterprises' point of view.

5.4 Protecting Personal Rights

Personal rights normally means rights to protect life, health, freedom, reputation, privacy, a full name, portraits, personal information and the like. The first three (life, health, freedom) have absolute protection of rights, as above-mentioned. Contrary to this, the other items are more likely to bear the nature of reciprocal obligations. Therefore, in case a company brings a lawsuit for the infringement of the latter items, the relevant court makes a decision, after considering all circumstances together, whether losses were truly caused. In other words, even if a company believes that a perpetrator defames its good reputation, the court would not always give a verdict in favour of the plaintiff depending on circumstantial evidence.

A corporate body is different from an individual. So, in reality, it does not have all the rights above-mentioned. In this context, reputation and a trade name are to be the subjects. In Japan, Article 723 of Civil Law establishes the right to claim compensation when reputation is damaged. In regard to protecting the name of a firm, Article 21 of Commercial Law and Article 2 of Unfair Competition Prevention Law protect from infringement. In the UK, the name of a firm is protected by the Trade Marks Act 1994. Otherwise, the law of torts takes care of this issue.

There are two terms in relation to defamation: "libel" and "slander". Under the English law of torts, there are clear distinctions. Libel is a statement in any permanent form, such as writing, recording or speech whereas slander is in a transitory form, such as verbal abuse[382]. There is an argument whether recorded defamatory words a medium (CDs, tapes, etc) is libel or slander: some would say libel as they are in permanent form and others say slander since there is no visual communication for such a medium. Considering the nature of cyberspace, any statement existing in cyberspace can vanish in a second although there is visual communication for this. Online statements can be seen by many people at once. Furthermore, it is not impossible to retrieve or record: it is recorded by printing. Therefore, cyber defamation is defined closer to libel.

In Japan, defamation is dealt with in Criminal Law and Civil Law.

---

[381] *Ibid.*
[382] V. Harpwood, *supra* n.313, at 302-335.

Although Civil Law does not have a specific definition on defamation, it is considered to be the same as Articles 230 and 231 of Criminal Law. It establishes defamation as insulting others or defaming by exposing a fact/truth about others in public unless it is a fact related to public interests. Distributing false personal information is also within the scope. The differences from Criminal Law are that opinions are defined as defamation in Civil Law and it is necessary to prove the existence of negligence of a perpetrator on the defamatory statement in general: the exception is the case of defaming by exposing others' truth in public[383].

Considering the English law, libel may be defined as a crime as well as a tort, whereas slander is defined as a tort. Defamation has a close relationship with reputation. It is said that the law in relation to defamation is more concerned with loss of reputation than insult[384]. In order to take a legal action, it is necessary to prove the statement is defamatory, referring to a plaintiff, and was published by the defendant[385]. Under the law of torts, the burden of proof is on defendants proving the statement to be truth. Unlike Japanese laws, this is because only disseminating false information is to be the scope of defamation proceedings. If the statement is proved to be true, no action is able to be taken[386]. Section 2 of the Defamation Act 1996 establishes the methods of resolutions that a person is alleged to have published a defamatory statement: making a suitable correction or/and an apology, publishing the correction and apology, and damages[387].

For financial institutions as a corporate body, keeping a good reputation is the first priority to running business smoothly. Defamation against a corporate public image has often occurred in using bulletin board system services (hereinafter "BBS"). BBS is very likely to be set up in the websites of individuals, open forums and the like. It is very unlikely to be set up in corporate websites. This is because corporate websites are solely for business purposes: not to provide opportunity for the general public to criticise their businesses. This does not mean that there is no opportunity to express one's discontent with the services that a corporation offers. It is possible to express one's complaint online by using email facilities. Hence, it is hardly possible to assume that a company X could defame an individual or another company Z in this way unless X's employee P defames Z in any BBS. P may write a defaming statement online about Z during working hours. Unless P's defamatory act is judged as being related to X's business, X is unlikely to be judged liable for it. In addition to this, a hacker Y gets unauthorized access to X's computer

---

[383] M. Kato, *supra* n.294, at 238-241.
[384] W.V.H. Rogers, *supra* at 179-180.
[385] B. Harvey and J. Marston, 'Cases & Commentary on Tort' (1994) Pitman Publishing, London at 374-375.
[386] V. Harpwood, *supra* n.313, at 311-313.
[387] See 'Defamation Act 1996', <http://www.legislation.hmso.gov.uk/acts/acts1996/1996031.htm> (print out on file with author).

system and alters data to show a defamatory statement regarding Z. X might be in the position to be blamed for negligence if X has not implemented a sufficient level of computer security so that Y could easily access to X. This theory could work in the USA where liability theory is well developed. It would not be impossible for Z to bring a lawsuit against X (as to vicarious liability for P) in applying negligence theory in both Japan and the UK. However, it is unlikely to adopt it in the Japanese court at this stage. It is not a rare case that Y alters data to defame X. The hacking cases that happened in early 2000 against the Japanese government offices are good examples[388]. Those injured parties were in the position of bringing a lawsuit against Y in civil trial although it has not yet been realised due to the absence of the suspects.

The other possibility of a financial institution X being accused is the misappropriation of personal information of clients. Financial institutions, in particular, are in the position of handling customers' information with careful deliberation. That information is very likely to infringe personal rights, privacy in particular, if it leaks or is handled inappropriately. In the USA, the then President Clinton signed the Gramm-Leach-Bliley Financial Services Modernization Act in November 1999. It establishes that:

> "SEC. 501. NOTE: 15 USC 6801 PROTECTION OF NONPUBLIC PERSONAL
> INFORMATION.
> (a) Privacy Obligation Policy.--It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' non public personal information.
>
> SEC. 502. OBLIGATIONS NOTE: 15 USC 6802. WITH RESPECT TO DISCLOSURES OF PERSONAL INFORMATION.
> (a) Notice Requirements.--Except as otherwise provided in this subtitle, a financial institution may not, directly or through any affiliate, disclose to a non affiliated third party any non public personal information, unless such financial institution provides or has provided to the consumer a notice that complies with section 503[389]."

Disclosure of personal information occurs through negligence or with intention. An operational error of employees as well as computer software/programme errors would cause the outflow of clients' personal information. Another possibility, but an intentional tort, is that a hacker is also likely to break into computer security, steal personal information and

[388] It is impossible to accuse Y of committing unauthorized access in criminal prosecution since Unauthorized Computer Access Law was introduced in February 2000 whereas the series of hacking had happened before the said law came into effect. For the details, see Chapter II.

[389] See 'GRAMM-LEACH-BLILEY ACT', <http://www.finmod.state.tx.us/content/theact/glbatext.htm> (print out on file with author).

sell it to a third party. Considering the difficulty of tracing a hacker, whether a perpetrator is an employee or a hacker, the company where that data is in custody is solely in a position to respond to the claim for damages. However, there is no such regulation in Japan and the Data Protection Bill, which somewhat follows it, yet remains under discussion. Tort or contract theory of Civil Law is applicable as a resolution. In the UK, there is a statute called the Data Protection Act 1998. Section 1 gives the broad interpretation on data, thus data that financial institutions deal with, are to be within the scope. Section 13(1) clearly establishes a right for an injured party to claim compensation damage suffered as a result of the contravention of data by a data controller. Distress an injured party suffers from the act is also within the remit of compensation.

5.5 Protecting Economic Losses

Economic loss occurs when ordinary services stop. It could be because of internal computer errors or external accidents; or due to the interruption caused by a hacker. Whatever the cause, the users of the services are likely to suffer economic losses.

The possible causes are mostly mentioned thus far. They are, for instance, negligence or external accidents, such as a power failure. If financial institutions cannot offer their ordinary online services due to a power failure, it is out of their control. To date, computers and the networks are necessary articles for running businesses. Financial institutions, in particular, provide the services online, such as Internet banking, securities trading and purchasing insurance policies. If the services stop, users of any service would suffer economic losses; the users of securities trading services would suffer far more than any other services due to the nature of business transactions. For online customers in relation to banking and insurance, it is unnecessary, at present, for their business transactions to have a strict time rule.

If the computer system of a securities firm X is shut down for some reason, all the customers, including an individual customer Y, cannot receive ordinary services from X. Is it possible for Y to claim economic losses that Y should not have suffered if X had offered services? First of all, it must be very difficult to verify the amount of losses. Secondly, even if such a case happens, a securities firm would assert itself not liable for the losses, pleading an exemption clause in the contract to shield itself from accusation. In general, all clauses of a contract are valid as long as the parties involved are legitimately signed. The then Tokyo Stock Exchange (currently Tokyo Stock Exchange, Inc., hereinafter "TSE") stated that there was a clause about this issue in the articles of incorporation[390]. However, there is a possibility to be void by the court when it is convinced

[390] The author is grateful to Mr M. Uchiyama, Head of Stock Market Department, and Mr K. Yoshida, Head of Foreign Stock Group, Listing Department, Tokyo Stock Exchange, for their invaluable comments and advice.

that the contract terms are too exacting from a customer's point of view, or they favour a securities firm over a customer[391].

The situation of computer security between a stock exchange and an ordinary securities firm should be different. TSE has an independent computer system from the general public: it has connections with registered securities firms only. Thus, it is said that hacking is hardly possible to be committed from outside the network. Technically speaking, it is possible to commit hacking after hijacking the computer system of a securities firm. To avoid this, TSE gives guidance for member firms to have sufficient computer security policy. In regard to the TSE website, there would not be an impact on the trading system since it does not connect with the system. For a physical backup, TSE has dual computer systems: in case one of the systems is stopped for some reason, it automatically switches on the other system. In Japan, there are two stock exchanges, in Tokyo and Osaka. So, if the conditions are clear, there is another market available for members who registered in both markets in case one stops the services[392]. In reality, the trading system of TSE has stopped several times in the past five years. In addition to the accidental suspension of services, TSE intentionally stops the service, such as a market price reporting system, for the practice of fair-trading[393]. The latter case seems to be common practice, thus, it could be exempt from a lawsuit claiming compensation. Regarding the former case, is it possible for member firms to bring a lawsuit against TSE if it accidentally suspends its services? At least, TSE commented that it had not been sued by any registered member[394].

Judging by the comment of TSE's, the trend in the USA is unlikely to be followed in Japan. Ronald Clark, a resident in California, obtained US $18,000 as compensation due to the failure of ETrade's trade ordering system in 1997. The decision was given by the panel at the National Association of Securities Dealers as a consequence of arbitration. The compensation was paid for the losses that Clark could have gained as assets if he had successfully ordered 3,000 shares in October 1997 — although he corrected the story later that he had intended to purchase 6,000 additional shares of the stock. As a result of their investigation, the panel was convinced of Clark's case[395]. By no means is US $18,000 is huge compensation. However, it is crucial that the court made a decision in favour of a claimant in regard to trading problems. If this would be the

---

[391] See '*Risuku-manejimento toshiteno houmu-senryaku vol.1* (The legal strategy on risk management vol.1)', <http://idc.sun.co.jp:10000/developers/column/column0110_1.html> (print out on file with author).

[392] The information was obtained from the interview with TSE.

[393] *Ibid.*

[394] As of August 2001, *ibid.*

[395] See 'ETrade Loses Tech Glitch Dispute', <http://www.wired.com/news/print/0,1294,20595,00.html> (print out on file with author).

main stream in the USA, it is not difficult to imagine that Japan will follow it sooner or later.

Another type of a serious case is the online abuse of share prices. A famous case occurred in the USA in 2000. Mark Jakob, a then employee of Internet Wire, issued a phoney press release, which caused Emulex's shares to drop by 62% in a quarter of an hour. He earned more than US $241,000 from Emulex trades. It is said that this plunge cost investors $50 million in losses. Jakob was arrested within a week after distributing phoney press release. Furthermore, this incident forced the CEO of Emulex into resigning and brought two lawsuits: one against Internet Wire, the employer of Jakob, and another against both Internet Wire and Bloomberg, the financial news service providers that actually released the information based on the controversial press release. Even if a perpetrator is not in a position like Jakob, it is very easy to cause a similar incident by using Internet messaging services to send bogus information. Titan Corp., a California-based technology services firm, suffered from this type of incident. In the Emulex case, Jakob is the perpetrator and it is reasonable to bring a lawsuit against him. However, he earned only US $241,000, which is far from the $50 million losses of investors. Thus, they changed a spear point at Internet Wire and Bloomberg. Considering the nature of their businesses, it depends whether they had to confirm the veracity of all information before making a story public. The theory is that any publisher, of all stripes, is not legally liable for unwittingly printing inaccuracies. If so, it would be too harsh and the freedom of speech would be harmed[396]. This is proved by the famous case of the Wall Street Journal occurred in the 1980's. The plaintiffs sued it for publishing wrong information, however the suit was dismissed. From the viewpoint of employer's liability, Internet Wire was not involved in Jakob's fraudulent act. However, an American lawyer who is specialised in securities commented that it would be a very weak suit against Internet Wire or Bloomberg[397]. So, the next possible defendant could be an individual broker to be sued. Similar cases are very likely to occur in both Japan and the UK; although information in the USA is more broadly aired than in any other country.

Turning back to Japan, there was a large-scale incident of computer technical failure in 2002. On 1st April, Mizuho Financial Group was officially established following the merger of three different financial institutions. As a result of combining three computer systems into one system with great haste, system risks became tangible: Mizuho was unable to deposit money as instructed, issued a lot of blank receipts,

---

[396] See 'Emulex Victims: Who Can We Sue?', <http://www.wired.com/news/print/0,1294,38581,00.html>, 'Lawsuit Aims at Short-Sellers', <http://www.wired.com/news/print/0,1294,38522,00.html> and 'Stock Hoax Suspect Had Motive', <http://www.wired.com/news/print/0,1294,38552,00.html> (print out on file with author).

[397] *Ibid.*

clients could not withdraw money to pay salary for their employees and so on. As a consequence of the series of errors, the JFSA started to investigate the incident. Some clients have decided to claim compensation. For instance, Kyûsyû Electric Power Company could not withdraw approximately 226 million yen (equivalent to £1.33 million[398]) as fees from its customers and incurred cost extra expense for re-issuing invoices, personnel expenditures and so on. So it stated it had intention to claim at least extra expense to Mizuho[399]. Tokyo Electric Power Company also claimed compensation of approximately 50 million yen (equivalent to £0.3 million), the metropolis of Tokyo claimed compensation of seventeen million yen (equivalent to £0.1 million) and Tokyo Electric Power Company claimed 9.8 billion yen (equivalent to £57.6 million)[400]. This case is classified as negligence since Mizuho was judged negligent regarding sufficient duty of care on the combined computer systems. In addition to this, it is not rare nowadays for a hacker to get unauthorized access to financial institutions' computers. Those attacks tend to be public knowledge from their beginning due to the open nature of the Internet. It is only financial institutions who are unlikely to disclose the extent of damage in public. The website of Kyûsyû bank in Japan was hacked and abused with slangy expressions in 2000. It commented when the fact became public knowledge that it was trying to find out whether any substantial damage had been sustained. At least that bank did not offer Internet banking services at the time of the attacks. Later, Kyûsyû bank re-stated that customer information and bank account information were safe since the Internet services were independent from intranet. Soon after this incident, the website of Kôbe Credit Union Bank, which was operated by Sakura KSC, was attacked and altered. This bank had offered Internet banking services at the time of the attacks, although the Sakura KSC, who delegated authorities from the bank to operate the services, stated the server for the Internet banking services was not the one being attacked by a hacker[401]. Their statements, as public incident reports, sound plausible, albeit some sceptical clients could not have been convinced.

When the cause of an incident satisfies the conditions of establishing the existence of negligence (four conditions in Japan and

---

[398] The exchange rate: £1 equivalent to approximately 170 yen.

[399] See '*Kyûden Mizuho ni seikû he* (Kyûsyû Electric Power Company decided to claim compensation to Mizuho)', <http://www.nikkei.co.jp/sp2/nt26/20020417eimi189717.html> (print out on file with author).

[400] *Nihonkeizai Shimbum* dated 17th April 2002 and also the information is obtained from *the Daily News Mail online* from Infostand (dated 19th June 2002) and *Nihonkeizai Shimbum* (dated 23rd August 2002), (print out on file with author).

[401] See '*Kyûgin-saito, kakikaerareru* (A hacker attack on Kyûgin website)', <http://www.mainichi.co.jp/digital/netfile/archive/200003/24-1.html> and '*Sakura KSC unyou no shinkin-saito, fusei-kakikae higai* (The incidents of unauthorized alteration on the websites operated by Sakura KSC)', <http://www.mainichi.co.jp/digital/netfile/archive/200003/27-4.html> (print out on file with author).

three in England), it is possible for the customers to bring a lawsuit against financial institutions. Unless the court judges it is harsh to charge financial institutions with damages, it would come to a decision in favour of customers. When a tort causing economic loss is a part of an unlawful act, for instance, it is likely to convince the court[402]. Under the English law of torts, it is more difficult to compensate for a plaintiff's financial losses suffered as a result of negligence than losses that were fraudulently caused through the tort of deceit. The law of contract, on the other hand, has no difficulty to do so[403]. Indeed, it is worth seeking civil relief measures under the law of contract if both parties are in a contract.

Whether an incident occurred as a result of negligence or the intention of a potential plaintiff, such as ETrade and Mizuho above-mentioned, losses cannot be compensated without limits. In reality, this is the basic theory to be applied for any case. Losses or injuries on property are acknowledged to be direct losses only. In other words, indirect losses, any damage that does not directly link with the cause, are out of the range of subjects to be compensated[404]. Nevertheless, X is likely to be obliged to compensate a huge amount of damages, especially a company who offers financial services. Furthermore, X would pay enormously for the restoration of its good reputation. This, rather than paying huge compensation, would possibly be the most serious problem for financial institutions.

6. Conclusions

Whoever the perpetrator for an incident or a criminal offence is, it is possible for victims to bring a lawsuit against the subject. Even if a loss is minor or zero physical loss caused (as a consequence of non-tangible property being damaged), the laws are designed to cover the losses. However, in reality, seeking civil remedies is not always successful except when the cases are originally classified as criminal offences. As is evidently shown, financial institutions are often in the vulnerable position of both a victim and a perpetrator at once. As a victim, the more one suffers a loss, the less one could recover the loss. In many cases, a potential perpetrator is an individual, either an employee or a third party, such as a hacker. It is very unlikely for an individual to have money to shell out for compensation. If a perpetrator remains unidentified, seeking damages is only a dream. There is another possibility that a financial institution's actual loss is bigger than the profit a perpetrator obtains through the incident. When being a passive perpetrator, a financial institution is a perpetrator against a third party as well as a victim of an incident that an actual perpetrator committed. A passive perpetrator, a financial institution, cannot expect to obtain damages successfully from the actual perpetrator: the possibilities of the successful acquisition of civil

[402] M. Kato, *supra* n.294, at 197-198, 225-226.
[403] V. Harpwood, *supra* n.313, at 67.
[404] M. Kato, *supra* n.294, at 218.

remedies would not show much difference from the case of being a victim above-mentioned. Contrary to this, the risk of being sued is highly possible as the passive perpetrator. It is likely for a financial institution to face the risk of paying damages. Nevertheless, the biggest concern for financial institutions is not money: it is retaining its good reputation up. Sometimes, to do this, they have to fight in the court when being defamed in particular. Sometimes, to maintain their good reputation, they give up bringing a lawsuit against a perpetrator. Sometimes a lawsuit is brought against them on negligence. In this case, they are likely to face not only damages but also huge expense for reconstructing reputation.

Taking a legal action also costs money in both Japan and the UK. Although it is difficult for an individual to sue a financial institution on negligence due to the cost issue, this is not a serious issue for financial institutions bringing a lawsuit. Furthermore, it is unusual if the case would not take a long time to settle. If a perpetrator is prosecuted in the criminal court prior to the civil court, as was previously mentioned, it is possible for plaintiffs to re-submit evidence, which had previously been submitted in the criminal court, in civil court under English laws[405]. However, this means that a civil action is able to be brought into court after a criminal action is settled.

Apart from the insufficiency of the legal systems, the present laws in both countries are practically applicable to cyberspace-related incidents[406]. However, there are two main factors that make the relevant law useless and fruitless from financial institutions' point of view: firstly it is due to a perpetrator being an individual, there are not enough financial resources available for damages. Secondly, a perpetrator ends up remaining unidentified. Those two factors are not the fault of the law. Therefore, financial institutions may as well try to avoid being involved in an incident, seek other solutions, or both.

---

[405] See T. Atsumi (ed.), '*Soshiki, kigyô-hanzai wo kangaeru* (The consideration on organised crime and corporate crime)' (1998) Chûô-daigaku Syuppankai, Tokyo, at 44-45.

[406] Except the fact there is no appropriate data protection law in Japan thus far.

Chapter V: An Analysis of Available Insurance Products in the Japanese Insurance Market

1. Introduction

What precautions does a company have in place for avoiding financial losses? The rapid evolution of technology in the last two decades has made business activity quicker and more complex but has also increased the risks. A crisis may be just round the corner for any company, and without adequate provision against possible events the CEO are gambling with his/her company's future[407].

One of the many risks facing businesses is computer crime. Hacking, sending a virus[408] via the Internet and Distributed Denial of Service[409] are no longer unusual crimes. According to the FBI, a 15-year-old boy can commit hacking without much difficulty if he has a computer with special software, which he can download through websites[410].

It is not, of course, the role of the private sector to crack down to such crimes; responsibility lies with legislators, the police and the judiciary. The choices facing legislators are either to introduce a brand-new cyber-law or revise the existing law to broaden its remit to include new computer crimes. Either of these options would take a long time to achieve. Businesses expose themselves to a great deal of risk if they take no defensive action until the law regards such actions as a criminal offence.

The 1998 G8 Summit in Birmingham[411], placed great importance on

---

[407] See R. Dembo and A. Freeman, 'Seeing Tomorrow: Rewriting the rules of Risk' (1998) John Wiley & Sons, New York, at 18. They state as
'...When we plan around a single view of the future, we are actually gambling. Sensible planning requires us to consider a multitude of possible events and explore how each one might cause us to react...'
from the Reichmanns' business blunder of the joint venture with George Soros in 1994.

[408] See *Insurance Online*, 'Study: E-Risk Coverage Stagnates' at 12 on 7 August 2000, reporting that the Love Virus (or the Love Bug Virus) damaged computers and equipment in at least 20 countries since May 2000 with damage estimated at 6.7 billion US dollars.

[409] 'Distributed Denial of Service' (abbreviated as 'DDoS') means to overload a server with sending massive unsolicited emails or running several computer-programmes simultaneously in order to make the server unable to provide services. See, The National Police Agency (ed) 'High-tech crime: the fact and the countermeasure' (1999) Tachibana Shobō, Tokyo, at 145.

[410] See *Mainichi Shimbun*, '*15sai no kodomo demo kanou. FBIsousakanbu, net-syakainoyowasa wo siteki* (FBI investigators said teenagers can crash network) ', <http://www.mainichi.co.jp/digital/netfile/archive/200002/10-2.html> (print out on file with author).

[411] It was held in May 1998 in the UK and has placed importance on combating international crime since the 1995 Summit in Halifax; 40 recommendations to combat international crime, provided in the G7 Summit in Lyon in 1996, are very famous. (This was also endorsed by the EU.) In this Summit, combating international crime was placed at the top of the agenda; there were ten basic plans provided, some of them as follows:
1) Setting up a 24-hour contact point in each country to ensure swift co-operation at any time
2) Making sure the law keeps pace with technology

combating high-tech crime. This prompted the Japanese government to introduce a brand-new law called "the Unauthorized Computer Access Law (UCAL)". The Japanese government's concern was that Japan was the only industrialised democracy, out of the G8 countries[412], without such legislation. As a result of this lacuna, hacking had not been recognised as a crime despite the threat it posed. At the end of 1999, it was discovered that most computers belonging to governmental authorities in Japan had been hacked for several months from outside the territory[413]. Fortunately there were no reports of any damage to the private sector where, if server computers had been interrupted for even one day, the damage would have been tremendous.

---

3) Taking high-tech crime into account when thinking about how countries can help each other
4) Ensuring that evidence and computer data are always accessible and that transborder searches can take place
5) Making sure everyone investigating a crime can get the information they need
Because the second clause has not materialised, even if a 24-hour contact point had successfully been set up, the Japanese government would not have been able to cooperate with other countries. In other words, if a person tried hacking into a UK financial institution through a computer in Japan, the Japanese judicial authority could not have arrested him even though the UK government legally requested it. See 'G8 AND INTERNATIONAL CRIME', <http://birmingham.g8summit.gov.uk/crime/> (print out on file with author).

[412] The Japanese government revised the existing criminal law to be applicable to computer crime in 1987, but it was not sufficient to deal with all the various kinds of cybercrime. For example, it was impossible to deal with any illegal activity which did not result in physical damage or a loss under the criminal law. This means that unauthorized access, without causing any damage or loss, was not a crime in Japan until the Unauthorized Computer Access Law was introduced in February 2000.

[413] The year 2000 should have been a memorable year for IT (=Information Technology), because of the implementation of the Unauthorized Computer Access Law and the introduction of guidelines against hacking. Those incidents unfortunately highlighted the weakness and vulnerability of Japanese computer security, and Japan was given the shameful nickname of 'the hacking haven'. See *Mainichi Shimbun*, '*Site shinnyuū: Secutiry-koushinkoku Nippon* (Developing country on computer securityJapan) ', <http://www12.mainichi.co.jp/news/search-news/811991/83T83C83g90N93fc-0-6.html > (print out on file with author).
Those hackers have not been found although the National Police Agency (hereinafter "NPA") found they attacked from outside the territory and were supposed to be ideologists, because they strongly criticised Japan for war crimes in the Second World War. Of course the NPA can never arrest them even if it finds a likely suspect, because the Japanese system does not allow for applying law retroactively under article 31 and 39 of the Constitution of Japan.

Article 31 [*Seitou tetsuduki no hosyo* (Secured fair legal proceedings)]
No person shall be deprived of life or liberty, nor shall any other criminal penalty be imposed, except according to procedure established by law.

Article 39 [*Sokyu syobatu no kinshi and Ichijifusairi* (Prohibition against retroactive penalty and prohibition against double jeopardy)]
No person shall be held criminally liable for an act which was lawful at the time it was committed, or of which he had been acquitted, nor shall he be placed in double jeopardy.

See T. Kobayashi, '*Kenpō* (the Constitution)' (1989) Nihonhyouron, Tokyo at 111 and 259-260, and also 'The Constitution of Japan', <http://list.room.ne.jp/~lawtext/1946C-English.html> (print out on file with author).

The first response to the risk of cyber crime in the private sector is to strengthen security systems. Options also include the use of cryptographs or development of new software to protect information. To this end, there are three areas of industry which profit from the threat of computer crime: the Information and Communication Technology industry (hereinafter "IT industry"), the risk consulting industry and the non-life insurance industry. Companies who were aware that their level of computer security was not sufficient against the threat of cyber crime naturally sought an IT or risk consulting company to check it[414] and where necessary to bring it up to standard. Another self-defensive method available to companies is pooling money to cover any loss incurred as a result of computer crime — not a realistic option due to the difficulty of maintaining sufficient funds to cover all eventualities. These issues will be discussed at length in the following chapter.

These are the conditions out of which arose the business opportunity for non-life insurance companies. They realised that there is a demand for an insurance product that covers cyber risks and could potentially be very profitable. The need for this type of insurance product was further highlighted by the huge accidental hacking incident in the Japanese public sector earlier this year[415].

So far there have been few studies made on this type of product due to the fact that it is a new product [416] and that there is a lack of available data. The rest of this chapter will analyse firstly, the current situation in the Japanese market, and secondly, all insurance products relating to cyber risks. Thirdly, the situation in the UK market is looked at and, fourthly, the Japanese and UK markets are analysed comparatively. Other responses against cyber risks will also be discussed in depth.

---

[414] For example, a Japanese branch of ISS Co. Ltd, the security company, was originally established by ex-hackers in the USA. It occupies 80% of the market share in Japan. It expected to earn two thousand million yen (=about £12 twelve million) by the end of year 2000, which is three times as much as the previous year. See *Mainichi Shimbun* '*Hacking tokuju* (Special hacking procurements) ', <http://www.mainichi.co.jp/digital/netfile/archive/200002/08-1.html> (print out on file with author).

[415] See related footnote No.6 in page 23.

[416] At first, a foreign company in Yokohama began the non-life insurance business in 1859. The first domestic Marine hull insurance company was established in 1879, and the Fire insurance company was established in 1888. The car insurance business started in 1914. Compared with those products, the debut of 'Computer Comprehensive insurance' was very recent, in 1975.
See The Marine and Fire Insurance Association of Japan (ed), 'Fact Book: Non-life insurance in Japan 1998-1999' (1999) The Marine and Fire Insurance Association of Japan, Tokyo.

2. Background

The notions of corporate governance and risk management are relatively new in Japan. To discuss in detail the history of risk management would divert from the purpose of this thesis. However, risk management has become an important issue for Japanese business as there have been many breaches or violations against the commercial code as well as legal cases brought since early 1990. Also several major developments had an impact on the financial industry. These were pricing down the fee for having a shareholder suit in 1993 and introducing a Product Liability Law in 1995. Several major developments in the early to mid 1990's also brought the issue of risk management to the forefront of business. These changes not only made companies and shareholders aware of potential risks but also encouraged shareholders and the general public to take steps against damage. Steps taken by shareholders might include court action although the Japanese are generally much more reluctant to take a case to court than, for example, in the USA. These days "consumer protection" is often discussed in Japan but Japanese industry has run successfully for the last two decades with only perfunctory regard to consumer protection. It is only now that companies are paying for neglecting the issue of consumer protection in the past. However, as modern technology makes the world increasingly borderless it is impossible to close the country and continue to run only domestic business. The borderless business world inevitably forces a company to face all sorts of risks. The most important issue for companies is surely to protect against lawsuits and their costs including liability; in other words legal risks[417].

Ôya defined legal risk management as a positive approach to the theory of risk based on a German Insurance study[418], which is a passive approach to risk management. This is because legal risk management is more likely to contain positive preventive measures before a hazard changes into a peril; whereas insurance is likely to be a passive risk management method to avoid risks increasing after a peril[419]. Even if a company buys fire or flood insurance policies, it does not provide any countermeasures against fire or flood. They minimise the damage that the company suffers when an event occurs. There is no doubt that legal risks are a human moral hazard and not a natural hazard such as flood. If so, those risks must be easier to avoid than a natural disaster. In this

---

[417] They involve three factors: civil, criminal and administrative liability.

[418] Y. Ôya, K. Murayama, & N. Takeuchi (1998) '*Legal Risk Management to Senryaku Houmu* (Legal risk management and strategy) ', Tax and Accounting Association, Tokyo at 6-9 and 15-19.

[419] See M. Kamiyama (2000) '*Hoken no shikumi* (the Structure of Insurance)', Nihon Jitsugyô Syuppan, Tokyo at 36-39. There are three words referring to risk in insurance terminology: hazard, peril and risk. A hazard means conditions or situations which are likely to increase the possibility of an accident or event, a peril means a direct cause of the accident, and risk means the possibility of taking losses caused by the accident. Kamiyama gave fire as an example that combustibles are defined as hazard, that fire is defined as a peril and its losses are defined as risks in a case of fire.

sense the theory above sounds reasonable.

Ôya's definition of legal risk management is broad and includes insurance products. In particular, Directors and Officers Liability Insurance has attracted considerable attention lately due to the Daiwa Bank shareholders' lawsuit[420] of October 2000. It should be mentioned that insurance products that cover legal risks have had their profile raised recently. However, insurance products do not always cover all risks. Cover for liability in particular is not sufficient.

3. Reform of the financial sector

In 1997, the then Prime Minister Hashimoto introduced the Japanese government's reform of the financial sector in the period referred to as the British reform [421]. Deregulation is one reform in the financial sector that has impacted greatly on the non-life insurance industry. Setting insurance premiums is now left in the hands of each company. Other industries, including foreign companies, are able to participate in the non-life insurance market. As a consequence of deregulation, the market will unavoidably become more competitive. This has forced all non-life insurance companies to explore ways to survive and thrive in the market and many of them have arrived at the same solution: merger. The majority of companies who chose to merge presented the news of their mergers to the public as a method of better satisfying their customers' needs.[422] As a result of these mergers, there will be four main insurance groups; Mitsubishi, Mizuho[423], Sumitomo-Mitsui[424], and United Financial of

---

[420] A loss of approximately 1.1 billion US dollars was discovered in Daiwa Bank's New York branch in 1995. The loss was a result of illegal off-the-books dealings by a head of the government bond trading department. He had done the illegal dealings for 11 years since 1984. A group of Daiwa Bank shareholders brought a civil suit against 11 former and current executives of Daiwa Bank at the Osaka District Court. The court ordered the 11 executives to pay a total of 775 million US dollars as compensation on 20th September 2000. See 'Daiwa Bank shareholders' lawsuit a wake-up call for company execs', <http://www.yomiuri.co.jp/index-e.htm> (print out on file with author).

[421] This reform runs five year-span from 1997 to 2001 and has three main objectives;
1. To implement broad market reforms based on three clearly defined concepts; Free, Fair and Global;
2. To establish a beneficial financial market for users
3. To sustain stability of the financial systems.
See 'About the financial system reform (The Japanese version of the Big Bang)', <http://www.mof.go.jp/english/big-bang/ebb1.htm> (print out on file with author).

[422] See press release of the Sumitomo Marine & Fire and Mitsui Marine & Fire Insurance Co., Ltd. 'Formation of New Comprehensive Insurance & Financial Services Group', <http://www.sumitomomarine.co.jp/english/pres20000218.html> (print out on file with author). A similar statement was also found in the article of the press conference for the Tokyo Marine and Fire, Nichido Fire and Marine and Asahi Life Insurance Co., Ltd. See *Nihonkeizai Shimbum* dated 20th September 2000, 'The age of reform in the insurance industry' at 7.

[423] Mizuho group is part of Fuyo group, which has its origins in Yasuda *zaibatsu*. See '*Gendai no Zaibatsu Rokudai Kihyou Syuudan* (Big six financial group at present) ', <http://www.geocities.co.jp/WallStreet/6757/09/09.htm> (print out on file with author).

[424] Sumitomo and Mitsui are two of the biggest non-life insurance companies. The

Japan[425]. All four groups formed part of a so-called *Keiretsu*[426], originating from *Zaibatsu* (=plutocracy), which was dissolved after the Second World War. (Table 4.1)

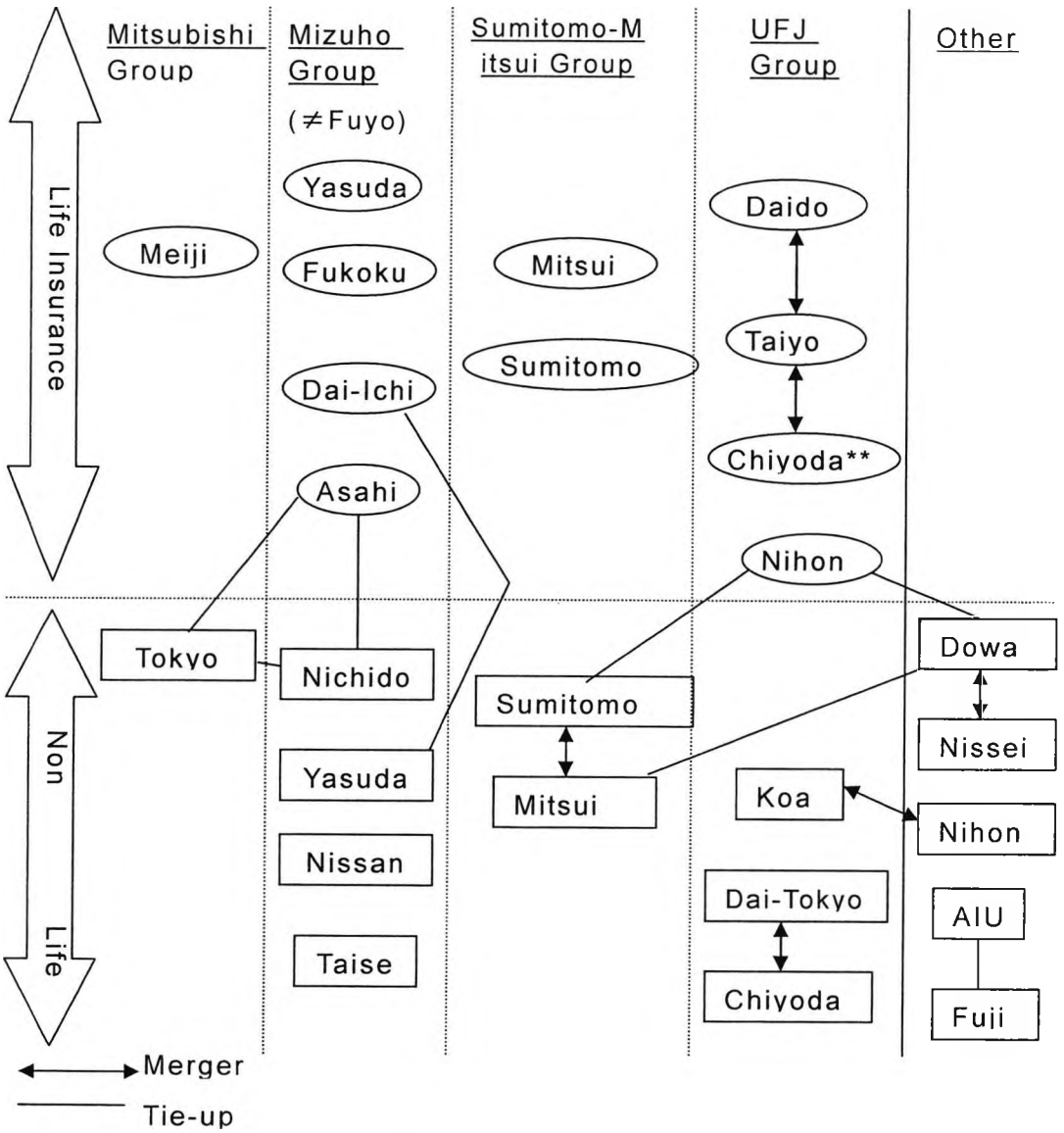
---

paid-in capital of Sumitomo is about £353 million, net premiums are about £3,177 million. As a result of the merger, a new company will have assets of about £34 million and a 17% share of insurance revenues in the domestic market. See 'Sumitomo Marine and Fire Insurance', <http://www.sumitomomarine.co.jp/english/index.html> (print out on file with author).

[425] Abbreviated as 'UFJ'.

[426] There are six big *Keiretsu* at present: *Mitsui, Mitsubishi, Sumitomo, Fuyo, Sanwa* and *Ichikan*. Although the *Zaibatsu* (=plutocracy) system itself was dissolved after the Second World War, the former *zaibatsu* groups built up the structure called *Keiretsu* to cooperate and conduct business with each other. In reality many of the companies in the same group hold each others' shares. See also '*Rokudai Kigyô Syûdan no kisochisiki* (The basic knowledge of six *Zaibatsu*)', <http://www02.u-page.so-net.ne.jp/pb3/keikyu-t/6dai.html> (print out on file with author) and also '*Gendai no Zaibatsu Rokudai Kihyou Syuudan* (Big six financial group at present) ', *supra* n.410.

Table 4.1: The list of mergers/tie ups of life and non-life insurance industries



UFJ=United Financial of Japan

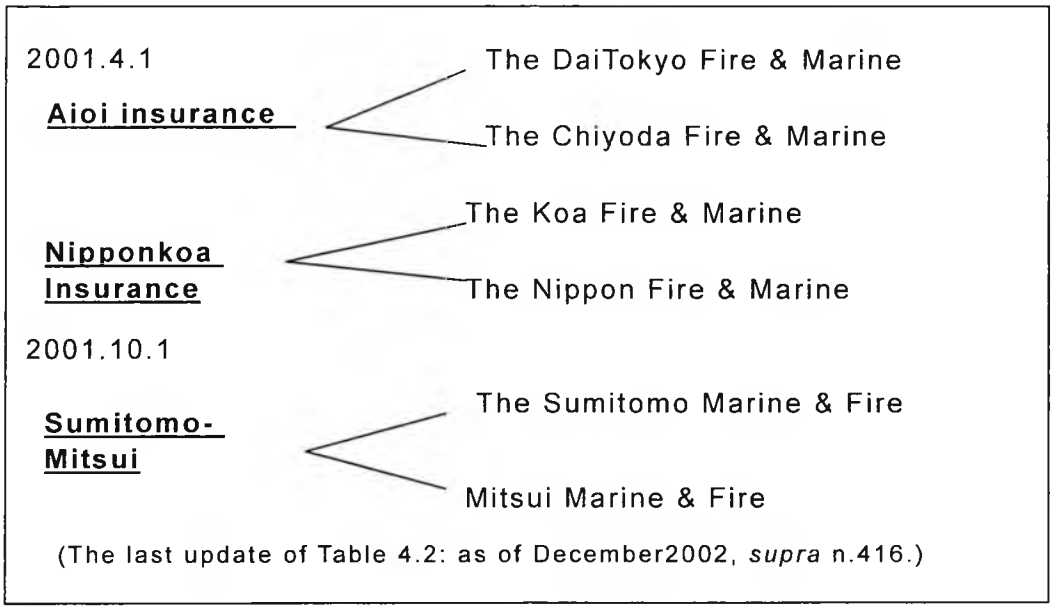
(Reference: *Nihonkeizai Shimbum*, 21 March 2000 at 5, 19 April 2000 at 3 and 9 October 2000 at 3.)

The last update of Table 4.1: as of October 2000.
** Chiyoda Mutual Life Insurance Co. went bankrupt in 2000.[427]

[427] Chiyoda Mutual Life Insurance Co. went bankrupt on Monday 9th October 2000.

In future the mergers and tie-ups will no longer be exclusive to non-life insurance companies but will be liberalised to include other industries as well as financial groups. What impact this will have remains to be seen.

Table 4.2: The schedule of the mega mergers



(The last update of Table 4.2: as of December2002, *supra* n.416.)

Furthermore, the financial sector itself has been changing in Japan, as mentioned earlier in this section. The merger rush seems to have not yet subsided and will come into effect one after another from April 2001.

This is the third life insurer to fail in 2000, and the fifth since 1997. The debt is the largest amongst all bankruptcy cases of any industry; at more than 2.93 trillion yen. Chiyoda Mutual applied for the implication of new fast-track legislation, which was introduced in June, to the Tokyo District Court, and has been discussing with American International Group Inc. (AIG) for help.
See *Mainichi Shimbun*, '*Chiyoda seimei: Kousei Tokureihou Tekiyou wo Shinsei. Sengo Saidaino Tousan* (The largest bankruptcy: Chiyoda Mutual Insurance) ', <http://www12.mainichi.co.jp/news/search-news/809459/90e791e393c90b696bd-0-5.html> (print out on file with author), and also 'THE YOMIURI SHIMBUN/DAILY YOMIURI: CHIYODA MUTUAL FAILS; AIG SAID POISED TO HELP', <http://search.ft.com/Search/MultiSearch/globalarchive.jsp?docId=001011003330&query=chiyoda&resultsShown=20&resultsToRequest=100> (print out on file with author). A brief history of bankruptcy in the Insurance industry in Japan is followed:

April 1997	Nissan Mutual Life Insurance Co.
June 1999	Toho Mutual Life Insurance Co.
May 2000	Dai-Hyaku Mutual Life Insurance Co.
	Dai-Ichi Fire and Marine Insurance Co.
August 2000	Taisyo Mutual Life Insurance Co.

The bankruptcy of Dai-Ichi Fire and Marine Insurance was the first case in the non-life insurance industry in the post-war period. See *Yomiuri Shimbun Japan* dated 1st May 2000 at 1.

(Table 4.2) According to the senior analyst in Japan Rating and Investment Information, Inc., it will take at least five years to get an overview of the financial sector after the financial reform.[428] Although the liberalisation of agent commission in insurance businesses has been postponed at least until March 2003[429], it seems just a matter of time before it is liberalised. Neither the Japanese insurance market nor the financial sector itself seems to be clear about the way forward.

4. The supervisory agency; the Financial Services Agency of Japan

There is one regulating body for the financial sector called the Financial Services Agency[430] in Japan (JFSA). The JFSA was set up in 1998 under the Japanese government's reform. One of its objectives was to enhance the financial services industry's initiatives to promote a free, fair and global market. In other words, it means the governmental authority leaves matters to the market's discretion within a certain legal framework. The JFSA also decided to implement authorisation and notification systems.[431] The authorisation system means that the JFSA authorises any brand-new financial product before a company begins selling it. The notification system means that it allows a company to notify the public (if potential risk to customers is low) about a new financial product by submitting documents beforehand.

5. The related organisation: the Marine and Fire Insurance Association of Japan, Inc.

There are 33 non-life insurance companies[432], several governmental and corporate institutions and associations related to the non-life insurance industry. Such an institution is the Marine and Fire Insurance Association of Japan, Inc. (hereinafter "the association")[433]. It was

---

[428] The author is grateful to Mr N. Uemura, senior analyst in Japan Rating and Investment Information, Inc., for his invaluable comments and advice. He is the author of 'Japanese Life Insurance Industry: Its crisis and the future' (2000) Japan Rating and Investment Information, Inc., Tokyo, and 'Risk management and Insurance Big Bang' (1999) Japan Rating and Investment Information, Inc., Tokyo.

[429] See the FSA website, '*Songai hoken dairiten seido no minaoshi nituite* (Re-constructing agency system for the non-life insurance industry)', <http://www.fsa.go.jp/p_fsa/news/newsj/f-20000524-1.html> (print out on file with author).

[430] The Financial Supervisory Agency was set up in June 1998 under the Prime Minister's Office. The Financial System Planning Bureau, Ministry of Finance, was integrated with this and reformed as the Financial Agency in July 2000. Although it has a strong relationship with the Ministry of Finance, it will remain under the supervision of the Prime Minister's Office. See generally FSA website, <http://www.fsa.go.jp/indexe.html> (print out on file with author).

[431] The author is grateful to Mr K Hori, Insurance division, Supervisory Dept. of the FSA for his invaluable comments and advice. The interview was held on 25th August 2000.

[432] As of May 2000.

[433] The author is grateful to Mr N. Hara, Director and General Manager, and Mr J. Sugita, Manager, International Department, and Mr A. Hozumi, Manager, Research and Development Department 2 of the Marine and Fire Insurance Association of

estabilished in 1946 after hostilities with other similar insurance organisations, and reorganised in 1948 as an incorporated body. The main objective of the association is to promote sound development and maintain reliability in the non-life insurance business. It is composed of thirty-three domestic companies as of 1st June 2000[434], and also has relationships with other non-life insurance organisations[435]. There is no hierarchy in terms of authority amongst these organisations and they have no power to direct or supervise individual non-life insurance companies. That role is played by the JFSA. However, the JFSA has approved the association as a representative of the industry with the expectation that the association gives guidance to the non-life insurance business in a non-competitive manner[436].

6. An Outline of the Computer Comprehensive Insurance Products

In the Japanese insurance market there are many different products produced by each non-life insurance company, for example: "Computer Comprehensive Insurance", "Computer Insurance", "Network Insurance", "Data Processing Insurance" and "Electronic Equipment Insurance". However, the conditions of almost all such products are similar or the same. Thus, the generic term "Computer Comprehensive Insurance" is used in this thesis to refer to insurance products covering cyber risks.[437]

The first computers were developed in 1946 in the USA and they were introduced in Japan between 1955 and 1965[438]. In the early 1970's, the governmental authorities focused on what impact Information Technology could have on the financial industry. Having responded in this way, the idea of an insurance product to cover losses on computers was born in 1975. Thus, one could say that the idea is not an entirely new one. The products sold in 1975 were called "Computer Comprehensive Insurance" and "Data Processors' Liability Insurance"[439], the matrix of the present "Computer Comprehensive Insurance" (hereinafter "CCI").

Japan, Inc. for their invaluable comments and advice.

[434] See generally 'the Marine & Fire Insurance Association of Japan', <http://www.sonpo.or.jp/outline/gaiyo.html>.

[435] For example, the Property and Casualty Rating Organisation of Japan or the Foreign Non-Life Insurance.

[436] From the interview with Mr K Hori of the FSA.

[437] The term "Computer Comprehensive Insurance" was chosen because this has been used in the Marine and Fire Insurance Association of Japan, Inc. In reality many non-life insurance companies simply call a product by this name. Most insurance products cover software, hardware and the Network are included in the word 'Comprehensive'. Details are examined in a later part. See Section Eight.

[438] See Non-life Insurance Research Centre (ed) 'New insurance product' (1999) Tokyo at 130-155.

[439] According to the chronology, 'Data processors' liability insurance' was renamed as 'Data servicing distributors and electric telecommunicators professional liability insurance' in 1988. See the Marine & Fire Insurance Association of Japan (ed) 'Non-Life Insurance in Japan 1998-1999' (1999) Tokyo at101-113.

A devastating fire[440] in Tokyo in 1984 highlighted the vulnerability of urban infrastructure. This prompted the Ministry of International Trade and Industry to request the non-life insurance industry to further develop the existing products[441]. Although the CCI product has existed since 1975, the current type of insurance product was re-developed in 1998. Since 1998, most insurance products have been able to cover the losses incurred as a result of a crime[442] being committed. By May 2000, 23 out of 33 non-life insurance companies had insurance products for computer or network losses.[443]

The conditions for purchasing this insurance product are presented in the form of a questionnaire for each potential client, which in turn checks the existing security system within the said company. If the questionnaire establishes that the level of security provided by the potential client is sufficient, a non-life insurance company has no problem in making the product available. If it is judged to be insufficient, there are three options available: 1) that the potential client must pay an extra premium, 2) it is instructed by the insurance company to raise its security level, or 3) the insurance company may reject a request to purchase its product. Thus, it is possible to say that this computer insurance product has the indirect purpose of raising the level of security.

The majority of CCI products are order-made and tend to be sold to large enterprises. Very recently some non-life insurance companies started to sell ready-made insurance products targeting small and medium-sized enterprises. The other significant feature of this product is that it can be sold through agencies. Small and medium sized companies often purchase it to improve their business reliance for their customers.

---

[440] The fire broke out underground in front of the Setagaya telephone office just before noon on 16 November 1984. It was difficult to fight the fire and finally took 17 hours to bring it under control. As a result of this accident, 220 meters of cable was burned; 88,817 domestic phones, 1,377 public phones became unavailable, a neighbouring four telephone offices suffered because relaying cables were also destroyed. The damage was also enormous in both the public and the financial institutions. 243 branches of the Mitsubishi Bank (at that time) and 63 branches of the Daiwa Bank (at that time) suffered business interruption because online systems were completely damaged. It took nine days to reconstruct. This accident was a typical example of an urban disaster demonstrating the vulnerability of cities in relation to information technology. See '*Setagaya Cable Kasai* (Setagaya Cable Fire: A 100 years of the urban disaster)', <http://xing.mri.co.jp/research/research/bousai/setagayacable.html> (print out on file with author).

[441] Indeed, there was a four-year gap after the fatal fire in 1984 till the Ministries, such as the Ministry of International Trade and Industry and the Ministry of Posts and Telecommunications, requested the non-life insurance industry to develop a product in 1988. Relevant authorities and the industry had a lot of meetings and conferences during the four years, an example of how public authorities take time to reach to a conclusion.

[442] For example, sending a virus, hacking, unauthorized access, and fraud.

[443] Some companies out of ten specialise in one or two products only, such as car and travel insurance products.

The product usually covers four main losses[444]:

1) Damage to computer equipment (both hardware and software)

If any computer equipment, which is listed in the schedule, suffers damage within the territorial limits, the cost of reinstatement or replacement will be covered.

2) Loss of information

If data or programmes on the computer property in the schedule are damaged as a result of accidental or malicious erasure, destruction, distortion or corruption, the cost of reinstatement will be covered.

3) Increased cost of working (i.e. temporary repairs and expediting costs)

Necessary and reasonable additional expenses, which are incurred as a result of business interruption such as accidental or malicious erasure, destruction, distortion or corruption, to continue daily business operations can be covered.

4) Loss of income as a result of business interruption

In cases where it can be expected that company profits are damaged in consequence of business interruption related to 1) and 2) stated beforehand, can be covered in accordance with the schedule. The reduced profits can be calculated as a balance of the operating revenue within the last twelve months before the accident happened, minus the profits to date.

Of course, as with most insurance products, a CCI is composed of two parts: covering property losses and liability for a third party. Thus, in the case of a client being sued by a third party for damages, it is possible to be insured for legal costs including indemnity in accordance with the schedule.

CCI products are in many ways an effective means of covering business losses but they are not perfect. Any loss, which is stated in the schedule, can be covered but the loss must be incurred in Japan. Cyberspace is, by its very nature, borderless and the risks it poses and the potential damage it could cause is enormous. The insurance industry is not prepared to take such a risk and in reality it limits the maximum insured amount to within five hundred million yen (equivalent to £3 million).

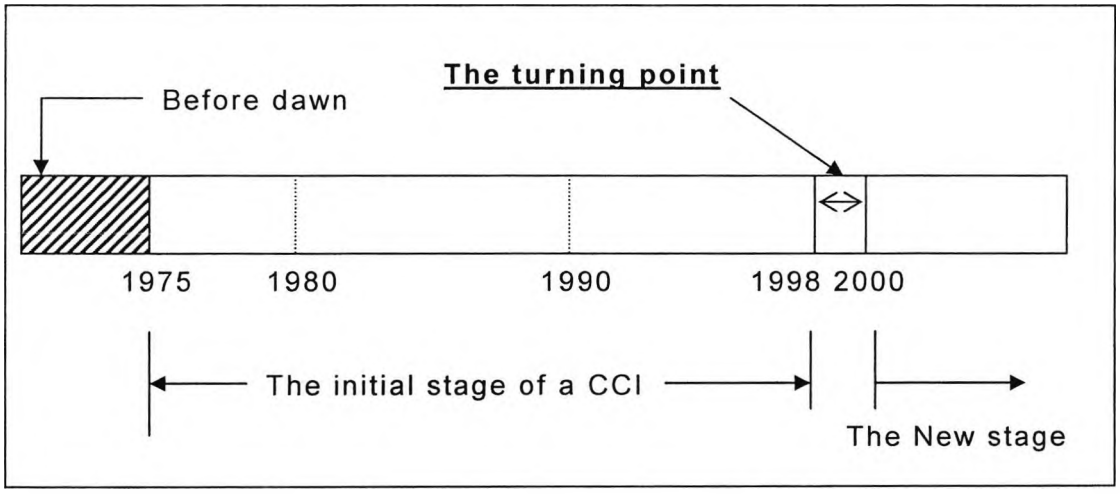
7. The development of CCI products

It is possible to identify three phases in CCI's development. The first phase is from 1975 to 1997 — the initial stage, the second phase is from 1998-1999 — the turning point, and the last phase is 2000 onwards —

[444] Reference from the computer file named "Computer insurance" in the Chartered Insurance Institute, London.

the new era. (Figure 4.1)

Figure 4.1: A CCI's transition since 1975



The first CCI product did not change for twenty years despite the rapid development in technology that was taking place during this period. The turning point was in 1998 after which the CCI products were adapted to keep pace with technology.

The global application of the computer network systems has made the value of information skyrocket. This alters the balance of the two values of information; the value of time and of information itself. In business one might lose a big business opportunity if one does not get certain information by a certain time. This suggests that the value of time is feasibly greater than that of the information itself. Advanced technology manages to make physical distance and time insignificant. One can attend a business meeting in New York "virtually" without moving from one's office in Tokyo. Moreover, cyberspace has been making borders and distance irrelevant. If technology can make "distance" and "time" irrelevant, the real value of information increases to a greater or lesser extent. Therefore, from the technical point of view, the CCI products are an insurance product which reflect the times. But from a coverage and capacity point of view, it is doubtful whether they are sufficient to cover losses in terms of the real value of information.

The initial CCI product in 1975 and the later version (after 1998) are significantly different. The biggest difference between them is derived from the rapid development of computer network systems. There is positive proof to support this. Firstly, many non-life insurance companies have entered into a technical tie-up with a consulting or high-tech company. CCI products are technologically very specialised; therefore it is difficult to develop such a product without assistance from specialists in that area.

Furthermore, those non-life insurance companies tend to entrust consulting or high-tech companies with technological matters including a constant surveillance of the product. The companies provide their know-how and technical skills to non-life insurance companies in order not only to develop CCI products but also to monitor them. It is out-sourcing in a broad sense. Secondly, most CCI products cover the new risks, such as hacking or computer viruses. These risks were not predicted in 1975 in the non-life insurance market. As was mentioned earlier, all provisions of the contracts in the insurance industry have to notify and be approved by a relevant authority[445]. Obviously the above-mentioned risks did not appear in the wording of the 1975 products. Therefore it was impossible to adapt the old product to address the new risks[446], and non-life insurance companies were obliged to make radical changes to CCI products after 1998. Finally, neither "Data Processors' Liability Insurance" nor "Computer Comprehensive Insurance" in 1975 were available to all industries. As the names of the products suggest, they were targeted at limited industries. However, as it becomes an increasingly important tool for running business, many industries are placing an emphasis on technology. Using technology in business is no longer specialised. As a consequence, the range of clients has expanded widely. This seems to be an external factor of the rapid development of the computer network.

8. On-the-spot survey of CCI products[447]

On-the spot surveys were conducted in Japan in both May and August 2000. The target companies were non-life insurance companies, which have already dealt in CCI products. There are in total five leading companies interviewed, which are all listed. Their headquarters are all located in Tokyo and they have broad sales networks throughout the country.

The interview questions addressed four areas: the developing, the composition of, dealing in, and the future of the CCI products. The questions were targeted at the companies' Underwriting or Products and Services Development Departments so their answers tended to be more idealistic and unilateral than those of the Sales Department. Sales Departments have to address the harsh reality of the market whereas Development Departments are able to focus on an ideal product.

The renewed version of CCI products after 1998 can be described as brand-new products, because of their drastic changes and recent technical

---

[445] The approval formerly given by a department of the Ministry of Finance is now given by the FSA (since 1997).

[446] While the analysis is based on the interviews with non-life insurance companies that the author conducted in Japan in August 2000, as agreed with the interviewees no names will be mentioned unless specific authorisation has been given.

[447] The Analysis is based on the interviews conducted by the author in May and August 2000 with the FSA, non-life insurance companies and the Marine and Fire Insurance Association of Japan.

innovation, although they have nearly 20 years' history in the market. In addition to this fact, there are new risks emerging day by day only some of which can be dealt with by the CCI products. Therefore, companies do not yet have a complete picture of how the CCI products are received in the market.

It is generally understood that most property damage[448] is covered under fire insurance. So there is no incentive to focus on property damage in terms of CCI products. Therefore, the motivation for non-life insurance companies to redevelop this kind of product is the new risks, which were not covered by existing insurance products — namely hacking, unauthorized access, and legal risks in cases where a client company is sued by a third party for financial damage[449]. CCI products may appear similar to Products Liability Insurance. Products Liability Insurance substantially covers damage if it is caused by a failure of a tangible product. However, it does not cover any damage on computer software, because computer software is regarded as intangible. That is to say that if a malicious act, such as unauthorized access, causes damage, it is not covered by Products Liability Insurance.

There are mainly three classification methods for CCI products. The first classification method is by its composition, whether it is a package or a single product. The basic elements of a product are: hardware (computer property and its related equipment), software (obtainable at stores and databases belonging to a business such as a clients list.), and increased working cost and/or loss of income as a result of business interruption. It depends on how each CCI product defines it. Some non-life insurance companies are prepared to sell an individual product even if they have put together a CCI as a package product.

The second classification method depends on the client's size, i.e., whether it is a large, medium-sized or small business. In this context, CCI products can be divided into ready-made products and order-made products. An order-made product is generally designed for large business and tends to be expensive. A ready-made product is appropriate for small and medium-sized enterprises. It is straightforward to deal with (so can be sold by agents) and is cheaper than an order-made product. The third classification is by potential clients' industry. The product, which the majority of non-life insurance companies have had since 1975, is, in fact, "Data Processors' Liability Insurance, " although "Computer Comprehensive Insurance" began to be sold at the same time. As was mentioned in the previous section, those products were targeted at limited industries.

---

[448] In this thesis "property damage" restricts damage against computer hardware and its related equipments. Thus damage against covered software (including self-developed software) or data in the computers is not included as property damage.

[449] Based on the interview with the Sumitomo Marine and Fire Insurance Co. Ltd. in May 2000.

Therefore, modifying the CCI products to be appropriate for all industries is another key factor in reshaping them. The choice for the non-life insurance companies is to prepare universal CCI products for all industries, only for a specific industry, or both. Although they are largely similar, each non-life insurance company has its own methods of attracting clients.

8.1 Questions regarding the development of CCI products

8.1.1 On what size of enterprise did your company focus for the CCI products?

The Tokyo Marine and Fire Insurance Co. Ltd. (hereinafter "Tokyo Marine") [450], one of the five non-life insurance companies interviewed, has developed five products since 1998, which are not designed to be specific for any size or type of client. However the different characteristics of each product make them more appropriate for one size of client than another. The reason the company gives for this is that it wants to keep a good balance over its markets[451].

The five interviewees are all major non-life insurance companies and their sales staff cultivates their own clients. Therefore, most of their clients are likely to be large businesses. For these companies it is not difficult to purchase a CCI product despite the high cost. The non-life insurance companies are unlikely to receive a request for an order-made product from small and medium-sized enterprises because of the cost issue. There are bigger potential risks for large companies than those of small and medium-sized ones, so that greater prudence is required in underwriting them[452]. This response from the five non-life insurance companies means that a product, which has big potential risks, always has smaller potential risks, too. In other words, as the Japanese proverb says, "the larger also serves for the smaller". Therefore, the premium of CCI products appears to be fixed, and its ratio is adapted according to the size of the potential risks and the enterprise. Obviously no insurance company can afford to supply an insurance product that might undermine itself, therefore most companies tend to set the maximum sum of coverage for the CCI products at between 588 thousand pounds and £3 million[453]. It is for non-life insurance companies to judge what amount of coverage a client

---

[450] The author is grateful to Mr T. Ichiki, Manager, Corporate Planning Department, and Mr M. Takahashi, Assistant manager, Liability Insurance Group, Commercial Lines Underwriting Department of the Tokyo Marine and Fire Insurance Co. Ltd. for their invaluable comments and advice.

[451] It is, of course, possible for any of the five non-life insurance companies to design a special order-made insurance product for a certain company at its request.

[452] From a business scale point of view large companies are judged to have larger potential risks. However, they are likely to have a sufficient level of computer security which reduces this potential. In contrast, small and medium-sized enterprises have an insufficient level of computer security and so their potential risks are increased and unlikely to be covered by CCI products.

[453] The exchange rate: £1 equivalent to approximately 170 yen.

needs from a product[454]. Equally, each company has its own method of calculating the premium based on the extent of a client's safety measures.

The Chiyoda Fire and Marine Insurance Co. Ltd. (hereinafter "Chiyoda") [455] said that it regards small and medium-sized enterprises as a developing market. Those companies are likely to sell CCI products to enhance confidence amongst their customers, preferring a ready-made product. It is also of benefit to non-life insurance companies to sell a ready-made product as it is non-time consuming and convenient. Despite their convenience however, ready-made CCI products are not currently a leader in the CCI market. There are three principal reasons for this. Firstly, small and medium-sized enterprises believe cyberspace to hold risks relevant only to large companies. Another factor in their reluctance is the cost issue. Thirdly, small and medium-sized enterprises rarely have a sufficient level of computer security and are reluctant to spend time and money raising it to the level required in order for the CCI companies to sell their products[456]. These obstacles between ready-made products and market leadership are not minor ones and therefore unlikely to be overcome in the near future.

8.1.2 Did your company focus on a specific industry for the CCI product?

Although most non-life insurance companies have clients in all areas of industry, the Sumitomo Marine and Fire Insurance Co. Ltd. (hereinafter "Sumitomo")[457] has designed a specific product for the data processing and IT industries [458]. In fact, the CCI providers have a stronger relationship with the IT industry than any other and feel that it is most in need of their products.[459] At the moment the risks for the data processing industry are

---

[454] The five non-life insurance companies are prepared to raise the maximum sum of coverage for 'good' customers within a certain limit depending on the situation.

[455] The author is grateful to Mr F. Ohkawabata, Manager, and Mr T. Matsuura, Chief Underwriter, Property and Casualty Underwriting Group, Products and Services Development Department of the Chiyoda Fire and Marine Insurance Co. Ltd. for their invaluable comments and advice.

[456] See footnote No.46.

[457] The author is grateful to Mr S. Takano, Manager, and Mr H. Okumura, Assistant Manager, Liability Division, Fire and Casualty Department, Mr K. Morita, Assistant Manager, Property Underwriting Division, Fire and Casualty Department, and Mr T. Tsuda, Assistant Manager, Commercial Lines Planning and Consultation Department, the Sumitomo Marine and Fire Insurance Co. Ltd. for their invaluable comments and advice.

[458] For Sumitomo one of the conditions to develop CCI products was whether an industry has specific technical knowledge. It considered the printing industry as having specific technical knowledge and Sumitomo's CCI product covers it (except for intellectual property). Sumitomo is open to developing a similar insurance product for any other industry if it is possible to estimate the risk and if there is sufficient demand in the market. It is very likely to take several years to estimate a risk for computerized business. The interviewees have emphasised that the most important and difficult point in the insurance industry is keeping a balance between measuring the risk as accurately as possible and knowing the market demand.

[459] Some non-life insurance companies tied up with a foreign non-life insurance company or risk consulting company in order to learn from their business know-how and experience. Thus Japanese CCI products were initially targeted at the same

still higher than for any other industry but if e-commerce continues to flourish the risks will be spread over all industries. CCI products are available to all industries and no special treatment is currently given to the data processing industry.

8.1.3 What does your company think is the most important issue for CCI products?

The five companies interviewed responded with two issues they regarded as the most important. These are computer security and risk hedging. In general it seems that non-life insurance companies favour CCI products for risk hedging rather than for the purpose of raising awareness about computer security. A company or organisation may either be reluctant to raise the standard of computer security to a sufficient level because of the costs involved or, because the company is of the view that the security is satisfactory and thereby does not address the issue until there is a breach. Therefore while one non-life insurance company maintained that selling their CCI product enhances clients' awareness (as non-life insurance companies know), marketing a CCI product on the basis of computer security does not necessarily help to sell the product. As mentioned in an earlier section[460], each non-life insurance company prepares questionnaires, which clients have to answer before a product is made available. This is helpful in showing what sort of action a client company has to take to strengthen its existing security measures.[461]

Naturally making a product attractive for clients is the first priority for any profit-making company; in this sense marketing CCI products from a risk hedging point of view is a better way of selling them than from the point of view of raising security awareness. As Mitsui Marine and Fire Insurance Co. Ltd. (hereinafter "Mitsui") [462] clearly stated, a major reason for providing business insurance products is to support and enhance economic activities, not only in terms of the client's industry but also the non-life insurance industry itself. Therefore any product must directly contribute to a stable economy.

Liability is another major reason for purchasing a CCI product. Large companies are likely to purchase them as a means of reducing a

---

specific industries inside Japan and were developed on the knowledge of the said foreign company. The selling of CCI products to the IT industry is a good example of this.

[460] See section five (An Outline of the Computer Comprehensive Insurance Products).

[461] However, it is possible to say that companies which are interested in the CCI products have already received a danger signal about their security level. Those companies should have adequate awareness in regard to security. It is not difficult for big enterprises to introduce their own security systems and also to purchase CCI products. Companies who choose to ignore the risks might become obsolete. Small-sized companies, who are not prepared to introduce sufficient computer security systems or purchase an insurance product in relation to the high cost, could well be left behind.

[462] The author is grateful to Mr Y. Takase, Assistant Manager, Liability Insurance Group, Non-Marine Underwriting Department, Mitsui Marine and Fire Insurance Co. Ltd. for his invaluable comments and advice.

possible liability payment, whereas smaller enterprises may purchase them in order to fully cover potential liability. All clients have their own reasons for purchasing CCI products but universally taking out an insurance product should not be the only means for a company to avoid business risks. Non-life insurance companies cannot take on all risks, especially when the risks posed in cyberspace are potentially so huge. Therefore in order to create a stable economy, CCI products must not be the only one method of avoiding risks.

8.1.4 On what does your company place the greatest importance, regarding selling the CCI products — property damage or liability for a third party?

A fire insurance product can cover any mechanical failure. The purpose of the CCI products is to cover losses that cannot be covered by a fire insurance product, such as unauthorized access to a computer. Any insurance product is a means of covering a loss for an insured, and compensating a well-intentioned third party if the loss is relatively easy to measure objectively. However, it is very difficult to measure a loss which is insurable under the CCI products because of the following reasons[463]. Firstly, the CCI product itself is brand-new so that no information exists to help to measure loss. Secondly, the loss could potentially be an astronomical figure. Non-life insurance companies have a department responsible for measuring losses and risks for any insurance product. If this department is not able to calculate a figure they may outsource the task. If using outsourcing does not work, it abandons dealing with such a loss or risk. In a sense, an insurance company buys a risk from a client. That risk must be within insurable size otherwise the insurance business is operating on an impracticable business theory. From this point of view, it is much easier to measure the scale of the risks of property damage than liability risks. In addition to the fact that the sellers place more importance on it, clients are also likely to purchase insurance products for property damages rather than for liability. This is simply because the idea of covering property damages by insurance products is much more familiar to Japanese society. Legal risks, such as the imposition of civil liability, have been an intimidating prospect for Japanese business.

CCI products usually consist of four elements[464]. All five non-life insurance companies interviewed include those in their products and seem to place equal importance on property damage and liability. Their difference lies in the products' construction: some non-life insurance companies prepare "all in one" CCI products where the client has no option

[463] Measuring only the property damage (see footnote No.42) is not difficult as long as all computer equipment is stated in the schedule. In the said questionnaire (see 7.1.3) the compositions and the computer network structure must be explained. The damage against software or data is seemingly difficult to measure, because the value of software or data depends on a company. Thus, non-life insurance companies consider that covering the loss of software or data is equivalent to the cost of reinstatement.

[464] See section five.

but to have all the components to cover all sorts of damages or losses; other products have optional components. However, it is possible to change this structure depending on a client's demand. This is left to the seller's discretion.

8.1.5 Who was involved in measuring the new risks from cyberspace and developing the CCI products?

Actuaries usually play a significant role in developing new products, particularly in the life insurance industry. However, in the case of CCIs, no sufficient empirical statistics exist, so underwriters act in place of actuaries as they are able to access the data provided by their own experience of established insurance products. This is one of the big differences between life insurance companies and non-life insurance companies[465].

As mentioned in Section Six, co-operating with IT companies is the principal means of measuring new risks in cyberspace and developing new products. Sumitomo and the Yasuda Fire and Marine Insurance Co. Ltd. (hereinafter "Yasuda")[466] have a connection with foreign IT companies, which have knowledge in this area of business outside Japan. IT companies play a leading role not only in developing the products but also in preparing questionnaires for clients. The questionnaires appear to be designed to prove that a client has a satisfactory level of computer security. If a client has a very poor level of security or risk management, the insurance company can reject selling its insurance product to that client. Alternatively, the client could spend a large amount of money to improve its security to a sufficient level. If a client's risk is very low, an insurance company may not regard it as cost effective to develop a product to cover it.

The questionnaires always have two main purposes: firstly to find the difference between the market's reality and its estimation. This helps in analysing its market and reconsidering the future possibility of an insurance product. Secondly, the questionnaire is a means of sifting through and excluding some companies from the client lists if their risks are too uncertain.

The evaluation of computer security for each client is based on the questionnaire. One section of the questionnaire refers to the guidelines for computer security systems prepared by the relevant governmental

---

[465] In reality there are not many actuaries working at non-life insurance companies.

[466] The author is grateful to Mr A. Okabe, Manager, Liability and Casualty Section, Property and Casualty Underwriting Department, Mr T. Amagai, Deputy Manager, Commercial Property Section, and Mr H. Iritani, Assistant Manager, Liability Insurance Division, Liability and Casualty Section, Property and Casualty Underwriting Department, the Yasuda Fire and Marine Insurance Co. Ltd for their invaluable comments and advice.

offices[467] or global standards such as ISO 9000[468]; the second is based on its own industry's risk management knowledge. Actual numbers of computers must be recorded and a company's network structure must be explained in the third section. All the questionnaires are designed to reach the security standard provided by the Ministry of International Trade and Industry of Japan.

8.1.6 The Summary

The continuing development of IT (or rather, associated new risks) creates a business opportunity for the non-life insurance industry. The non-life insurance industry in Japan does not cover all risks; it is impossible to do so. Liability is a particularly difficult area to cover and the Japanese non-life insurance industry has chosen to disregard it and the business opportunity it presents. One possible view is that the Japanese non-life insurance industry is reluctant to further develop the area of CCI products, although it is impossible to state this categorically without undertaking an in-depth analysis of the products.

8.2 Questions regarding selling CCI products

8.2.1 What types of skills do sales staff need? (I.e. special/technical knowledge?)

The sales staff in any industry in Japan usually present their products to the general affairs department of a company, and make a contract with this department even though a product has not been purchased for it. This is sometimes a very strict rule in Japan, particularly in large or old-fashioned companies. Currently, an IT department (or any department) which plans to purchase the CCI product, often gets involved in a general affairs department at the sales talk stage or is even allowed to make a contract directly to a non-life insurance company. Therefore, it is possible to reduce time if the sales staff are able to explain their CCI products directly to a person from the IT department, who has knowledge of technical or computer system matters. Sales staff have a slightly more difficult job selling CCIs than other insurance products. They are required to have in-depth knowledge of a new product as well as IT knowledge[469]. Some non-life insurance companies provide in-house training and prepare handbooks for their sales staff. Other companies provide sales staff with an IT technician[470] as

[467] For example, the Ministry of International Trade and Industry, the Ministry of Posts and Telecommunications and the FSA.
[468] International Organisation for Standardization. ISO issues three standards; ISO 9000, 14000 and 14001.
[469] Such as hardware, software, and networks, and so on, to a certain level.
[470] There is usually no technician in an insurance company although it has its own IT department. An insurance company tends to cooperate with an IT company to develop this insurance product because of its IT nature. A technician here means a person with whom an IT company has sought to cooperate.

support. They also invest in producing and distributing documents to clients in an effort to decrease difficulties in sales.

Despite the extra effort involved in selling CCI products, the trend to give authority to individual departments in Japanese business industries provides more sales opportunities as long as the sales staff gives an appropriate and persuasive presentation and the client understands how vulnerable their company is against computer risks. Two non-life insurance companies expressed a significant opinion on this point. Tokyo Marine explained that the first step in the sales process is often made by the client, who approaches a CCI provider to advise them on products. In this way the CCI provider usually has a good idea of what product will be appropriate for the client's need. One of the five non-life insurance companies[471] said that it does not provide any training or meetings internally because of the time and manpower this would consume against profits. Instead staff who have an interest in IT specialise in selling the CCI products. This company acknowledged that relying on individual manpower is not an ideal way for a CCI provider to expand this market. It needs to make CCI a target area for all sales departments.

Each individual non-life insurance company judges the profitability of developing the CCI market or sticking to traditional markets such as car insurance. So the development of any new product is dependent on this decision.

8.2.2 Does your company think that the risks in cyberspace are counted as a catastrophe risk?

It is well understood that the potential risks associated with computerised business are enormous. Yasuda mentioned the "Love Bug" virus as an example of an ever present and serious threat. E-commerce continues to flourish and is becoming a major method for conducting global business. If a network stops operating (whether accidentally or through ill intention), the cost in terms of property damage is far outweighed by the cost of liability to a third party.

However, all the non-life insurance companies interviewed are of the opinion that the limit of the CCI products' coverage is unlikely to be on the scale of earthquake insurance. Therefore, the risks in cyberspace are not counted as catastrophe risks although the potential risks are similarly considerable. This idea appears to be concrete throughout this industry.

[471] Here the company remains anonymous at the company's request. The author would like to thank the company for its frankness.

8.2.3 Does your company think re-insurance is necessary for CCI products? If so, what insurance companies does your company ask to re-insure? (I.e. domestic or international?)

No insurance company expects to underwrite a risk, which needs to be re-insured, particularly in the area of liability. Furthermore, there is no great volume of either demands or losses, which require re-insurance at this stage. However, the possibility of being re-insured is not completely overlooked by any company. If a risk exceeds the expectations of a non-life insurance company, that company will arrange to be re-insured. Companies can request it, but the decision to reinsure lies entirely with the reinsurance company and they are under no obligation to do so. Furthermore, there is a limited number of domestic non-life insurance and reinsurance companies. Therefore, it is difficult for a non-life insurance company to distribute the risks of a CCI product inside Japan because its risks are unique. If it needs to be re-insured, it would have to request it from a number of reinsurance companies rather than just one. Mitsui and Yasuda mentioned that reinsurance companies outside Japan have more experience and capacity to reinsure the risks, so requesting reinsurance from an international re-insurance company is a practicable solution. Many non-life insurance companies stated that they would ask reinsurance companies outside Japan.

8.2.4 To what extent do the risks increase in a one-year span? How often does your company have to reassess products?

As information technology improves, new types of risk are perceived. Hence the necessity to re-examine contracts on a regular basis, normally annually. However, risks associated with CCI products can rise very rapidly, even on a daily basis. How does each non-life insurance company cover a risk if the incidence of breach of security has increased? The answer is the contract remains unchanged until the contract year ends. At the end of the year, the sellers decide whether it is necessary to increase the premium. If a client physically installs or removes a computer, the client can modify the schedule. In a situation where an insured company's risks increase partway through a contract, that contract will not be affected although the premium is increased or decreased if a client installs or removes a computer. Furthermore, what happens if the risks increase but there has not been any incident in the previous contract year? According to Chiyoda, it is almost impossible to change the premium in this case because those two issues must be related. In reality, one of the five companies interviewed[472] has not changed the premium for the last two years.

[472] Here the company remains anonymous at the company's request. The author would like to thank the company for its frankness.

8.2.5 Do you differentiate on pricing by geographic area?

It is not possible to differentiate the premiums of CCI products by geographic area except that portion of the premium covering property damage. Most companies used the premium rate of fire insurance, which differs according to geographic area, for calculating property damage in CCI products. Another example of differentiation is the west Japan has many more typhoons than the east part of the country. Thus, it makes sense to set the price of an insurance product for typhoon losses higher in west Japan than in east Japan. It is possible to consider the likelihood of business interruption being caused by a large-scale typhoon breaking the computer networks. However, no insurance company thinks it is necessary to alter pricing by regions. The reasons for this are various, but it is primarily because fire or flood insurance products usually cover property damage. If a client purchases both fire and CCI products, the premium is likely to be reduced, although non-life insurance companies usually avoid selling insurance products, whose coverage overlaps. Tokyo Marine pointed out that there is not a higher possibility of network interruption occurring in the west part of Japan compared to the east.

No clear evidence was given for the necessity of making a different premium for liability as a result of business interruption. Business interruption could cause huge damage and a client be sued by third parties wherever they are located. In other words, a client can unintentionally cause damage to anyone all over the world, i.e., throughout cyberspace. A more effective method for non-life insurance companies to avoid taking huge risks would seem to be to fix the range of compensation rather than changing the premium rate by geographic area.

8.2.6 To what extent is it possible to cover losses regarding computer crime[473]?

One difficulty is how a client proves that they have suffered damage through a certain crime. As was mentioned earlier[474], all clients have to answer questionnaires to prove their security system is of a sufficient level before they can purchase the CCI products. If a client manages to prove a crime has been committed, the resulting damage or losses suffered are covered. In this situation a client must inform the non-life insurance company of an incident within a certain period of time after it discovers the damage[475]. Needless to say, it is sometimes difficult not only to prove the damage was caused by a crime, let alone to know a crime has been committed in cyberspace.

---

[473] Such as hacking, virus damage and on-line fraud.
[474] See section five and also 7.1.3.
[475] The period of time depends on the type of products. Some products require that the seller be informed within 24 hours, others allow 30 days following a client's discovery of the damage.

If a client company itself suffers damage as a result of hacking, four areas are covered by the CCI products: property damage, loss of information, extra working costs for business interruption, and loss of income. If a third party suffers damage through a client's computer network as a result of hacking or unauthorized access, this case is not as straightforward. The client has liability to compensate the third party, but the determination of the extent of liability (including court costs and legal fees) would be problematic. For instance, suppose the case that a third party "X" had its business interrupted by unauthorized access by a criminal "Y" through a CCI product's client "Z". Because it was impossible to specify a suspect, X decided to sue Z for negligence. However, can it be said unequivocally that there was no alternative to continue business, such as by phone or fax? The court would judge whether Z had responsibility for X's damage on every single issue. Mitsui was of the view that it would be very difficult to handle such a case because there has so far been no judicial precedence.

8.2.7 To what extent is it possible for an insurance product to cover losses caused by employees' dishonesty?

Any internal illegal act is usually an exemption. However, some insurance companies agreed that it is crucial to regard employees' dishonesty as a risk to a company. Many insurance companies usually have an insurance product called fidelity credit insurance. On the one hand, it is, in fact, impossible to avoid employees' dishonest acts such as fraud. According to Sumitomo, it is possible to develop an insurance product in terms of surety for an employee, but they are not keen to pursue this, because the potential risks will be huge. The only way a company can attempt to avoid dishonest acts by an employee is by introducing in-house training and education, which teaches employees what actions are illegal and what sort of regulations exist and can be applied to a case. Despite such efforts by a company, human nature makes it impossible to avoid all dishonest acts by employees. Moreover, it is very difficult to estimate and quantify the losses caused by fraud which makes underwriting employees' dishonest acts problematic. Thus, the premium tends to be high and it is the least popular type of CCI products. On the other hand, reputation plays a crucial role in controlling the fate of a company. In the case of an employee committing fraud against a company, to what extent does the company lose its reputation? Is there any possibility of insuring the reputation of a company? This is intrinsically difficult because there is no way of quantifying the reputation. Even if it is possible to quantify it, the next issue will be how to estimate the extent of "lost" reputation by an employee's dishonest act, considered apart from the other elements such as social background and recession. However, it is possible to develop such an insurance product. For instance, to re-build its reputation a company may choose to issue a newspaper advertisement to improve its image. Chiyoda has included cover for this in its CCI products. But this is largely an issue for each client's in-house management.

8.2.8 The Summary

The Japanese non-life insurance industry continually follows the industry in Europe and the USA, although the availability of CCI products in those nations is higher than that of Japan. Of course taking huge risks is not the way to achieving sustainable economic stability in the industry. However, it seems there are some avenues available to cover major risks although no insurance company is willing to take such an unpredictable opportunity. There are no empirical statistics of risks of cyberspace at present so each non-life insurance company has been exploring its own way in the CCI market. Each non-life insurance company makes its own judgement on whether to press ahead with developing CCI products or wait until the market is more favourable.

8.3 Questions regarding the future of the CCI products

8.3.1 How much revenue does your company expect in FY2000 from CCI products?

Some non-life insurance companies expect more than £1.2 to 1.8 million as revenue in the fiscal year 2000. One quoted the revenue as more than £6 million.[476] The Koa Marine and Fire Insurance[477] published in its news release that the expected revenue is two hundred million-yen for three years. This can be explained by the difference in the size of businesses or types of potential clients. Two insurance companies replied that it is very difficult to predict revenue because of the character of CCI products. However, they seem to have different outlooks. Yasuda sounded very optimistic about selling CCI products and believes the products will make profits in the future (despite the difficulty of underwriting them). According to this company, the cost of one of their products, which is a ready-made CCI product developed on the basis of other products, is almost zero excluding personnel expenses. Surprisingly many non-life insurance companies have a very small number of staff (maximum of five people) devoted to developing the CCI products. Despite the small number of staff assigned to it, Yasuda will not consider the possibility of ceasing to sell their CCI products as long as the loss ratio[478] is low.

---

[476] The exchange rate: £1= approximately 170 yen.

[477] Koa Marine and Fire Insurance is a medium-sized non-life insurance company in Japan.

[478] The loss ratio means 'the ratio of losses and loss-adjustment expenses incurred to premiums earned, usually expressed as a percent. The loss ratio is an estimate of the value of insurance benefits and loss-related services relative to premium payments' cited from C. Williams, M.L. Smith and P. Young, 'Risk management and insurance: the eighth edition' (1998) McGraw-Hill, London.

8.3.2 Is it possible to cover any loss occurred overseas at present and in the future?

All non-life insurance companies restrict the geographical coverage of CCI products to Japan. Loss or damage incurred overseas is normally listed as an exemption in the clause. However, it is impossible to estimate the future of CCI products without taking account of the global aspect of borderless computerised business. In fact, no insurance company denies that the possibility of suffering damage outside the territory is high. The problem is specifying where risks exist. Without specifying it, it is impossible to judge to which jurisdiction it would apply. Some non-life insurance companies conceded that they would have to consider their global risk in the future. However, it seems to depend to what extent the CCI market flourishes in the next three to five years (a fairly passive response to this issue). In reality, when the insured risk becomes bigger, the risk for an insurance company becomes bigger: no insurance company can insure a risk so big as to leave its management vulnerable to bankruptcy. Thus, one solution may be to restrict insuring risks within a certain level, for example excluding computer risks overseas, to help reduce vulnerability.

All the companies the author interviewed sounded very reluctant to tackle this issue even though they have recognised the possibility of damage from outside the territory. Therefore it is presumed that it is impossible for the Japanese non-life insurance industry to take this risk at present, because the market does not seem to have the flexibility to take such a potentially great risk. However, it is assumed that once a non-life insurance company decides to take this risk, then the others would gradually follow suit[479]. Otherwise the industry would be swallowed up by foreign affiliated companies.

8.3.3 The Summary

In the near future, each non-life insurance company seems sure of its share of market demand. It is arguable, however, that in order to retain and expand the CCI market, CCI providers will have to become more flexible and be willing to take higher risks. The most important point is to discover the method to deal with higher risks, not to avoid them.

8.4 Others

[479] One reason why CCI products were similar was that the reforms to the financial sector had not yet been introduced when CCI products were initially developed. Thus non-life insurance companies were obliged to develop their insurance products under the guidance of the relevant authorities (the FSA since 1998). See section two for the reform in the financial sector in Japan and section three for the FSA.

8.4.1 To what extent does your company compare between its own CCI products and the others?

Surprisingly, all the insurance companies commented that they only analyse other companies' CCI products on a basic level. According to one of the five non-life insurance companies interviewed[480], it is frankly not very interested in similar insurance products in other companies as long as it does not have to share the market. Surprisingly again, each company has its own market, which does not clash with others. The same company stated that this is a peculiarity of the Japanese non-life insurance market; that it is friendly without cut-throat competition. It was true in Japan until very recently that the higher reputation a company has, the more its clients are reluctant to consider switching to another company offering a similar product more cheaply. But the Japanese economic depression no longer allows such unswerving loyalty to exist. Indeed, to a greater or lesser extent, all markets must have competition, otherwise an economy has no growth. That is not to say however that each non-life insurance company still enjoys a strong relationship with its clients. Despite their reluctance and passivity towards branching out into CCIs, many companies are approached by their clients and therefore begin to sell CCIs to satisfy them. Furthermore, big non-life insurance companies are in the position of being able to hand over the sales of CCIs onto their agencies and brokers.

All the five non-life insurance companies are actually leading companies in Japan and have good products. However, the competition has become severe owing to entry into the market by other industries and foreign companies. If a non-life insurance company rests on its laurels, even if it does not lose its existing clients, it may lose the opportunity to further develop the market. In terms of the products themselves, one non-life insurance company argued that a client who does not have an understanding of its own risks will not benefit more from one product than another and may even purchase a product which is not appropriate to their needs. The differences of content amongst the CCI products are not significant at this stage although they are adapted and elaborated on by each non-life insurance company. As one insurance company mentioned, the most attractive selling point might be the co-operative IT company behind non-life insurance companies.

8.4.2 What does your company think of Internal Controls?

This question is similar to the issue of employees' dishonest acts but covers a broader area including self-defensive methods for non-life insurance companies themselves.

It would appear that all non-life insurance companies have in place

[480] Here the company remains anonymous at the company's request. The author would like to thank the company for its frankness.

mechanisms of corporate governance and compliance in a broad sense, under the guidance of the Ministry of Finance, to ensure sound company business. For instance, they have in-house training for both new employees and experts alike in regard to relevant regulations and good employee conduct. All five companies maintained that their computer security levels are more than sufficient. The reason for this is the large-scale development of computer security that was achieved to combat the Y2K problem in 1999 rather than a specific countermeasure against computer crime. They appear confident that regular internal checks on the condition of computer networks ensure security and make the networks less vulnerable to hacking. Therefore none of them has alternatives, such as pooling money or purchasing the CCI products for themselves. In addition it would prove difficult to find a company willing to underwrite for purchasing the CCI products. The reason given by one of the non-life insurance companies for not having the CCI products themselves is that they are difficult to purchase.

Sumitomo stated their method of ensuring internal security is through regular emails to all employees on specific topics of security and regulation to keep these issues at the forefront. They employ (as a form of punishment) the disclosure of all security breaches to all employees by email. In this case, everything goes public, such as the details of the case, who is penalised and what the penalty is. It may happen that an individual's boss is penalised or at least given a warning for inattentive supervision of a guilty employee. This aims to avoid recurrence of a similar case by pillorying the first guilty employee. This in-house punishment works to some extent but only if the illegal act is committed in-house.

The issue of ex-employees is also crucial but it is not easy to prevent their illegal acts at this stage, as is to what extent a non-life insurance company can control its agency's business. Cash is handled by agencies and then sent on to the finance and asset management departments of the non-life insurance companies. In these circumstances, the head office has responsibility for managing its agencies.

8.4.3 The Summary

All non-life insurance companies have realised that CCI products are very active and dynamic. In the USA, risks are classified and dealt with individually by specialised insurance companies, and any company is free to sell CCI products. Sumitomo speculated that the Japanese CCI market is likely to go the same way as the American market. This would enable the Japanese market to expand, otherwise the market is in danger of losing its sustainability.

One of the five non-life insurance company's official[481] statements was that it is interested in information technology that would avoid computer risks altogether. Unfortunately, although technology makes rapid progress, so do the associated risks. The same official questioned how it was possible to enforce a law in such way that a person can be arrested as soon as he/she produces a virus, in addition to the existing law where a person is arrested when he/she damages property or data in another's computer. This would indeed reduce risk, however this is complicated by two issues. Firstly, the question of how the police can discover a person who has produced a virus before any damage occurs. Unauthorized access to a computer is likely to be carried out just for fun and it is almost impossible to find a virus that exists in a potential criminal's private computer before it causes any damage. Secondly, the enforcement of law does not always ensure the protection of human rights. Law is not a perfect solution and can infringe even basic human rights.

Sumitomo explained that Japanese insurance companies have analysed American insurance products of all products. However because of the cautious nature of Japanese business it is unlikely to follow American business style. In the past, every new risk occurred in the USA before anywhere else in the world. Japanese insurance companies observed the American insurance companies and made their decisions based on that. No Japanese company would consider taking on a risk that the American companies regarded as unreasonable. Even risks that the American companies judged to be insurable were not necessarily taken on by the more cautious Japanese companies.

In contrast, in recent years some types of risks are encountered all over the world. This means that Japanese insurance companies are no longer able to avoid action until the results can be observed elsewhere. They are now obliged to take action as soon as they encounter a risk. Their lack of experience makes them liable to panic, and label the rule as an exemption — thereby ignoring it altogether. Therefore, one of the five non-life insurance companies interviewed[482] hopes to develop a method of early detection of risks, in order for them to "buy time" in preparing to tackle it. This company also disclosed its keenness to develop a product based on cyber risk which is potentially very high but is unlikely to occur. Although realistically, because of the speed of technological innovation it is almost impossible to develop such a product.

---

[481] Here the company remains anonymous at the company's request. The author would like to thank the company for its frankness.

[482] Here the company remains anonymous at this company's request. The author would like to thank for this company's frank opinion.

Chapter VI: An Analysis of Available Insurance Products in The British Insurance Market

1. Background

The City of London has been the centre of the global insurance business. Lloyd's, in particular, has played an indispensable role since its birth in Edward Lloyd's coffee house along the Thames in the seventeenth century. It is said that it is no exaggeration that non-life insurance history has its first step from Lloyd's[483]. According to the Association of British Insurers, the UK insurance industry contributes £8 billion per annum to UK overseas earnings; it accounts for more than 20% of investments in the stock market and pays £225 for pension and life insurance, and £41 for general insurance claims per day. There are about 822 authorised (by the UK or another European Economic Area member) insurance companies in the UK: approximately 600 companies are eligible to run general business only (motor, household and commercial insurance policies), 165 are eligible to run long-term business only (life insurance and pensions) and approximately 60 companies are eligible to run composite businesses[484]. The UK insurance market itself ranks third largest in the world of premium income (America is first and Japan second)[485]. Its supervising authority is the Financial Services Authority (FSA).

The UK insurance market is surely different from the Japanese. Comparing the structures, it is possible to discern that the UK market is less concentrated than the Japanese in both life and non-life insurance markets[486]. Approximately 660 companies (a simple addition of 600 for general business only and 60 for composite businesses from the above statistics) in the UK run general insurance companies whereas there are approximately 30 non-life insurance companies in Japan. Having a variety of distribution channels is another difference. Although the whole financial sector has been changing since the Japanese government announced a reform of the financial sector in 1997[487], unlike the British market, the dividing line between underwriters and brokers in Japan is not yet evident to the general public. Brokers are the most critical channel for the distribution of insurance in the UK; they have had more than a 50% share of individual and over an 80% share of commercial lines over the

---

[483] See ' The present and the future of Lloyd's (*Lloyd's no genjô to syôrai)*', <http://www.yasuda-ri.co.jp/quarterly/data/qt31-2.pdf> (print out on file with author).

[484] See 'The Association Of British Insurers', <http://www.abi.org.uk/Display/default.asp?Menu_ID=507&Menu_All=1,506,507> (print out on file with author).

[485] See 'Changes in EU Financial and Insurance Markets and New Strategies of EU Financial Institutes and Insurers throughout the 1990's, especially in the UK, German and French Markets', <http://www.sj-ri.co.jp/quarterly/q32.html> (print out on file with author).

[486] In the UK, the Association of British Insurers shows three main types of insurance: general insurance, life and pensions, and health and protection. In Japan, it is generally classified into life and non-life insurance. General insurance in the UK is the same as non-life insurance in Japan. So 'general insurance' is to be used in this context. For reference, see 'Introducing Insurance', <http://www.abi.org.uk/Display/default.asp?Menu_ID=508&Menu_All=1,506,508> (print out on file with author).

[487] In regard to the reform of Japanese financial sector, see Chapter IV.

past six years[488]. It would be pointless to enumerate every single difference between the two markets in this context — the question is one of motivation.

Some people in the British insurance business have often asked the author why purchasing insurance products in general has not been firmly established in Japan. On the one hand, it is common for Japanese to have life insurance products and, in particular, they are very likely to choose a product with an accumulated dividend in the future. Having motor insurance is mandatory for drivers. On the other hand, they are unlikely to purchase other types of insurance products such as earthquake insurance (on dwelling risks) even though Japan lies on the Pacific Rim earthquake zone. After the Great Hanshin-Awaji Earthquake in 1995, there was a rush to purchase earthquake insurance products but only for a short while immediately after the incident. Why are the Japanese reluctant to purchase earthquake insurance? Firstly, because it is expensive. Secondly, the Japanese are likely to be accustomed to earthquakes as a consequence of their frequency. Above all, there is a very fundamental conceptual reason. Lloyd's Japan agreed that the Japanese are likely to think that purchasing such insurance products returns nothing when their term ends[489]. The general concept of insurance is that it purchases "a guarantee" for the term of the contract obtaining coverage in case any loss or damage occurs to an insured subject. This purchased product is invisible and does not make money; while a buyer would get money to repair or compensate the losses in the event of an incident, such money is clearly not defined as profit. If nothing happens, nothing will remain except for the fact that the buyer had a peaceful year. Thus, it seems hardly possible for the Japanese to consider that one peaceful year costs premiums. As a result of this involuntary concept, purchasing insurance products is considered either a waste of money or, that its cost performance is ineffective.

Indeed, the chart proves that people in Japan and the UK have completely opposing interests regarding their assets. Insurance and pensions account for more than 50% of the majority of British individual monetary assets. On the other hand, savings and trusts account for more than 60% of Japanese individual monetary assets (Table 5.1). Both countries want to prepare for the future, but by using different means. It has been said that the Japanese were very likely to save money rather than invest it in other financial products. This tendency has not changed, even with a continually low interest rate over a long period since August 1995[490].

---

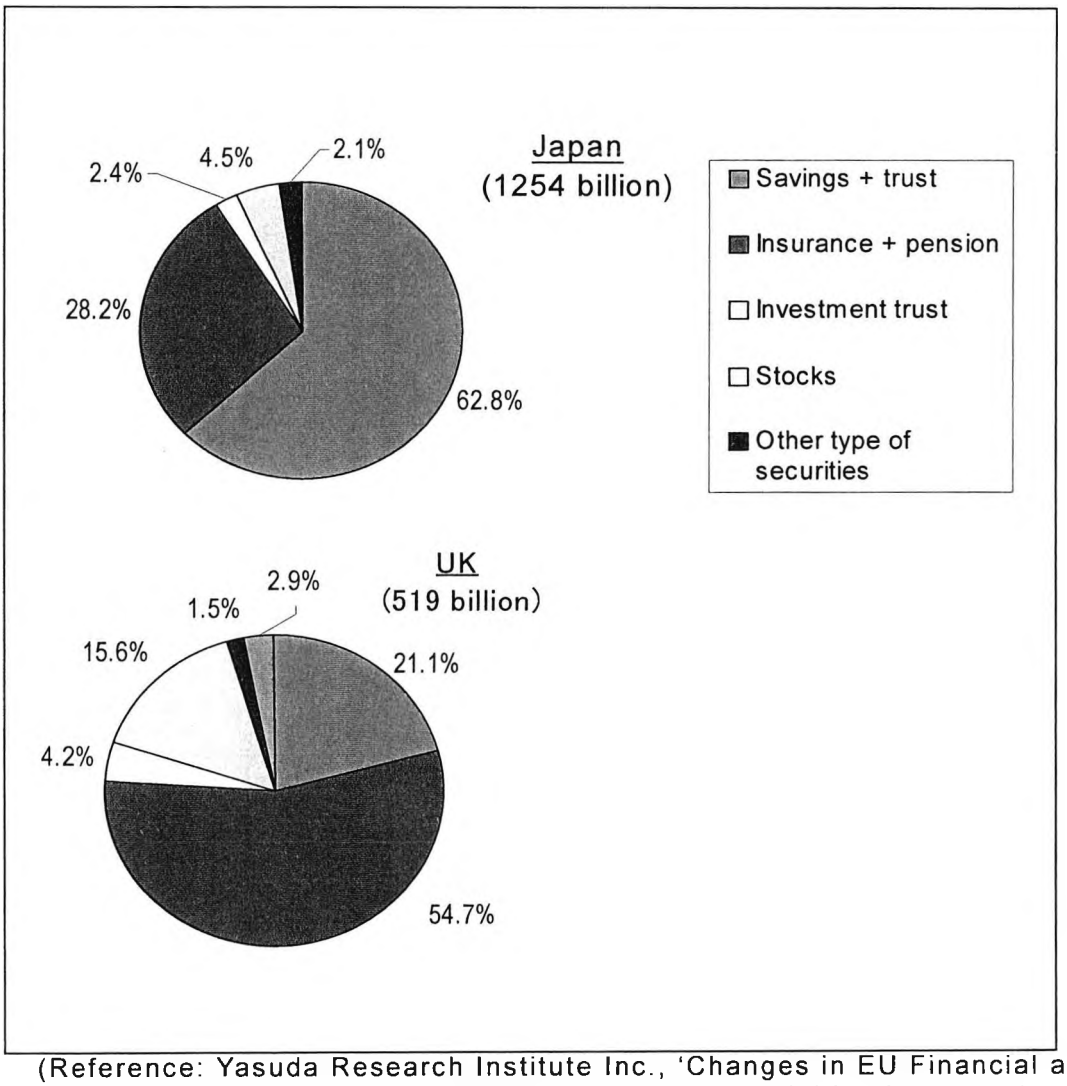
[488] See 'Changes in EU Financial and Insurance Markets and New Strategies of EU Financial Institutes and Insurers throughout the 1990's, especially in the UK, German and French Markets', *supra* n.472.

[489] The author is grateful to Mr Y. Fujita, Manager of Production & Underwriting Department, Lloyd's Japan, for his invaluable comments and advice.

[490] Although the interest rate marked over four percent at one time, it has been under one percent since August 1995. See 'Finance@nifty', <http://finance.nifty.com/stocks/tsumitate/column/co1.htm> (print out on file with

One of the reasons behind this is the myth of immortality, which the Japanese had believed for a long time: that banks would never go bankrupt.

Table 5.1: The composition of individual monetary assets in three countries



(Reference: Yasuda Research Institute Inc., 'Changes in EU Financial and Insurance Markets and New Strategies of EU Financial Institutes and Insurers throughout the 1990's, especially in the UK, German and French Markets', *supra* n.472 *et seq.* Data was sampled in each country by the end of 1998.)

As was mentioned in the previous chapter, the Japanese insurance market in general follows those of Europe and the USA. From this viewpoint, it is possible to say that the UK insurance market, or the European insurance market in a broad sense, is more mature than that of Japan, particularly the general insurance market. The main items of

---

author).

general insurance are vehicles, then property (such as fire insurance). Both fidelity and extra expense insurance have been on the rise of late. In reality, insurance products which cover financial losses increased their market share by 2.3% between 1992 and 1998[491]. Business interruption and related insurance have been attracting considerable attention. This does not necessarily indicate the influence of the development of online activities and electronic commerce (e-commerce). Financial losses can be triggered by any factor, so e-commerce could be merely one of the potential reasons for loss. In reality, it is unnecessary for them to cover risks associated with cyberspace.

2. Specific insurance for financial institutions

2.1 Traditional insurance

Before moving on to the main issue of covering cyber risk, it is necessary to describe long standing insurance for financial institutions. This is traditional insurance such as Bankers Blanket Bond (hereinafter "BBB"). It is said that this originated from a Burglary Insurance Policy developed by an underwriter named Cuthbert Heath in 1877. Later, he completed a prototype BBB, and by the 1980s the present BBB forms, such as KFA '81 and NMA2626, had been completely updated. BBB is sometimes given different names, such as the Financial Fidelity Bond in the Chubb Group of Insurance Companies (hereinafter "Chubb"). It is not only for banks but also other businesses, such as securities firms. BBB is extensively called the Financial Institution Bond (hereinafter "FIB") in the USA[492].

BBB basically covers financial losses and property damages of a bank (the assured) as a consequence of employee dishonesty, theft, receiving counterfeit money and so on. To give a detailed explanation, insuring clauses in the policy are divided into seven parts: 1) employee dishonesty, 2) premises, 3) transit, 4) forged cheques, 5) forged securities, 6) counterfeit currency and 7) offices and contents.

1) Employee dishonesty
Direct financial losses caused by employees committing dishonest or fraudulent acts (to make personal gains) are covered. It is not necessary for it to be a lone employee's crime or a conspiracy with others. The definitions of "employee" and "employees" are wide open:

---

[491] See 'Changes in EU Financial and Insurance Markets and New Strategies of EU Financial Institutes and Insurers throughout the 1990's, especially in the UK, German and French Markets', *supra* n.472.

[492] This thesis is targeted at the risks within financial institutions: not just banks. However, in this chapter, the discussions are expected to centre mostly on insurance products for banks as these products, are developed and mature. See 'The classification and the application of operational risk (*Operational risk no bunrui-taikei to katsuyôhô*)', <http://www.kinzai.jp/books/new_book/20010815/10128-2.pdf> (print out on file with author).

from people who work on a salary or wages basis to guest students pursuing studies on the premises.

2) Premises
Property within the premises is covered if it disappears, is damaged, destroyed, misplaced or stolen. However, any property damage in connection with terrorism is excluded. "Property" means tangible items, such as paper currency, coins, bullion, precious metals and stones, stamps, insurance products, cheques, securities, bankers drafts, money orders and so on. That is to say, electronically recorded data is not included in property.

3) Transit
Property in transit which is in the custody of any employee of the assured or a security company in an armoured vehicle is covered if it is lost or damaged.

4) Forged cheques
If the assured issues or pays any fraudulent (signature forged or perfidiously made alterations) cheques, bills of exchange, bankers' drafts, bankers' acceptances or certificates of deposit, the related losses are covered.

5) Forged securities
If the assured, in good faith and in the ordinary course of business, bears any fraudulent (signature forged or perfidiously made alterations) or counterfeited securities and/or similar written instruments, or if any genuine securities are stolen or lost, the losses are covered.

6) Counterfeit currency
If the assured, in good faith and in the ordinary course of business, accepts counterfeited paper money or coins, the losses are covered.

7) Offices and contents
If the interior of and/or contents within the premises of the assured are directly damaged by theft, vandalism or malicious mischief, the losses are covered. 'Contents' means furnishings, fixtures, equipment, stationery, safes and vaults. However, it does not include computer hardware, software, any media, or computer data. This does not cover losses as a result of fire or terrorism[493].

In general, BBB is combined with other types of insurance: policies to cover other properties and policies for professional liability. The typical examples for the former types are Electronic and Computer Crime Policy (hereinafter "CCP") and Kidnap/Ransom insurance. The latter examples are Professional Indemnity Policy (hereinafter "PIP"), Directors &

[493] See Lloyd's Worldwide Bankers' Policy (NMA2626).

Officers Liability Insurance (hereinafter "D&O") and Employment Practices Liability, Unauthorized Trading Policy and so on. As is obvious, policies covering property, such as BBB and CCP, cover a fund's losses but not liability. Some brokers combine some or all of these and call them the Combined Bankers Blanket Bond. Chubb, for example, provides a specific product named ForeFront Security combining financial fidelity, CCP, workplace violence and kidnap/ransom, and extortion coverage[494].

CCP covers 1) computer systems, 2) electronic computer programme, 3) electronic data and media, 4) computer virus damage, 5) electronic and telefacsimile communications, 6) electronic transmissions, 7) electronic securities, and 8) voice initiated transfers.

The losses are covered if an assured wrongly settles any transaction (payment or delivery of funds) as a result of:

1) Computer systems
   fraudulent data being inputted into computer systems, or data being modified or destroyed within the systems;

2) Electronic computer programmes
   computer programmes being modified, altered, or destroyed;

3) Electronic data and media
   electronic data stored in the assured's or related computer systems or any media on which data is recorded being altered maliciously or destroyed, as well as when media is stolen, lost or damaged;

4) Computer virus damage
   computer viruses causing losses;

5) Electronic and telefacsimile communications
   communications being intercepted then either being stopped or modified;

6) Electronic transmissions
   communications being intercepted and instructed fraudulently so that the assured is liable to the losses a customer or other institutions involved suffered;

7) Electronic securities
   fraudulent instructions being made to a Central Depository so that the assured is liable for the losses the Central Depository suffered;

---

[494] Kidnap/Ransom covers financial losses and expenses when a bank is threatened by ransom or extortion demands. See 'Financial Fidelity/Mail/Kidnap Ransom for Banks', <http://www.chubb.com/businesses/dfi/index8.html> (print out on file with author).

8) Voice initiated transfers
the assured having transferred funds of a customer by being given fraudulent voice initiated instructions.

There are some exclusions, such as the loss of potential income, losses caused by an identifiable director or an employee of the assured, indirect and consequential loss, and so on. Losses as a result of mechanical failure, error in design and gradual deterioration are also excluded[495]. If any loss caused by a director or an employee of the assured is not covered by CCP, this means all types of the above-mentioned incidents must be committed by a criminal/criminals outside the institution. When BBB was developed, there was no scope for advanced computerization, therefore it was not prepared for covering losses of an electronic or computerized nature. CCP was designed to fill those gaps.

On the other hand, insurance products for liability differ from one other. D&O is likely to be the most popular product since it is available to all businesses. As the name shows, it is literally prepared for directors and officers in case shareholders, regulators or others make allegations of misconduct against them. On the contrary to this, PIP covers claims against employees. Chubb, for instance, developed ForeFront combining some liability insurance, such as D&O, employment practices, fiduciary and so on. The tables below briefly show which insurance products are available to cover each risk in financial institutions (Tables 5.2 & 5.3)[496].

[495] See Lloyd's Electronic and Computer Crime Policy (Worldwide 1998 Form).
[496] Tables 5.2 and 5.3 exclude some irrelevant risks in this context, such as environmental, health & safety and personnel/welfare risks from the original. The original table was given by a person concerned with general insurance and the author has his permission to re-arrange it for this thesis. The name of the person remains anonymous at his request. The author would like to thank him for his frankness and generous advice. The author is to blame for any typographical errors.

Table 5.2: Legal Risk

Category	Risks	Available policies
Litigation risk	Litigation from the third party for bodily injury and property damage	* Public liability insurance
	Litigation targeting executives personally	* Directors & Officers (D&O) liability insurance
	Litigation from employees and ex-employees Trouble due to harassment in the workplace	* Employment practice liability insurance
	Litigation in terms of professional advice	* Professional Indemnity Policy
	Litigation relating to pension management	* Pension Trustee liability insurance
	Litigation relating to libel & slander	* Libel & Slander liability insurance
	Cost for legal proceedings in general	* Legal expense insurance
Jurisdiction risk	Litigation in disadvantageous jurisdiction	* Depending on all liability insurance wordings
Documentation risk	Legal liability because of errors and omission	* Professional Indemnity under * Bankers Blanket Bond * D&O liability insurance
Security Risk	Political risk	* Political risk insurance

Table 5.3: Operational Risk

Category	Risks	Available policies
Crime risk	Crime risk by employees	* Fidelity cover under Bankers Blanket Bond
	Crime risk by non-employees/outsiders	* Commercial Crime Insurance
Violation of internal rule	Loss due to transaction beyond authority	* Unauthorized trading insurance
Physical Disaster Risk	Fire/explosion & other risk of own property	* Property Insurance * Loss of revenue cover under * Business Interruption insurance * Additional Increased Cost of Working cover * Loss of Rent insurance * Public Liability Policy
Terrorism	Bombs and other sabotage	* Terrorism insurance (fire/explosion)
	Abduction of executives	* Kidnap & ransom insurance
IT Risk	Computer crime Financial loss caused by computer viruses	* Computer crime insurance
	Loss due to misdirection (remittance /crediting) caused by computer viruses Loss/cost for the repair of the electronic data caused by computer viruses	* Computer crime insurance * Computer All Risks

Is it, in fact, necessary for financial institutions to purchase said traditional insurance? It is necessary for all banks in the USA to purchase a FIB by the order of the Federal Deposit Insurance Corporation (FDIC). Unlike the US, there is no such obligation in either the Japanese or the UK financial markets. Nonetheless the saturation level of BBB in Europe is said to be over 90%[497]. There are no certain statistics; however, it is said that the great majority of UK banks have purchased BBBs. With regard to Japan, as expected, BBBs are very unlikely to be mainstream although they have been on the market since the 1970s. What could be the reason for the differences between the two countries? Japanese banks have never been keen on purchasing BBBs; rather, they have been keen to avoid making errors or having accidents. In reality, there has been a concept amongst the general public that being employed in financial institutions is very popular. The possible reasons are (1) the Japanese believe that banks never go bankrupt, and (2) banks tend to pay a higher salary more steadily than most other industries. Therefore, recruits inundate banks to get a job and banks can choose from huge numbers of applicants; big financial institutions are only likely to choose graduates from good universities. Banks are able to carefully select candidates who are well educated as well as from a good background so that potential employees can provide a written pledge from two good references. In case he/she commits a crime against the bank, the employer asks the referees to cover or compensate for the losses. The referees are customarily obliged to compensate them to honour their signed pledges. Having this customary rule, banks are reluctant to purchase costly BBBs. Furthermore, many banks which the author interviewed expressed the view that Japanese financial institutions consider it uncustomary to doubt their employees, since the Japanese have a traditionally-based ethical doctrine that human nature is fundamentally good, although this sounds slightly inconsistent with having to have good references for each employee.

Thus, even if a bank purchases a BBB, it would not disclose the fact to its employees, to avoid being thought of as unfaithful to them. On the other hand, in the UK, the BBB market is mature according to Zurich London[498]. Not only British-originated banks but also foreign capital banks purchase BBBs and related insurance. Amazingly enough, even Japanese banks in the UK purchase BBBs[499]. This local BBB self-subsistence is opposite to the European style, which is a top-down system where the headquarters purchase insurance to cover its global businesses. A London branch of a Japanese bank covers losses more widely than its

---

[497] See 'The classification and the application of operational risk (*Operational risk no bunrui-taikei to katsuyôhô*)', *supra* n.479.

[498] The author is grateful to Mr C. Brown of Financial Institutions Underwriting and Mr L. Fielder of Manager, Professional Lines, Zurich London Limited for their invaluable comments and advice.

[499] Here the name remains anonymous by request. The author would like to thank the company for its frankness.

headquarters at home does. That is to say that the London branch adopts difference risk management measures and recourses compared to its headquarters. One underwriter commented that UK financial institutions have learnt that BBB works to reduce losses. Thus risk managers in each institution judge purchasing BBBs as cheaper than the cost of losses. Furthermore, the concept "some bad apples amongst many good apples always exist in any society" is comprehended in the UK market[500]. In reality, £10 billion in England and Wales is the estimated cost of corporate fraud per annum and approximately 30% of identified frauds are committed by employees who have been in institutions for over five years[501].

It is evident that a conceptual difference exists between Japan and the UK; UK businesses consider their relationship with employees without sentimentality. If Japanese moral philosophy cannot accept entertaining doubts against employees' loyalty there are two options left for Japanese institutions: either reconcile losses or engage in other types of precautions to avoid losses. To a greater or lesser extent, this is likely to be an excuse not to purchase a BBB since it covers losses not only insiders make but also those which outsiders make. In addition to this, it is dubious whether employees, knowing that their employer has insurance, are encouraged or discouraged in dishonesty and criminality. It is hardly possible to say that someone, whether an insider or outsider [502], spontaneously considers how a bank covers losses as a result of his/her own offence. So it is very likely to be irrelevant if a bank obtains insurance in order to promote employee honesty.

If the losses Japanese banks suffer are considerably less than those of UK banks, the Japanese banks' reluctance towards BBB is understandable. Unfortunately, there are no statistics available in public to compare the size of the losses. This is because incidents are not always reported to the relevant authorities. A bank especially prefers to deal with an offence in confidence so as to avoid its reputation being lost if indeed an employee has committed a crime. It is common for banks to have a reserve fund: it makes good the losses if an incident occurs. It works as self-insurance. Some risk managers or managing directors in financial institutions would consider it better than purchasing a BBB, since the reserve fund would not be spent if nothing happens and reputation would not be lost.

2.2 A brand-new type of insurance

To sum up the previous section, it has been traditionally satisfactory

---

[500] Here the name remains anonymous by request. The author would like to thank the company for its frankness.

[501] See 'Fidelity & Crime Insurance', <http://www.tyseruk.co.uk/cri.html> (print out on file with author).

[502] In this context, an insider means a criminal who works in an institution as an employee and an outsider means someone else. Ex-employees are considered outsiders.

for a bank to cover all the risks within its businesses by having BBBs, CCPs, PIPs and D&Os[503]. The question is whether the above-mentioned traditional insurance covers brand-new risks occurring in cyberspace. It was reported that the "Love Bug Virus" in early 2000 caused damage estimated at US$6.7 billion. The incident and its damage drew considerable attention from all over the world. There are other statistics showing the vulnerability of cyberspace: it costs a company US$125,000 per hour when its website is shut down for outages. The FBI estimated that US$142,000 was the average cost of a network security breach in 1999[504]. But for the gap in coverage of existing insurance products for financial institutions, a brand-new type of insurance named cyber insurance and similar products would not have been developed (hereinafter "cyber insurance" is used as a blanket term for any product covering cyber risks). Unfortunately, it is unmistakable that they missed some brand-new risks in cyberspace: infringement of copyright, defamation, cyber extortion and the like. Observing types of loss, neither loss of income as a result of business interruption nor extra expense (i.e. the increased cost of temporary repairs and expediting costs) are covered. However, these types of loss are not unique to cyberspace. Those are likely to happen in any business. Thus, policies covering such losses are available not only for financial institutions but also other industries. It is crucial to focus on whether or not a risk or loss is characteristic of cyberspace or cyber business activities.

The US Chamber of Commerce published figures which show that 40 billion US dollars per annum is lost by businesses as a result of employee theft[505]. The cases illustrate some of the problems. The first concerns Visnet, a Seattle-based Internet service provider. Its network was attacked by a hacker 44 times in two weeks in 1998. Christopher Bisciglia, later identified by the FBI as an 18-year-old former employee of Visnet, deleted files from the network, shut it down by spamming, inserted pornographic pictures and sent customers a derogatory message about Visnet. The company had basic business insurance and submitted a claim of US$346,000 for data replacement, public relations costs, and reduced revenue as a result of losing customers and so on. The insurance company decided to accept the US$19,000 which the FBI estimated as the loss. Visnet found some exclusions, such as the coverage of online defamation. The losses Visnet suffered could have been covered by cyber insurance, however it is said that it did not exist on the market when

---

[503] Although the context is limited to only four policies, an institution is very likely to have other insurance policies, such as Fire insurance, ERISA (Employee Retirement Income Security Act) liability (mainly in the USA), and so on, for other business purposes.

[504] See 'Prepare for the worst', <http://www.darwinmag.com/read/120100/worst_content.html> (print out on file with author).

[505] See 'Crime, Chubb Group of Insurance Companies', <http://www.chubb.com/businesses/ep/crime/crime.html> (print out on file with author).

the series of attacks on Visnet started. By 2000, the average premium for such a product was around 20,000 US dollars with high deductibles. It is doubtful whether Visnet could have afforded it even if it had been available on the market[506].

Some well-known companies and organisations have also fallen victim to cyber crime. Approximately 50 high-profile domain names, such as Manchester United and Adidas, were attacked on 9th April 2000 by a group suspected to be Serbian hackers[507]. The domain names were hijacked and as a consequence, the political propaganda of the group was broadcast against the will of the website owners. Adidas, particularly, was threatened by these cyberterrorists to pay a ransom instead of having a virus implanted in its computer systems and network[508]. Demon, the British Internet Service Provider, was awarded £250,000 when a defamation case was settled in the High Court in early 2000. Norwich Union ended up paying £450,000 in compensation when email of one of its employees libelled a competitor[509]. Some reported extortion cases show that a company is likely to face an absolute minimum of a £10 million ransom in the event of cyber extortion (Table 5.4).

Table 5.4: The reported cyber extortion cases

Ransom	Threats and their target industries
10 million	A computer crash threat against a British brokerage house
12.5 million	Blackmail threats against a British bank
10 million	Blackmail threats against a British brokerage house
10 million	Threats against a British defence firm

Currency unit: Pounds sterling.
(Reference: See 'COMPSEC 2001, Recent Cases of Electronic Fraud and Recovery', <http://www.pcbsols.com/links/compsec_2001.htm> (print out on file with author).

The above Visnet and Adidas cases do not relate to financial institutions. However, similar incidents are very likely to happen to financial institutions and the losses could be worse. On the other hand, financial institutions are very likely to be targets of cyber extortion. The most costly expenses in the Visnet case were loss of income as a result of business interruption and extra expenses; it was not physical property

[506] Bisciglia pleaded guilty to unauthorized access and computer damage and faced either up to a year in prison or US$100,000 fine. See 'Prepare for the worst', *supra* n.490, and 'Got Cyber Insurance?', <http://www.compuerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47_STO48721-,00.html> (print out on file with author).

[507] See 'Domain War Motive a Guess', <http://www.wired.com/news/business/0,1367,35708,00.html> and "Serb hackers' on the rampage', <http://news.bbc.co.uk/1/hi/world/europe/712211.stm> (print out on file with author).

[508] The information was obtained from an interview with Willis Limited.

[509] See 'Cyber liability insurance', <http://www.tyseruk.co.uk/cli.html> (print out on file with author).

damage of computers and servers. It is, in reality, not impossible to estimate how much computers and their equipment cost in case of breakdown whatever the cause is. In addition to this, replacing damaged computers and servers generally will not be an enormous claim against insurance companies and underwriters. The most crucial and intrinsically exorbitant risk is, without doubt, liability. In general, liability claims are very likely to remain uncertain depending on the situation but they could be huge. If a party files a suit against a company, and if the court judges the claim of the plaintiff reasonable, legal costs as well as financial compensation seem to be unavoidable for the defendant. Involving cyberspace in businesses makes liability issues more intricate. In essence, potential, litigious enemies for a company are within the scope that its own products or services reach. However, if it is involved in cyberspace, due to its nature, there is no wonder it may conflict with anyone from anywhere in the world. None of the above cases state whether or not the companies had cyber insurance, except the Visnet case where the company only had traditional products. However, considering the time of the attacks against Adidas, it was unlikely to have purchased cyber insurance since such insurance was not popular at the time. It is worthwhile to examine some specific risks of what is likely to damage businesses in connection with cyberspace:

1) Cyber liability

If Company X contains any cyber items connected with its business, such as emails, websites or intranet, they could cause trouble for X itself. For instance:

(a) X, unknowingly, could infringe intellectual property rights;
(b) Following a rush of published corporate homepages, cybersquatting[510] gave birth to a new type of a threat;
(c) Defamatory messages against X could be distributed by emails or posted on a website;
(d) X could breach confidence or invade someone's privacy;
(e) X could negligently distribute a computer virus, logic bomb or the like and interrupt a third party's business; and
(f) If a hacker gets unauthorized access to X's computer data, obtains X's electronic signature, electronic certificate or the like, and swindles a third party in good faith for his/her own purposes for the purpose of criminal gain.

---

[510] "Cybersquatting" is explained in the U.S. federal law known as the Anti-Cybersquatting Consumer Protection Act as "registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else". A 'domain name' is defined in the World Intellectual Property Organization (WIPO) as 'an alphanumeric string that corresponds to a numerical address on the Internet.' See 'searchWebManagement.com Definitions', <http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci213900,00.html > and 'Publication 833 Joint Recommendation & Article 1', <http://www.wipo.int/about-ip/en/development_iplaw/pub833-01.htm> (print out on file with author).

This is likely to exclude covering liability if it is caused as a result of an employee's dishonest act.

2) Cyber damage
Damage to electronically kept data, websites, intranet, computer systems, and/or computer network is likely to be made by a hacker. This also includes a hacker copying or stealing X's data or programmes. If the said damage occurs, the expenses for replacement or repair would be covered. If a policy is just for cyber liability, this clause would not be included.

3) E-commerce fraud
As it is mentioned in 1), a hacker could obtain X's electronic signature, electronic certificate or the like by unauthorized access. The outcome of X's electronic signature being used for fraudulent purposes is that X is likely to deliver a substitute: products, money and so on. The financial losses X sustains would be covered.

4) Loss of income (i.e., protecting revenue)
If attacks occurred within the remit of 2), X's business is very likely to be interrupted. This would result in loss of income. This clause mostly involves "time retention" which excludes a certain period of time from the whole incident period. That is to say that only losses for consecutive hours in excess of a certain time are covered.

5) Cyber Extortion
Like Cybersquatting, this is a new risk. A third party threatens X and demands ransom money. The difference to a traditional extortion crime is that all the blackmailer needs is his/her computer skills to kidnap or hijack the safety and integrity of a computer system, computer data and the like: he/she threatens to damage, destroy or spread a computer virus to the said items. X's confidential information, such as trade secret, is also in danger of being kidnapped. Not only the ransom but also the negotiators' or risk consultants' expenses are covered. The negotiators or risk consultants (contracted by insurance companies or underwriters) not only negotiate with the blackmailer but also judge whether the blackmailer has adequate skills to fulfil his/her threats[511].

6) Cyber crime committed by an employee
X's employees, excluding directors and officers, can get unauthorized access very easily and commit further crime. If any cyber content is damaged, destroyed, misused or copied for personal gain, replacement and repair expenses.

---

[511] The author is grateful to Mr R. Coello, Account Executive, and Mr J. Naish, Advisor of Global Financial & Executive Risks Practice, Willis Limited for their invaluable comments and advice.

7) Charge-backs
"Charge-backs" are defined in a policy of Tyser (UK) Limited as sums X wants to be reimbursed for the cost of goods or services bought by a customer which his/her bank did not honour. Although Tyser's Comprehensive Esurance Policy covers this, some insurance companies are reluctant to cover charge-backs.

Exclusions exist: firstly, and obviously, if an accident or incident occurs which falls outside the remit of the seven risks, then damages or losses incurred are not covered; secondly, specific exclusions within the remit of the seven risks could be included in policies taken out by different companies. The most common exclusions are the losses incurred in relation to nuclear explosions, terrorism and war[512].

Rossi said risks are divided into two categories: first and third party risks[513]. First party risks contain natural peril property damage, employee dishonesty, third-party crime and malicious conduct, extortion, computer programming errors, business interruption and extra expense. Third party risks literally contain liability for damages of a third party who has been in good faith. The tables below show a comparison between cyber insurance and traditional insurance depending on the type of risks (Tables 5.5 & 5.6[514])

[512] The above information is arranged after comparing insurance policies the author was given by some underwriters and obtained online. For the purpose of their business interests, the names remain anonymous. The author would like to thank the companies for their frankness. A Specimen Policy of Tyser's Cyber Liability Insurance is available online from <http://www.tyseruk.co.uk/esurance.pdf> (print out on file with author).
[513] See 'First-Party E-Commerce Risks', <http://www.irmi.com/expert/articles/rossi002.asp> (print out on file with author).
[514] Tables 5.5 and 5.6 were completed adding some extra risks in relation to this context. The original tables were given by Mr R Coello, Account Executive of Willis Limited, and the author has his permission to arrange them for this thesis. The author would like to thank him for his frankness and generous advice. The author is to blame for any unintentional or incorrect typographical errors or characterisation. The author would like to thank him for his frankness and generous advice.

Table 5.5: First party risks

(Loss to property including Extra expense, Business Interruption, Forensics and Public Relations)					
Type of risks	**Cyber insurance** (Information assets)	**Property** (Physical damage to tangible property)	**BBB** (Money, securities, other property)	**CCP** (Money, securities, electronic data)	**Kidnap & Ransom**
Denial of Service - no direct or indirect physical loss to data or systems	C	N	N/A	N	N/A
Human/administrative error	C*	Q	N/A	N	N/A
Unauthorized disclosure, copying of proprietary, private or confidential information	C	N	N	N	N/A
Destruction, alteration, erasure, corruption of data by:					
Virus	C	N	N/A	C1	N/A
Malicious attack	C	N	Q	C1	N/A
Extortion against information assets:					
Divulge trade secret or confidential information	C	N	N/A	N	C
Any other information or system	C	N	N/A	N	N
Introduction of virus	C	N	N/A	N	C
Publicity of data alteration	C	N	N/A	N	C
Ransom monies	C	N	N/A	N	C
Business interruption	C*	N	N/A	N	Limited
Computer Fraud - theft of monies or transfer of goods by:					
Employee	N	N	C	C	N/A
Non-employee	C*	C2	C	C	N/A
Theft or loss of trade secrets	C*	N	N	N	N/A
Patent / copyright infringement	C*	N/A	N/A	N/A	N/A

(Continues from the previous page)

Type of risks	Cyber insurance	Property	BBB	CCP	Kidnap & Ransom
Repudiation of access	C*	N	N/A	N	N/A
Theft of digital certificate	C*	N	Q	Q	N/A
Telecommunications theft	C	N	N	Limited	N/A
Hacking of smart / access cards	C*	N	Q	Q	N/A
Mobile Commerce (M-Commerce)	C	N	Q	Q	N/A
Server side E-Wallet -Electronic systems and communications/ data protection/ credit card fraud/ liability for encryption	C	N	Q	Q	N/A
Software lack of performance	C*	N	N	N	N/A
Use of third party (ASP- Application Service Providers) Infidelity/ errors/ data protection/ business at ASP	C*	N	N	N	N/A
Aggregation services (theft of monies is excluded since it is possible to fall into computer fraud)					
as its service provider attacked to destroy, alter, erase, corrupt of data or systems by:					
Employee	N	N	Q	N	N/A
Non-employee	Possible	N	Q	Possible	N/A
Extortion threat	Possible	N	N/A	N	Q
as a business partner of its service provider attacked to destroy, alter, erase, corrupt data or systems by:					
Employee	N	N	Q	N	N/A
Non-employee	Possible	N	Q	Possible	N/A

C = covered.
C* = Coverage available under specific e-risk products/tailoring.
Q = Questionable coverage.
N = No coverage.
N/A = Not applicable to this policy.

C1 = Covered destruction or damage but not Business Interruption.
C2 = Covered for theft of physical property only.

Table 5.6: Third party risks

(Defence costs and indemnity payments)					
Type of risks	**Cyber insurance** (wrongful act -Internet, technology, enterprise network & multimedia)	**Commercial General Liability (CGL)**	**Bankers' Professional Liability** (wrongful act from professional services)	**Electronic Crime** (Defence and indemnity)	**Technology Errors & Omissions** (covers OTX only for technology services)
Errors & Omissions including unauthorized access					
Professional banking services	C*	N	C	C3	N
Internet services	C	N	Q	C3	C-OTX
Technology services	C	N	Q	N	C-OTX
Virus transmission	C	N	N	N	C-OTX
Aggregation services as its service provider	Possible	N	Q	Q	Possible C-OTX
Advertising online					
Broad media perils	C	Q-limited	Q-limited	N	C-OTX
Publishing /Multimedia					
Broad multimedia perils	C	Q-limited	Q-limited	N	C-OTX
Privacy violations	C	Q-limited	Q	N	C-OTX
Chat room /bulletin board	C	Q-limited	Q-limited	N	Excluded if edited or censored by the Assured
Software development and/or sales	C	N	Q	N	C-OTX
Software copyright infringement	C*	N	Q	N	C-OTX
Software patent infringement	C*	N	N	N	N
C3 = Covered for hacker virus damage to customer data.					

The polices are compared by the various types of potential risks and crimes. Cyber insurance covers approximately 96% of first and 100% of third party risks relating to cyber risks. Contrary to this, other traditional products cover less than 20% of first party risks. With regard to third party risks, the Technology Errors & Omissions Policy covers approximately 70%, however other traditional products cover, again, less than 20% of risks[515]. Insurance companies deal with duplicated coverage. The cyber risks thus far seem to be fully covered, although covering the risks in relation to aggregation services remains to be seen since it has just been introduced in the financial market. Technically, the risks are covered by insurance to some extent. The points are that, firstly, a new type of risk needs time to be judged and secondly, a decision must be taken as to which policy should take care of it. Therefore, a company must be cautious in the face of new cyber risks, or before using any services in cyberspace which may or may not be covered.

So, what types of cyber insurance are actually available on the UK market? The table below is a survey of cyber insurance mainly in the USA, as well as in Europe and Australia (Table 5.7). In fact, the cyber insurance market in the USA is livelier than anywhere else. As is universally known, the notion of liability is fully developed in the USA. The UK insurance market follows that of the USA but it does not exceed it[516]. It is, therefore, no wonder that the US market (more than any other) is far more keen on developing and purchasing cyber insurance. Furthermore, international foreign capital insurance companies, such as AIG, Chubb and Zurich, run insurance businesses in the UK and Europe. Safeonline Limited, for instance, has done business for four years in the UK and two years in the USA. By 2002, the great majority of customers were in the USA[517]. Those who have businesses in multiple countries tend to supply similar or the same cyber insurance to the original products (supplied in the USA) in the UK and Europe.

[515] The risks in aggregation services are excluded.
[516] The information was obtained from an interview with Lloyd's Japan.
[517] The author is grateful to Ms S. Alton of Safeonline Limited for her invaluable comments and advice.

Table 5.7: Stand Alone E-commerce Market Survey

Insurer, Managing General Agent, or Insurance Broker	Policy Name	3rd Pty. Crime	Employee Dishonesty	BI and EE	Extortion	Prof. Svcs. Liab.	Media E&O Liab.
Policies Sold in the U.S.							
AIG	NetAdvantage Pro + Internet Professional Liability Policy	No	No	No	No	Yes	Yes
	NetAdvantage Security + Internet and Computer Network Security Policy	Yes	Yes	Yes	Yes	No	Yes
	Net Advantage Liability Internet and Professional Security Liability Insurance	Partial*	Partial*	No	Yes	Yes	Yes
	ProTech Technology Liability Insurance Policy	No	No	No	No	Yes	Yes
	Cyber Security	Yes	Yes	Yes	Yes	No	No
Chubb Executive Risk	Safety'Net Internet Liability Insurance	No	No	No	No	No	Yes
Hiscox	Hacker Insurance	Yes	Yes	Yes	Yes	Yes	Yes
Legion Indemnity Company	INSUREtrust Electronic Information E&O (EIE&O) Liability Policy	Partial*	Partial*	No	No	Yes	Yes
Lloyd's	Computer Information and Data Security Insurance	Yes	Yes	Yes	Yes	Yes	Yes
Lloyd's (WISP)	Website Crime & Intranet Insurance	Yes	Yes	Yes	Yes	Yes	Yes
Lloyd's (Besso)	Technology, Media and Professional Liability Insurance	No	No	No	No	Yes	Yes
Lloyd's (JLT Risk Solutions)	E-Comprehensive	Yes	Yes	Yes	Yes	Yes	Yes
Marsh	NetSecure	Yes	Yes	Yes	Yes	Yes	Yes
Media/Professional Liability (Gulf)	CyberLiability Plus Insurance Policy	No	No	No	No	Yes	Yes
Royal Surplus Lines	Computer, Telecommunications and Internet Services Liability Coverage	No	No	No	No	Yes	Yes
St. Paul	Technology Premier Computer Network Security Protection (Networker)	Yes	Yes	Yes	Yes	No	No
	Cybertech+ Liability	No	No	No	No	Yes	Yes
Tamarack (Great American)	Dot.Com Errors and Omissions Liability Insurance Policy	No	No	No	No	Yes	Yes
Zurich North American Financial Enterprises	E-Risk Protection Policy	Yes	Yes	Yes	Yes	No	Yes
Policies Sold in Europe							
ACE Europe	DataGuard	Yes	Yes	Can be added	Yes	No	No

Hiscox	Hacker Insurance	Yes	Yes	Yes	Yes	Yes	Yes
Lloyd's (JLT Risk Solutions)	E-Comprehensive	Yes	Yes	Yes	Yes	Yes	Yes
Marsh	NetSecure	Yes	Yes	Yes	Yes	Yes	Yes
Park Insurance Services	Internet Insurance	No	No	No	No	Yes	Yes
Zurich North American Financial Enterprises	E-Risk Protection Policy	Yes	Yes	Yes	Yes	No	Yes
Policies Sold in Australia							
Marsh	NetSecure	Yes	Yes	Yes	Yes	Yes	Yes
St. Paul	Technology Premier Computer Network Security Protection (Networker)	Yes	Yes	Yes	Yes	No	No
	Cybertech+ Liability	No	No	No	No	Yes	Yes

* Partial: for liability arising therefrom.

(Reference: See Stand Alone E-Commerce Market Survey, July 2001, by Michael A. Rossi, Insurance Law Group, Inc., <http://www.irmi.com/expert/articles/rossi004chart.asp> (print out on file with author).

The following table presents some products available in the UK market (Table 5.8).

Table 5.8: UK cyber insurance businesses

Name	Property damage	Cyber liability
ACE Insurance S.A.-N.V. (UK branch)	ACE fraudProtector - Comprehensive Crime Insurance	applicable
AIG Europe	applicable	AIG netAdvantage Suite (SM)
Beazley	N/A	AFB Skinny Tech (SM)
Hiscox Syndicates Ltd	Covered by Cyber Insurance to some degree	Cyber Insurance
Media/Professional Insurance	applicable	CyberLiability Plus (TM)
Safeonline	SafeData SageAsset	SafeEmail SafeEnterprise
St. Paul International Insurance Company	applicable	Cybermedia Liability Network Security
Some related brokers registered in Lloyd's		
Dickson Manchester and Co Ltd		
Holman Insurance Brokers Limited		
MRM Intermediaries Limited		
Swinglehurst Limited		
(Reference: The information was obtained through the websites, particularly Lloyd's.com, <http://www.lloyds.com/> as well as by direct enquiry by the author. The author is to blame for any unintentional incorrect mistyping or characterization.)		

Now that it is clear what types of risks exist in relation to cyber insurance and how cyber insurance covers such risks, the next question is how far an assured is covered. The loss scenarios Chubb have prepared show that:

1) a bank is likely to suffer a direct loss of US$ 750,000 as a result of e-theft (hacking into a bank's network, creating fake accounts, debiting the accounts and withdrawing money immediately);

2) Certain financial institutions could be held to a US$1 million ransom over credit card numbers. This type of threat seems to be easily leaked into the public domain. As a consequence of this series of occurrences, the institutions involved would also lose their good reputation as well as customer confidence. These incur extra expenses for public relations;

3) a bank is likely to suffer a direct loss of US$1.5 million dollars as a consequence of an e-signature being stolen or altered and used for fraudulent purpose [518].

The highest coverage of property damage by cyber insurance is said to be up to US$200 million; its premium ranges from $10,000 to $25,000 per million per annum. For up to $1 million, coverage of liability starts at $2,500 per annum. A premium of $7,000 per annum for $1 million is necessary to cover computer crime. The premium of Business Interruption coverage on e-commerce sales is $50,000 to $70,000 per annum. It covers sixty days' business outage for a company which earns $40 million per annum online. For a smaller company, $1,000 or $2,000 per annum will do for $100,000 coverage[519]. Other indices are $1,000 minimum premium for a coverage limit of $250,000 or split limits of $100,000 to $300,000, or $2,500 minimum Self-Insured Retention for each loss [520]. These are, however, merely examples. The premiums of products differ from the size of the assured's businesses, the composition of the product itself, which risks the assured prefers to be covered and so on Taking SafeEmail as an example, this product is developed for covering liability targeted at small companies, such as those employing up to 250 people. It works in the event that an email or an instant message sent by an employee causes any problem, such as defamation, infringement of privacy, or the transmission of a computer virus. The premium for covering 250 email users would be $8,000 for the coverage limit of from

[518] See 'CyberSecurity by Chubb[SM] for Financial Institutions', <http://www.chubb.com/businesses/dfi/cyber/index.html> (print out on file with author).
[519] See 'The Policy of Protection', <http://www.nwfusion.com/research/2000/1023feat2.html?nf> (print out on file with author).
[520] See 'Greenhalgh Insurance Insurance Cyber Liability', <http://www.greenhalghinsurance.com/cyber.html> (print out on file with author).

$100,000 up to $1 million[521].

In addition, there is a report stating that a computer using the Windows NT operating system (OS) is more vulnerable security-wise than if it were to use other systems. Thus, an insurance company called Wurzler Underwriting Managers, Inc. imposes 25% extra on its anti-hacking policy for companies using Windows NT OS. Leyden argued this stance was unfair since having tight security is far more important than the products (=OS) being installed in computers and security is likely to be dependent on the infrastructure of computer hardware[522].

As to the extent of capacity of cyber insurance, some insurance companies prefer to keep their limits to US$2 to 3 million for first party risks whereas some companies offer a bigger capacity[523]. In regard to the third party risks, it has a wide range from $10 to 15 million; for example, AIG covers up to at least $25 million[524]. Safeonline commented that it sets the limit up to $25 million in general[525].

3. The issues of cyber insurance

3.1 Tangible or intangible?

Notwithstanding the discussions above, cyber insurance remains a newborn baby in any insurance market. To be a mature insurance product, it is necessary to have plenty of time to develop and analyse the product as well as the risks it covers. Furthermore, cyber businesses themselves have still been developing and changing day by day. Technically it is seriously difficult for the insurance industries to catch up or forecast the kaleidoscopic evolution of cyberspace and each brand-new risk occurring therefrom. It is impossible to predict what type of brand-new services would be developed or what type of new offence a high-tech maniac would commit in cyberspace in the future. Hence it is useless to ponder how new risks attending to new services or offences should be covered. It is more practical to direct attentions at what is always directly at risk: computer data and the like, intellectual property and privacy[526]. Even if any new service or offence is established, the potential direct damage

---

[521] See 'Digital Insurance Now Available for IM', <http://www.instantmessagingplanet.com/enterprise/article/0,,10816_1141401,00.html> (print out on file with author).

[522] See 'Anti-Hacking premiums 25% higher for Win NT', <http://www.theregister.co.uk/content/8/18324.html> (print out on file with author).

[523] See 'New Stand-Alone E-Commerce Insurance Policies for First-Party Risks', <http://www.irmi.com/expert/articles/rossi006.asp> (print out on file with author).

[524] See 'New Stand-Alone E-Commerce Liability Insurance for Third-Party Liability Claims (Part 1)', <http://www.irmi.com/expert/articles/rossi004.asp>, 'Technology and Cyber risk', <http://www.tennant.com/p-cyber.html> (print out on file with author) and 'Greenhalgh Insurance Cyber Liability', *supra* n.505.

[525] The information was obtained from an interview with Safeonline Limited.

[526] A good reputation could be indirectly at risk, however an indirect damage is out of this context.

would be very likely to be done against one (or all) of these three items. In other words, whatever happens in the future, it is unnecessary to worry as long as the said three items are covered by insurance products.

There has been an unsolved issue for a long time not only in insurance markets but also in the legal field: whether computer data is "tangible property" or "intangible property". This is the biggest conceptual point at issue in relation to cyber insurance's first party risks. It is because traditional insurance products generally use the term "property damage" and cover physical damage or injury to tangible property, or the loss of its use[527]. There are two issues behind this; firstly, if computer data is intangible property, whether it is impossible to cover the loss of computer data being damaged. Secondly, it is whether altering, damaging or corrupting computer data is to be judged as physical damage or not. Since computers have existed for more than a few decades, computer data has also existed for the same amount of time. Without any slightest influence of this, these two points at issue remain uncertain. In addition to this, there is a related issue. The term used in this context, "computer data and the like" is actually very ambiguous. To be precise, this means electronically recorded or stored information, such as computer data, programmes, software and other media[528]. If so, what about web contents? Can the information contained on a website be included in this category?

There is, of course, a last resort if cyber insurance, without using the term "property damage", defines in the policy that damage or loss of computer data is covered. However, as this will be discussed as the next issue, some companies, big companies in particular, are likely to prefer not to purchase a stand-alone insurance policy such as cyber insurance[529]. Thus, it is advisable not to exclude traditional insurance products from covering cyber risks.

In 1990's in the USA, the said issues were referred to by some court decisions but no definite answer was given. So it is said that the approach of the Y2K issue was confused[530]. Technically speaking, computer data is not visible and touchable unless it is kept in any media, therefore it is judged as intangible property. However, businesses are not that simple. No one would deny that computers are deeply involved in today's businesses. Data assembled by computers are the assets of a

---

[527] See 'Third-Party Liability E-Commerce Risks and Traditional Insurance Programmes', <http://www.irmi.com/expert/articles/rossi003.asp> (print out on file with author).
[528] See 'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 1', <http://www.irmi.com/expert/articles/rossi008.asp> (print out on file with author).
[529] See 'Bringing Order to Chaos Insurance Issues for E-Commerce Activities', <http://www.irmi.com/expert/articles/rossi001.asp> (print out on file with author).
[530] See 'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 1', *supra* n.513.

company without doubt. From an assured's viewpoint, data, as intangible property is often more important than computers, substitutable tangible property. As long as computer data and the like are consciously or unconsciously accepted as "property" by companies in general, there is no surprise in their belief that "such asset" is covered by insurance products they have purchased. Unfortunately this does not arouse sympathy from insurance companies. Thus, the issues over whether the loss of computer damage and the like is covered by traditional insurance products or is to be subject to the "physical loss or damage" clause, must be clearly presented.

Examining the legal aspect, computer data and the like are intangible property in the UK. Thus, the Criminal Damage Act 1971 was not applicable to criminalise the accused in *Cox v. Riley* (1986) 83 Cr App Rep 54 in the time of 1986 since "property" is defined in section 10 as "a tangible nature"[531]. However, the Computer Misuse Act 1990, in effect since 1st September 1990, has criminalised unauthorized access to computer material, unauthorized modification, and further offences[532]. This enables the criminalisation of the offender who damages or alters intangible property, i.e., computer data and the like.

Apparently Japan had a similar situation until the Unauthorized Computer Access Law (UCAL) came into effect on 13th February 2000; although its criterion for criminalising an offence had been whether or not any damage was given[533]. In general, there is no doubt that law is not established to protect something meaningless; some legal interests must exist beneath each Act. Unmistakably, both the British Computer Misuse Act 1990 and the Japanese UCAL target to protect computer data and the like from being damaged or altered. That is to say, it is possible to conclude that they are basically the assets which need to be protected whether they are recognised as tangible or intangible property. Criminal law is, of course, different from civil law. Even if criminal law is in the interest of protection, civil law in relation to insurance law does not follow this straightforwardly. Insurance is based on contract; if a clause that clearly defines tangible property does not involve computer data and the like, and if both an assured and an insurer signed the contract document, it is hardly possible to be overturned. As *Retail Systems, Inc. v. VNA Insurance Cos.*, 469 NW2d 735 (Minn App 1991) in the USA shows, it may be possible to cover the loss if media-stored information (such as a disk) is lost since media is tangible. However, this case was resolved due to the existence of media: no suggestion was given to the issue of tangible property[534]. It would be practical to switch the issue to whether damaging or altering computer data and the like would physically damage tangible

---

[531] See 'Case: Cox vs. Riley (1986)', *supra* n.252. The details of the case are discussed in depth in Chapter II.
[532] See 'Computer Misuse Act 1990 (c. 18)', *supra* n.255.
[533] The details are discussed in depth in Chapter II.
[534] See 'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 1', *supra* n.513 and *infra* n.522.

property. In the *Bellwether Ingram Micro* case, the computer data of the assured was lost as a result of power outage, and the company lost data processing capability for several days until the default system was replaced. When the insurer argued there had been no physical damage since the assured had had the replacement, the court commented that:

> "'Physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes the 'loss of access, loss of use, and loss of functionality."

Rossi concluded the case proposed that if computer data within a computer is damaged, it means the computer itself is physically damaged[535]. This view may sound somewhat radical. However, it is surely reasonable to consider that computer data and the like are stored contents with the computer itself as a receptacle. If a pair of them are marred, the damage or loss should have coverage possibilities. In regard to the web contents, the differences from computer data and the like are that the web contents are stored in a server computer and are public. In a sense, judging from the public exposure, such information is more at risk than others. As long as the web contents are the assets of a company, there should be no reason to differentiate them from computer data and the like.

On the other hand, the case law is likely to support coverage of third party risks, considering computer data as tangible property. The underlying theory is the same as the Retail Systems case mentioned earlier[536].

In practice, there are some insurers in the USA who have paid for claims, including computer data damages or losses, under traditional commercial insurance policies with the issues of tangible or intangible yet unresolved. In addition to this, some companies present their positions — that computer data is considered as tangible property — in their policies[537]. However, it is evidently not the mainstream.

3.2 The approach to purchasing insurance products

There are likely to be two different approaches to purchasing insurance products covering risks associated with cyberspace: firstly, to amend or add to existing policies of an assured; secondly, to purchase an

---

[535] American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc., 200 U.S. Dist LEXIS 7299 (D Ariz Apr. 18, 2000), see 'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 1', *supra* nn.513 and 519, and 'American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc', <http://www.phillipsnizer.com/int-art199.htm> (print out on file with author).

[536] See 'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 2', <http://www.irmi.com/expert/articles/rossi009.asp> (print out on file with author).

[537] See 'Is Computer Data Tangible Property or Subject to Physical Loss or Damage Part 1', *supra* nn.519 and 521.

insurance product just to take care of cyber risks. The latter type of product is generally called a stand-alone insurance product.

To date, without any doubt, the great majority of companies have some commercial insurance products. Whether or not they have insurance products to cover cyber risks depends upon two points: to what extent they know of or have interests in cyber risks as well as whether they have money to spare for purchasing cyber insurance.

The report published by the *Fortune 500* companies and associations disclosed to what extent cyber insurance and the like had been disseminated by 2000:

* Electronic Data Processing Insurance that extends beyond general business liability policies (14%);
* Specialized Network Security Insurance (17%);
* Media Liability Insurance (22%);
* Patent Infringement Insurance (27%);
* Computer Software and Services Errors & Omissions Insurance (31%);
* Product Liability Insurance (42%); and
* D&O Insurance (53%)[538].

The year 2000, was, in a sense, the memorial year that cyber insurance made its début in the markets. So there is no surprise in the low saturation level of insurance illustrated in the figures shown above. Another possible reason for this, as briefly mentioned earlier, is due to how companies arrange insurance products. Small and medium companies, and newly established Dot.com companies in particular, are very likely to purchase a stand-alone insurance product. The reasons are explained that, first and foremost, stand-alone cyber insurance is to be an exact policy with which the risks of a company are concerned. Of course, how close cyber policy is to the point depends on each industry or business type. Secondly, they are unlikely to have abundant funds and risk management experiences, especially at the initial stage of their businesses. A ready-made product will therefore suffice rather than an order-made one[539].

Even if cyber insurance is the targeted product to purchase, an assured must carefully confirm the details. The meanings of the technical terms for insurance are not always exactly the same as in daily life, or are likely to be limited in a certain way, although this tendency applies to all types of insurance products to some degree. Some points an assured should confirm with an issuer are[540];

---

[538] See 'Survey Reveals Business Not Prepared for E-Risks', <http://insurancejournal.com/html/ijweb/breakingnews/archives/national/na0700/na0731004.htm> (print out on file with author).

[539] *Ibid.*

[540] See 'Investigating International Developments in eCommerce Insurance Policies',

- The definition of "professional services"[541];
- Whether or not losses as a result of the items listed below are covered under the policy:
  1. Claims in relation to others' activities[542];
  2. Infringement of intellectual property;
  3. Trade secrets or other confidential information;
  4. Natural perils;
  5. Innocent computer programming errors;
  6. Negligent act, error or omission;
  7. Liability assumed by contract;
  8. Liability to others caused by employee dishonesty or crime;
  9. Liability to others caused by third- party theft;
  10. Business interruption and extra expense to contingent risks.

Contrary to small and medium companies, the *Fortune 1000* companies are not pleased to purchase any type of stand-alone insurance product. This is because the more a company purchases a stand-alone product, the more trouble it incurs, such as negotiating and administrating. Large companies are eligible to have an order-made insurance policy to cover all risks in each business line. That is to say, there is only one wording for covering many different risks in different business lines. Although an order-made type policy is far too expensive, it is easy and convenient not only to understand the concept of the policy but also to administrate it from an assured's point of view. In practice, uncovered risks (by insurance) for large companies would be newly developed risks only; in other words, cyber risks. Such risks are just like chinks between other covered risks. It is natural that companies prefer to tweak the existing policy to fill them in[543].

Rossi proposed to the assureds how clauses should be amended by insurance products as follows[544]:

Potential Changes to Property Policy
* To add clear language covering losses as a result of "denial of service attacks" as well as "non-physical events";
* To explain precisely indemnity period provisions for time element

---

<http://www.inslawgroup.com/pdf/marcusevans020801ppt.pdf> (print out on file with author) and 'New Stand-Alone E-Commerce Insurance Policies for First-Party Risks', *supra* n.508.

[541] The definition of 'professional services' varies from each insurance company. See 'You say Professional Services, I Say B2B Activities', <http://www.irmi.com/expert/articles/rossi010.asp> (print out on file with author).

[542] It is assumed that 'banner ads', 'links' and the like on an assured's website are likely to infringe a third party's right. See 'Investigating International Developments in eCommerce Insurance Policies', *supra* n.525 and *infra* n.529.

[543] See 'Bringing Order to Chaos Insurance Issues for E-Commerce Activities', *supra* n.514.

[544] See 'Investigating International Developments in eCommerce Insurance Policies', *supra* nn.525 and 527.

losses involving e- commerce activities;
* To consider the issues when services are interrupted and a contingent time element;
* To make liability issues clear for the occurrence of others' property losses under an assured's care, custody or control;
* To beware of "computer virus" exclusions (to be discussed as the next issue).

Potential Changes to Crime Policy
* To ensure business interruption coverage for employee dishonesty;
* To add clear language covering losses involving media;
* To add clear provisions covering an assured's liability for theft of property of others (i.e., a case when customers' credit card information is stolen)
* To add clear provisions covering cyber extortion risks.

Potential Changes to Kidnap & Ransom Policy
* To add clear language covering cyber extortion risks that computer data, software, programmes, media and the like that are likely to be in jeopardy, such as;
  → threat of introducing a computer virus;
  → threat of hacking into the computer system to corrupt, delete or otherwise disrupt;
  → threat of "non-physical events", such as a denial of service attack;
* To add clear language covering business interruption and extra expense when a policy is triggered, and how the coverage works.

Potential Changes to CGL/Umbrella Policy
* An assured has to consider whether it wants coverage for infringement of privacy. If necessary, the language "publication or utterance" must be deleted;
* To consider whether it is necessary to have a clear definition of computer data and the like as "tangible property";
* To consider whether an assured wants to build coverage for professional liability, media liability and intellectual property infringement for e- commerce activities and otherwise into this policy.

Potential Changes to Professional Liability Policy
* To consider whether an assured wants to cover the losses of its customers, vendors and the like replied to on its website, intranet and other services;
* To consider whether an assured wants to cover liability for hosting a website;
* To consider whether an assured wants to cover media liability and liability for infringement of intellectual property in relation to cyberspace activities;
* To consider whether it is necessary to have a clear definition of computer data and the like as "tangible property";

Potential Changes to Media Liability Policy

* To consider whether an assured wants to cover technology errors and omissions (products and services, hardware and software);
* To make sure whether the IP infringement coverage extends to the computer data and the like on the website, network, computer systems and so on.

The majority of insurers were said to have been reluctant to amend their policies to cover cyber risks[545]. However, this could change depending on how markets respond. Kae Lovaas, president, Global Technology Underwriting, the St. Paul Companies, addressed that despite two years of cyber insurance availability in the US market, the demand had not been much until the last six months of 2000[546]. Nonetheless, the cyber insurance market is hardly successful even at present. An insurance company described itself as unsuccessful for three years by mid-2002, due to the slow growth of customer demand[547]. The leading factor in cyber insurance's popularity in 2000, as above mentioned, was because interests upon such policies are accelerated as a consequence of serious denial-of-service attacks and e-mail viruses. This proves that a serious incident will definitely and easily attract huge attention from the general public.

3.3 Exclusion clauses

There is no insurance policy without exclusions. How can an assured cover the losses falling under the exclusion clauses that it believed to be covered by the policy? The greater the losses, the more fatal to the assured they are likely to be. This is proved by the Visnet case above-mentioned. There are some points in a policy for a potential assured to regard cautiously, as mentioned in 3.2. A typical example of this is an incident involving a computer virus.

The following is a sample of exclusions named 'NMA 2914' prepared by the Non Marine Association in London;

"1. Electronic Data Exclusion

Notwithstanding any provision to the contrary within the Policy or any endorsement thereto, it is understood and agreed as follows:

a. This Policy does not insure, loss, damage, destruction, distortion, erasure, corruption or alteration of ELECTRONIC DATA from any cause whatsoever (including but not limited to COMPUTER VIRUS) or

---

[545] See 'First-Party E-Commerce Risks', *supra* n.513.
[546] See 'The Policy of Protection', *supra* n.504.
[547] Here the company name remains anonymous by request. The author would like to thank the company for their frankness and generous advice.

loss of use, reduction in functionality, cost, expense of whatsoever nature resulting therefrom, regardless of any other cause or event contributing concurrently or in any other sequence to the loss[548]..."

It seems to be assumed that both the UK and the European insurance markets believe that computer viruses cannot cause physical damages against computer equipment and the like. This leads to the consequence that no insurance policy would be triggered for covering the first party property damage caused by a computer virus[549]. Besides, neither kidnap and ransom policy nor cyber insurance are also likely to be triggered; for instance, AIG is said to have decided to exclude potential losses from its policy in case extortion threats of implanting a computer virus are carried out. It is surmised that computer viruses generally attack any computer or network system where they arrive[550]. In other words, they attack everything whether it is a specific target or not — can not attack only the target without harming any other non-targeted objects[551]. Therefore, the potential losses would be unlimited.

To make the situation even worse from the assureds' viewpoint, in of May 2002, it was said that reinsurance companies were likely to support the computer virus exclusions for reinsurance renewals in 2002[552]. If reinsurance is unavailable, the majority of cyber insurance policies and the like will immediately consider adding the exclusions, or at the very least taking appropriate precautions.

3.4 The issues of jurisdiction

Needless to say, cyberspace has no boundary; a claim could be made by anyone from anywhere in the world. An assured's property could be potentially damaged by a hacker thousands of miles away, or the assured could infringe a third party's intellectual property rights on the other side of the earth. It is, however, not an issue to consider the first party losses. They are generally covered by an insurance policy that is domiciled in its country of origin. However, it is critical for third party liability claims to be considered. A certain cyber insurance policy maintains that it applies to claims made anywhere in the world[553].

---

[548] See 'The End of Computer Virus Coverage as We Know It?', <http://www.irmi.com/expert/articles/rossi011.asp> (print out on file with author).
[549] *Ibid.*
[550] The information was obtained from an interview the author had pursued. Here the company name remains anonymous by request.
[551] There was serious loss caused by a malicious computer worm called 'Code Red' in July 2000. It was programmed to target the White House on 19th July. That is to say that a computer worm is able to attack a specific IP address (not a URL). However, it infected approximately 300, 000 corporate computers within two weeks. Thus, it is possible to describe the series of Code Red incidents as indiscriminate attacks. See 'Code Red Dormant--For Now', <http://www.internetweek.com/story/INW20010730S0002> (print out on file with author).
[552] See 'The End of Computer Virus Coverage as We Know It?', *supra* n.533.
[553] The information was obtained from an interview with one of insurance companies

However, does this mean every single loss or cost would be covered, even if a dispute is brought anywhere in the world against the assured? If a policy does not (unlike the former case) precisely assert its coverage, it definitely causes a great deal of problems in relation to cyber risks. The important issues are: firstly in which jurisdiction a loss/losses occur, and secondly, which jurisdiction would be applied for.

One of the problem-solving possibilities would be to purchase any policy with Difference-in-Conditions coverage (hereinafter "DIC") and Difference-in-Limits coverage (hereinafter "DIL") bases. Those DIC and DIL work to support a master policy and they are usually prepared for large companies to run their global businesses. DIC provides an excess coverage over the master policy in regard to its extent. DIL, on the other hand, works similarly to DIC, but in relation to the limits[554]. The example prepared by Zurich explains this with the case of a global business enterprise, running businesses in some Asian countries, and purchasing insurance policies there for local coverage (Figure 5.1). Filling the gaps left by DIC and DIL in the master policy, all the risks within Asia for this company are covered.

In fact, both DIC and DIL are basically applied for covering property damage. It is not impossible to apply them to liability. DIC and DIL are mostly prepared for covering big losses, such as more than £20 million. Cyber risks, cyber liability in particular, are very likely to cause immense damages or losses. So, technically there is no problem to apply DIC and DIL for cyber insurance. Contrary to this fact, the UK insurance market judges it as unlikely to happen[555]. This is based on whether or not cyber risk is distributable. In other words, it is because of the issue of reinsurance. In general, insurance companies arrange a treaty among themselves. When one insurance company undertakes a huge risk, other companies in the treaty accept some portion of the risk. Assume company X purchases an insurance policy from insurance company Y. Y insures X's risk worth £15 million by receiving the premium. Y undertakes £5 million out of £15 million only. Then, the rest of the £10 million is undertaken by company B and Z under the treaty[556]. So, X is unknowingly covered by B, Y and Z. This system prevents an insurance company taking a huge risk alone. If no one is willing to undertake cyber risk, it is impossible for any single insurance company to assume, on its own, a potentially huge risk[557]. It remains to be seen to what degree insurers are

---

the author interviewed.

[554] See 'International Insurance', <http://www.roughnotes.com/ao-onlinedemo/pfm/300/329_0402.htm> (print out on file with author).

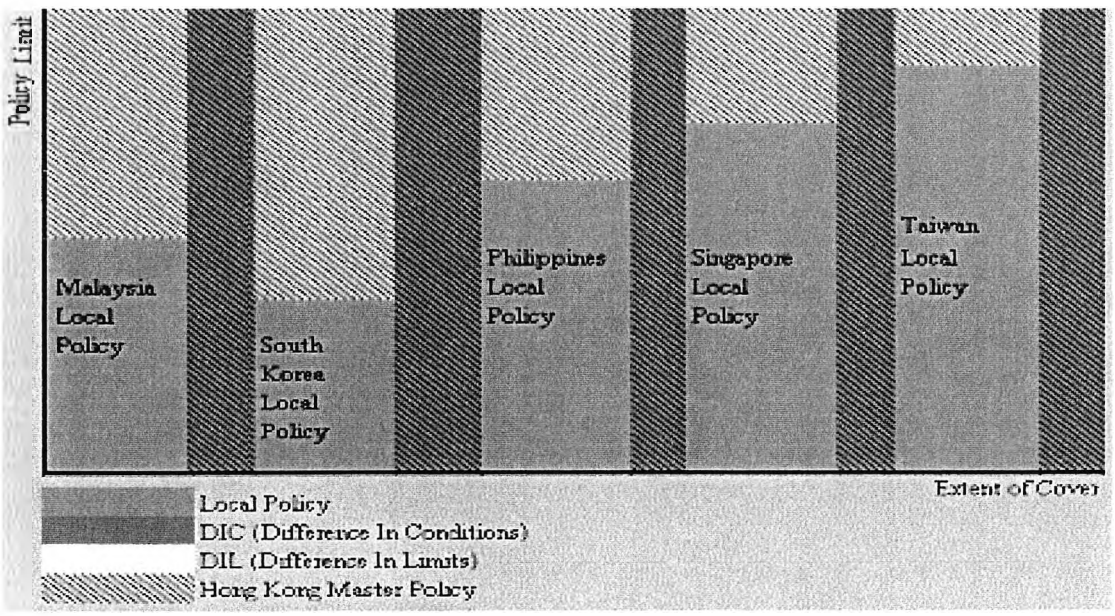
[555] The information was obtained from interviews with some of insurance companies the author interviewed.

[556] The information was obtained from an interview with AIG Europe (UK) Limited.

[557] To apply DIC and DIL in Japan is more problematic. Firstly, it is necessary to be approved by the Japanese Financial Services Agency (JFSA). Secondly, the Japanese insurance market is too small to distribute a huge risk. Thus, they have to reply on foreign insurance markets, such as the British or the Swiss market. If

prepared to take cyber risks.

Figure 5.1: How DIC and DIL corporate with the master policy for a global business



(Reference: See 'International Insurance Programme', <http://www.zurich.com.hk/zicd/ip.htm> (print out on file with author)

When a company X brings a lawsuit against another party Y, Y can be a company having a foreign registry with a local branch or an affiliated company Z. Examining the cases of domain name disputes, a plaintiff tends to sue a defendant in the defendant's jurisdiction. If X suffers extensive damage as a result of Y's services, X is likely to sue Z within the local jurisdiction[558]. Even if Y is a large company, Y is unlikely to be the direct defendant in X's case. Another potential defendant in this case is Z's superior (mostly directors and officers) in Y to whom Z directly has to report its financial matters and the like. In such cases, D&O policies will do. If Y offers online financial services in its own jurisdiction and X, in its own jurisdiction, receives the services via the Internet, there is obviously no local branch or affiliated company in X's jurisdiction. This will be discussed in the next section in depth.

4. The cyber insurance and the perceptions

Lovaas addressed that "Big Three of technology-based risk — namely intellectual property, privacy and network security."[559] His comment can

---

they do not take a risk, there is no way for them to take a risk. *Ibid.*

[558] Depending on whether Z is a local branch or an affiliated company in the local jurisdiction, a degree of the head office's participation is different by an applicable company law. *Ibid.*

[559] See 'The St. Paul Companies Educates Washington, D.C.-Area Agents and

be paraphrased in one word: liability. The said three issues mostly attract both existing and potential clients to the extent that they cause liability losses. Indeed, this is the issue that is unable to be predicted in advance.

Chapters IV and V clearly showed the different attitudes towards liability between the Japanese and the British insurance markets. The former market has realised that liability is an upcoming business opportunity although in reality, its growth seems slower than expected. It is said that taking legal action is not popular in Japan as a consequence of a small number of lawyers compared to the number of lawyers in western countries. This is, however, unlikely to be true since they are two entirely different issues. It is rather because the concept of bringing a suit has not been firmly implanted in Japanese culture. However, the more businesses become global, the more frequently Japanese companies face the possibility of being sued. Sooner or later, insurance products for liability will be indispensable in businesses in particular. On the other hand, the UK market seems to have understood the general importance of a liability policy in general. But it is unlikely to be reached purchasing cyber liability.

This issue also relates to the territoriality of the coverage of policies. The Japanese market adamantly limits its territoriality of any policy related to computers or networks within Japan. That is to say, a policy is triggered if a loss or damage occurs within the territory of Japan. Even if a foreign individual or company files a suit against an assured located in Japan, the expense or potential compensation is not covered. Whether a loss is for liability or property damage, risks which an insurer takes will be somehow minimised if the territorial limit exists. Unfortunately, this is insufficient to cover cyber losses, which are very likely to come from any jurisdiction. Contrary to this, the UK market allows for coverage of loss that occurred outside the jurisdiction. The British policies deal with cases by the British law. This is a natural consequence, to apply for local law where an insurance contract is signed. It would need a tremendous exertions and labours to deal with losses by local law where they occur. Another possibility is to have a special law in cyberspace to resolve issues. It is conceptually possible to have since there is no boundary in cyberspace; only one jurisdiction named "cyberspace" exists and one jurisdiction basically has only one law. However, this is not realistic at present. Who administers and enforces solitary cyber law when there are physically more than two hundred countries and jurisdictions in the real world? Therefore, the possibilities to deal with losses incurred in cyberspace are:

Brokers about E-Commerce and Technology Risks', <http://www.risk-engineering.com/rep/s/knowledge_navigator/search/kno_quickview_popup.jhtml?docId=256440&Links=CYB.RISK&image=yahoo#> (print out on file with author).

(1) An assured's jurisdiction;
(2) A claimant's jurisdiction;
(3) The jurisdiction where the losses exactly occurred if it is different from (1) or (2); or
(4) The jurisdiction where a computer server is physically located if it is different from (1) or (2).

Neither the third nor the fourth possibility tends to be convenient for an assured, a claimant and an insurer. So, the first possibility is the most suitable from both an assured and an insurer's viewpoints.

Here is the product analysis table of the Japanese products in regard to cyber risks. (Table 5.9) Compared to the UK or other markets, Computer Comprehensive Insurance (CCI) commands a large majority. As was explained in Chapter IV, CCIs do not cover cyber liability or property damage as a result of hacking or computer viruses. There are very limited numbers of products available to cover cyber liability. In regard to the coverage of computer equipment damaged by hacking or computer viruses, the choices are very limited. However, the concept behind this seems to be shared between the two markets. As explained here in Chapter V, the UK market considers that computer equipment is unlikely to be damaged by computer viruses or hacking as a result of unauthorized access, and they believe such damage, should it occur, would not be high.

Table 5.9: The Details of Computer/Network Related Insurance Products in Japan

(see next page)

	Non-life insurance companies	Name of products	E&O					Hacking					Computer Virus					Computer error					Natural Perils				Employee's offence	Copyright	Privacy	War, Earthquake
			BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW				
1	Ace	Data Processing Insurance	×	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	○	×			×
2	Chiyoda Fire & Marine	System Security Comprehensive	×	×	SP		×	×	SP	SP	×	SP	×	SP	SP	×	SP	×	×	×	×	×	×	SP	SP	○	×	×	SP	×
3	Daido Fire and Marine	Computer Comprehensive	×	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	○	×			×
4	Dowa Fire & Marine	Computer Comprehensive	×	○	×	○	×			SP		×			SP		×	×	×	×	×	×	○	○	×	○	×			×
5	Dowa Fire & Marine	Network Interruption	○	○	×	×	×			×	×	×			×	×	×			×	×	×	○	○	×	×		×	×	×
6	Dowa Fire & Marine	Data Servicing Distributors and Electronic Telecommunicators Professional Liability	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	SP	×	×	×	×	×	×	×	×
7	Fuji Fire & Marine	Computer Comprehensive	×	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	○	×			×
8	Koa Fire & Marine	Computer Comprehensive	×	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	○	×			×
9	Koa Fire & Marine	Pa-So-Co-N		×	○		×		×	○		×		×	○		×		×			×	×	○	○	○	×			×
10	Kyoei Mutual Fire & Marine	System Power Support		×	○	○		○	×	○	○	○		×	○	○	○		×				○	×	○	○	×	○	○	×
11	Kyoei Mutual Fire & Marine	Computer Comprehensive	×		×		×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×	○	×			×
12	Mitsui Marine & Fire	Network Security	×	×	×		×	○	○	○	×		○	○	○	×		×	×	×	×	×	○	○	×	○	×	×		×

	Non-life insurance companies	Name of products	E&O					Hacking					Computer Virus					Computer error					Natural Perils				Employee's offence	Copyright	Privacy	War, Earthquake
			BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW				
13	Nichido Fire & Marine	Computer Comprehensive	○	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	○	×	○	×			×
14	Nichido Fire & Marine	Information System Comprehensive	×			○	○		○	SP	○	○		○	SP	○	○	×		×	×	○		○	○	○	×	○	○	×
15	Nissan Fire & Marine	Computer Comprehensive	○	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	○	×	○	×			×
16	Nisshin Fire & Marine	Computer Comprehensive	×	○	×	○	×			SP		×					×	×	×	×	×	×	○	○	×	○	×			×
17	Secom Tokyo General	Computer Comprehensive	○	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	○	×	○	×			×
18	Sumitomo Marine & Fire	Professional Liability Insurance for IT services	×	□	□	□	×	□	○	○	○	○	○	○	○		□	×	○	×	×	×		○	○	□	×			×
19	Taiyo Fire & Marine	Computer Comprehensive	×	○	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	○	×			×
20	The Asahi Fire & Marine	Computer Comprehensive	○	○	×	○	×			SP		×					×	×	×	×	×	×	○	○	×	○	×			×
21	The DaiTokyo Fire & Marine	Comprehensive Insurance for ISPs	×	×	×		○	○	○	○	×	○			○	×	×					SP	○	○	SP	○	○	○	○	×
22	The DaiTokyo Fire & Marine	Extra-net Comprehensive	×	×	×		○	○	○	○	×	○			○	×	×					SP	○	○	SP	○	○	○	○	×
23	The DaiTokyo Fire & Marine	Net Banking										○																×	×	×
24	The DaiTokyo Fire & Marine	Password Theft										○																×	×	×

	Non-life insurance companies	Name of products	E&O					Hacking					Computer Virus					Computer error					E Natural Perils				Employee's offence	Copyright	Privacy	War, Earthquake
			BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW				
25	The Nippon Fire & Marine	Network System Comprehensive	○	○			○	○	○			○	○	○			○	○	○			○	○	○		○	×	×	○	×
26	The Nippon Fire & Marine	Computer Comprehensive	×	○	×	○	SP	SP	SP	SP	×	×	SP	SP	SP	×	×	×	×	×	×	×	○	○	×	○	×	×	×	×
27	The Taisei Fire & Marine	Computer Comprehensive	×	○	×	○	×			SP		×					×	×	×	×	×	×	○	○	SP	○	×			×
28	The Taisei Fire & Marine	Network Interruption	○	○	×	×	×			×	×	×			×	×	×	○	○	×	×	×	○	○	×	×		×	×	×
29	The Taisei Fire & Marine	Data Servicing Distributors and Electronic Telecommunicators Professional Liability	×	×	×	×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	SP	×	×	SP	○	×	×	×	×
30	Tokyo Marine & Fire	Computer Comprehensive	×	○	×	○	×	×				×	×				×	×	×	×	×	×	×	○	×	○	×			×
31	Tokyo Marine & Fire	E-click						○	○	○		○	○	○	○		○		○	○		○	○	○	○	○	×	×	○	×
32	Tokyo Marine & Fire	E-risk Solution						○		○		○	○		○		○	○		○							×	○	○	×
33	Tokyo Marine & Fire	Network Comprehensive										○		○	○		○	○	○			○		○	○	○	×		○	×
34	Tokyo Marine & Fire	Network Interruption																												
35	Tokyo Marine & Fire	Data Processors' Liability																												
36	Yasuda Fire & Marine	Pasocom Ointment	×	×	○	○	×	×	×	○		×	×	×	○		×	×	×			×	×	×		○	×			×

	Non-life insurance companies	Name of products	E&O					Hacking					Computer Virus					Computer error					E Natural Perils				Employee's offence	Copyright	Privacy	War, Earthquake
			BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW	L	BI	EE	Data	HW				
37	Yasuda Fire & Marine	Online Interruption	o	o	×	×	×			×	×	×			×	×	×			×	×	×	o	o	×	×		×	×	×
38	Yasuda Fire & Marine	Information System Comprehensive	o	o	o	o	×					×					×	×	×			×	o	o	o	o	×			×
39	Yasuda Fire & Marine	Cyber Guard	×	×	×	×	o	×	×	×	×	o	×	×	×	×	o	×	×	×	×	o	×	×	×	×	×	o	o	×

* Business Interruption->BI, Extra expense-> EE, Computer data and the like-> Data, Hardware-> HW, Liability-> L
* SP->Special contract if necessary
* The words in policies are 'Unauthorised Access' although they are very likely to mean 'Hacking'.

(Reference: All information are based on brochures and specially prepared documents which are given by each insurance companies to the author as of 2001. Therefore, the author is to blame any unintentional incorrect mistyping or characterization.)

Focusing on computer data and the like, they are commonly uncovered in Japan unless an assured purchases a special policy to cover them. There seems to be a very thin line between computer equipment (a.k.a., tangible property) and computer data and the like (a.k.a., intangible property) in general. Thus, if computer data is kept in a media, the losses are covered, but only the cost of media. CCIs themselves do not cover intangible property or liability. So, it is hardly possible to expect having extra expenses covered for recovering damaged data under such products. The special policy for covering computer data and the like is, however, prepared for losses or damage of computer data and the like; it does not cover liability. It remains to be seen depending on how each insurer reacts, whether any Professional Indemnity Policy (PIP, such as Data Processors' Liability) covers any loss resulting from computer viruses. However, such PIPs are prepared mainly for Data Servicing Distributors, Electronic Telecommunicators, Internet Services Providers, or IT services providers. The possibilities for financial institutions are very limited, such as Net Banking (by The DaiTokyo Fire & Marine). Despite the fact that the Japanese market goes where the European and US markets proceed, the status quo of cyber liability in Japan is quite different from that in the said markets. This is likely to be based on a few demands of the whole cyber insurance products. As mentioned, the UK market has not experienced success with such products to date. Considered from this viewpoint, it is perhaps possible to say that the Japanese market has carefully observed other markets.

Chapter IV proved that the Japanese insurers are likely to collaborate with IT companies. The UK and US markets are also in partnership with other industries, such as IT security specialists. AIG, for example, has entered into partnership with Unisys Corporation; more precisely, AIG eBusiness Risk Solitions, a division of a parent company (American International Companies). Unisys conducts security assessments for the said company as well as assisting its development of insurance products covering risks in relation to security breaches and so on[560]. ACE USA, J.S. Wurzler, Lloyd's of London and Marsh & McLennan have said that they also have engaged in such technical partnerships: J.S. Wurzler with Hewlett-Packard Co[561]. In fact, it is practical to enter into a technical tie-up with professionals in regard to cyber insurance risks in particular, unless an insurer has its own subsidiary or institution to pursue research on such risks. An insurance broker the author interviewed commented, "the perceptions of risks would differ from the ones who know computers to the ones who do not. Computer experts probably can tell

[560] See 'Unisys, AIG eBusiness Risk Solutions Partner To Minimize Business Risk From Cyber Attacks', <http://www.unisys.com/news/releases/2001/apr/04037082.asp> (print out on file with author).

[561] See 'E-commerce Insurance: New Riders of the Digital Age', <http://www.cfo.com/article/1,5309,4662|7|A|55|8,00.html> and 'Got Cyber Insurance?', <http://computerworld.com/cwi/Printer_Friendly_Version/0,1212,NAV47-665_STO48721-,00.html> (print out on file with author).

how far a risk could be expanded at which part of a computer or the network is interrupted.[562]" This should be true. Cyber risks are generally brand-new to the majority of people. Moreover, computer technologies are changing as well as computer equipment. Technical professionals will help insurance companies to refine their understanding and up-to-date awareness on cyber risks.

Another way of technical professionals being involved in this business is to assess computer security levels of a potential client company. Insurance companies would simply not sell their cyber liability policies unless a potential client's security is proved to be up to their standards. The lower a client's security level, the more risks of an insurer increase. Moreover, being checked professionally is advantageous for the potential client to reduce not only its security holes but also its premium[563]. Such security checks are prepared by both the Japanese and UK markets.

Cyber insurance as a whole is not yet perfect: there are shortcomings or unresolved issues as mentioned in Chapters IV and V. Are they really serious enough problems to make companies reluctant to purchase cyber insurance? Many professionals the author interviewed agree that cyber insurance are good policies. On the contrary, an insurance company frankly commented that cyber insurance is better for distributors than customers[564]. This is because those policies are designed not to take an excess risk. Thus, insurance companies are extremely likely to be hesitant rather than eager to sell cyber insurance. They will surely avoid selling them to any industry or company that holds potentially high risk. Financial institutions hold relatively higher risks, such as trading risk. Therefore, it would be natural that the financial industry is not the sales target of cyber insurance. It would appear that one of the critical problems behind cyber insurance's lack of success seems to be the perceptions of both clients and insurance companies in relation to cyber risks. In terms of the perceptions of insurance companies, they seem to have advanced awareness and knowledge on cyber risks. They know, at least, exactly what they cover by insurance products and what they do not want to take. Even if there are risks they prefer not to take, there may exist some alternatives or methods which make such risks possible. For instance, lawsuits take time and costs. If Alternative Dispute Resolution in civil litigation works as the mitigation of the costs of expenses, it will be another possibility for insurance

---

[562] Here the name remains anonymous by request. The author would like to thank him for his frankness and generous advice.

[563] The information was obtained from an interview with AIG Europe (UK) Limited.

[564] Cyber insurance is, in a sense, more similar to life insurance than car insurance. For example, if a customer files a claim with an insurance company after a car crash, the company can have a crashed car as collateral. If there is any part of the car adequate to sell, it can at least collect some money from the parts. However, it is unlikely to happen in case of cyber insurance. An insurance company is not in the position of claiming for client's data or information which is abused by a hacker. The information was obtained from an interview with AIG Europe (UK) Limited.

companies to reduce payments for clients[565]. Indeed, the perceptions of cyber risks for insurance companies have huge gaps in their customers' perceptions. It will be necessary to make efforts to fill those gaps to be more persuasive to their customers.

Regarding clients or potential clients of cyber insurance, the perceptions seem to have not been sufficiently developed. In other words, they are aware of such risks but are not prepared to accept them as real dangers to their businesses. AIG Europe commented that the Japanese companies seem to believe that the probability of an incident happening to cause cyber losses is far less than the probability of no incident happening[566]. That is to say that they would consider insurance only after a terrible incident happens and causes tremendous damage or losses to their businesses. This would be the reality and it seems to be a negative attitude towards cyber risks. To a greater or lesser extent, these attitudes are shared with other markets. The majority of insurance companies and brokers the author interviewed judge that this will definitely change in the event of a large scale incident happening with resultant massive cyber losses. Strangely enough, this viewpoint is exactly the same as the Japanese insurance companies commented.

It is most important for all companies to react to cyber risks. Without finding out what risks they are likely to face, they cannot go to the next stage, i.e., purchasing cyber insurance, pooling money or strengthening computer security. The questions they should strive to answer are[567]:

(1) What cyber risks are in general;
(2) For which cyber risks a company is most likely to be vulnerable;
(3) Possibly try to estimate how much losses could be;
(4) What types of risk transfer methods are available;
(5) Which risk transfer methods are the best for a company to take, and
(6) Considering all points above, make a complete plan preparing for potential cyber risks to avoid the loss or minimise the impact.

This does not suggest that this is an appropriate method to combat computer crime, but it is a way forward to encourage more companies to disclose more cybercrime cases publicly. Purchasing cyber insurance will, without any doubt, show up as one of the best risk-mitigating methods.

---

[565] Alternative Dispute Resolution (a.k.a. ADR) is defined as "any method of dispute resolution (other than litigation) where a neutral third party or parties [is/are] involved." See 'JCA Newsletter Number 10', <http://www.jcaa.or.jp/e/arbitration-e/syuppan-e/newslet/news10.html> (print out on file with author).

[566] The author is grateful to Mr T. Matsumura, Regional Manager of Japanese Business Division, AIG Europe (UK) Limited for his invaluable comments and advice.

[567] As for reference, see 'Bringing Order to Chaos Insurance Issues for E-Commerce Activities', *supra* n.514.

Chapter VII:
An Analysis of the Various Risk Management Methods

1. Introduction

It is no longer necessary to explain how seriously cyber risks affect financial institutions. Having observed how to deal with cyber risks, it has been shown that there are two main pillars: by legislation or by purchasing insurance policies. However, as has been mentioned, they are not perfect solutions. In some cases, a loss would be tangible as a consequence of risks slipping through a chink between the two pillars, which merely work as a sieve of large mesh. In this chapter, some relevant applications are examined for filling up the holes.

2. The conceptual assistance: operational risk and cyberspace

The Basel Committee on Banking Supervision (hereinafter "the Committee") of Banks for International Settlement (hereinafter "the BIS")[568] published the consultative paper called "The New Basel Capital Accord" (hereinafter "the New Accord") in January 2001. This is the reaffirmation of the 1988 version of the Capital Accord. It aimed at preserving the integrity of capital in banks: its viewpoint was to give an index of the total capital amount in banks reducing the risks of insolvency and bankruptcies. By the year 1999, it was found necessary to change to a more flexible and risk-sensitive system owing to the massive changes in many aspects of banking: market systems, regulatory supervisions and so on. Although the New Accord mainly targets the internationally active banks, it is also intended to apply to various types of banks. Though not yet finalised, it is expected to be implemented in 2005[569].

The New Accord has been expressed by three main pillars: (1) minimum capital requirement; (2) supervisory review process; and (3) market discipline[570]. An epoch-making point was introducing operational risk. Operational risk was acknowledged as being other than credit risk and market risk. It suggests operational risk as the third category to determining capital levels. The first pillar of the New Accord suggests measuring capital adequacy as[571]:

---

[568] BIS is the international organisation located in Basel, Switzerland. It was originally established in 1930 in the context of Young Plan, particularly for executing the mission of the reparation imposed on Germany by the Treaty of Versailles. At present its main aims are: (1) providing an opportunity to have a forum for central banks worldwide; (2) contributing to research on monetary and financial stability and the like; (3) performing traditional banking functions, such as reserve management and gold transactions (for central bank customers and international organisations); and (4) providing emergency financing to support the international financial system if necessary. See 'BIS History', <http://www.bis.org/about/history.htm> and 'Profile of the BIS — Bank for central banks', <http://www.bis.org/about/profcbank.htm> (print out on file with author).

[569] See 'Basel Committee reaches agreement on New Capital Accord issues', <http://www.bis.org/press/p020710.htm> (print out on file with author).

[570] See 'The New Basel Capital Accord: an explanatory note', <http://www.bis.org/publ/bcbsca01.pdf> (print out on file with author).

[571] *Ibid.*

$$\text{The bank's capital ratio (Minimum 8\%)} = \frac{\text{Total capital (unchanged)}}{\text{Sum (Credit + Market + Operational risk)}}$$

Then what exactly is operational risk? It was firstly defined as "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events" in the Consultative Document published in January 2001. This definition was based on the survey conducted by BBA, ISDA, and RMA[572]. Later same year, the Working Paper on the Regulatory Treatment of Operational Risk refined it as 'the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events[573]." It includes legal risk but excludes reputational, strategic and systemic risk: this is to minimise the capital charge of regulatory operational risk [574]. The said working paper published in 2001 also introduced the details of classifications of operational risk in the Table 6.1 below.

[572] The survey report 'Operational Risk — The Next Frontier' was published in June 1999 by the cooperation of British Bankers' Association, International Swaps and Derivatives Association and Robert Morris Associates. The information was obtained from the interview with the Centre for Financial Industry Information Systems (Japan). The author is grateful to their invaluable comments and advice.

[573] See 'Working Paper on the Regulatory Treatment of Operational Risk', <http://www.bis.org/publ/bcbs_wp8.pdf> (print out on file with author).

[574] Systemic risk is different from system risk. Systemic risk is defined as "risk resulting from the possibility that an entire financial market or system could fail catastrophically", 'investorwords.com', <http://www.investorwords.com/cgi-bin/getword.cgi?5817> whereas system risk is defined as "risk resulting from a halt, wrong operations, inadequacies or an abuse of computer systems", '*Sonota no risk kanri* (Other risk control)', <https://www.jbic.go.jp/japanese/investor/siryou/risk/others.php> (print out on file with author).

Table 6.1: Detailed loss event classification of Operational Risk and cyber-elements

Event	Category	Examples	Cyber risk?
Internal fraud	Unauthorized activity transactions not reported (intentional)	Transaction not reported (intentional)	Possible
		Trans type unauthorized (w/monetary loss)	Possible
		Mismarking of position (intentional)	Possible
	Theft and fraud	Fraud / credit fraud / worthless deposits	Possible
		Theft / extortion / embezzlement / robbery	Possible
		Misappropriation of assets	Possible
		Malicious destruction of assets	Possible
		Forgery	Possible
		Check kiting	Possible
		Smuggling	Possible
		Account take-over / impersonation / etc.	Possible
		Tax non-compliance / evasion (wilful)	Possible
		Bribes / kickbacks	Possible
		Insider trading (not on firm's account)	Possible
External fraud	Theft and fraud	Theft/Robbery	Possible
		Forgery	Possible
		Check kiting	Possible
	Systems security	Hacking damage	Yes
		Theft of information (w/monetary loss)	Yes
Employment practices and workplace safety	Employee relations	Compensation, benefit, termination issues	No
		Organised labour activity	No
	Safe environment	General liability (slip and fall, etc.)	No
		Employee health & safety rules events	No
		Workers compensation	No
	Diversity & discrimination	All discrimination types	No
Clients, products & business practices	Suitability, disclosure & fiduciary	Fiduciary breaches / guideline violations	No
		Suitability / disclosure issues (Know Your Customer, etc.)	No
		Retail consumer disclosure violations	No
		Breach of privacy	Possible
		Aggressive sales	Possible
		Account churning	Possible
		Misuse of confidential information	Possible
		Lender Liability	Possible
	Improper business or market practices	Antitrust	No
		Improper trade / market practices	No
		Market manipulation	Possible
		Insider trading (on firm's account)	Possible
		Unlicensed activity	Possible
		Money laundering	Possible

(Table 6.1 continued)

Event	Category	Examples	Cyber risk?
Clients, products & business practices	Product flaws	Product defects (unauthorized, etc.)	Possible
		Model errors	Possible
	Selection, sponsorship & exposure	Failure to investigate client per guidelines	No
		Exceeding client exposure limits	No
	Advisory activities	Disputes over performance of advisory activities	No
Damage to physical assets	Disasters and other events	Natural disaster losses	No
		Human losses from external sources (terrorism, vandalism)	No
Business disruption and system failures	Systems	Hardware	Yes
		Software	Yes
		Telecommunications	No
		Utility outage / disruptions	Yes
Execution, delivery & process management	Transaction capture, execution & maintenance	Miscommunication	No
		Data entry, maintenance or loading error	Yes
		Missed deadline or responsibility	No
		Model / system misoperation	Yes
		Accounting error / entity attribution error	No
		Other task misperformance	No
		Delivery failure	No
		Collateral management failure	No
		Reference Data Maintenance	Yes
	Monitoring and reporting	Failed mandatory reporting obligation	No
		Inaccurate external report (loss incurred)	No
	Customer intake and documentation	Client permissions / disclaimers missing	No
		Legal documents missing / incomplete	No
	Customer / client account management	Unapproved access given to accounts	No
		Incorrect client records (loss incurred)	No
		Negligent loss or damage of client assets	No
	Trade counterparties	Non-client counterparty misperformance	No
		Misc. non-client counterparty disputes	No
	Vendors & suppliers	Outsourcing	Possible
		Vendor disputes	Possible

Notes: 'Yes' in a cyber risk column means that the quoted incident has already been committed thus far or has been pointed out the possibility to happen. 'Possible' means that the possibility of this type of incident being committed cannot be denied. 'No' means that this type of incident is hardly possible to be committed at present.

(Reference: The author revised the original published in 'Working Paper on the Regulatory Treatment of Operational Risk', *supra* n.558 *et seq.*)

As is shown, the majority of the events relate to cyberspace to a greater or lesser extent. In addition to this, most potential cybercrime, or incidents that have been discussed in this thesis thus far, have been included in the list above. There is only one big issue excluded from

operational risk concerned with the issues discussed thus far: reputational risk. However, the causes of triggering reputational risk are more or less listed.

During the 1990s, a series of serious financial disasters occurred at banks: Bankers Trust in 1994, Barings Bank and Daiwa Bank (New York branch) in 1995 and National Westminster Bank in 1997. These incidents made the executives in financial institutions worldwide aware of the existence of operational risk and its hazards. Whether the BIS imposes a minimum 8% of bank capital or not, financial institutions should have pursued their own researches on operational risk to avoid them. A working group of the Committee conducted a survey of the management of operational risk in 1998 of approximately 30 major banks from the member countries. According to this survey, some banks had already arranged an internal department in charge of this issue by then[575].

However, those 30 banks were very likely to be considered either internationally active banks or mega banks. It is not always possible for all level of banks to pursue the same goal, in that league, due to lack of resources. So what are banks' advantages as a result of knowing operational risk or being included in the New Accord? Some banks (within the 30 banks in the said survey) commented that a potential benefit was the possibility of developing incentives for business managers to lead sound risk management practices through capital allocation charges, performance reviews or other mechanisms[576]. This is, however, a merely latent benefit. The direct benefit is to acknowledge the existence of risks categorised in operational risk and to seek the ways of:

(1) preventing operational risk from being tangible;
(2) avoiding suffering a loss in case of operational risk being tangible: and
(3) minimising a loss in case it is not avoidable.

It is hardly possible that the vast majority of operational risk (excluding natural perils and some unexpected incidents, such as fire or terrorist attacks) becomes tangible all of a sudden. There must have been some type of sign or indication[577]. For instance, a trader in Daiwa Bank New York branch had continued off-the-book dealings for nearly eleven years[578]. This incident would have been disclosed much earlier if the bank had had an adequate corporate compliance system. Operational risk could also become tangible on a chain of unfortunate events: it paraphrased that losses occurred because controls over each business

---

[575] See 'Operational Risk Management', <http://www.bis.org/publ/bcbsca07.pdf> (print out on file with author).
[576] *Ibid.*
[577] Arthur Andersen (ed.), 'Operational Risk' (2001) Kinzai, Tokyo, at 2-3.
[578] For the details, see Chapter III.

transaction were lost and did not constantly function[579]. Whether its explanation is persuasive or not, the BIS Committee also addressed that breakdowns in corporate governance and internal controls hold the essential position in operational risk. This is because such breakdowns were, in other words, chances that an institution could have discovered and thus avoided taking financial losses as a consequence of error, fraud, or failure[580]. If an employee committing a fraud is discovered by an institution itself through the adequate systems, not only does it frustrate unlawful behaviour and protect its financial assets and good reputation to some degree, but also deters further unlawful behaviour in the future. This is the subsidiary advantage of establishing a successful operational risk management system.

It is a misunderstanding of operational risk management if any institution is reluctant to deal with them and only does so because of the New Accord. All financial institutions are liable to prove to their customers that the operation of their banking business is sound.

However, the difficulty is that operational risk used to be identified as the rest of all risks after excluding credit and market risk. Thus, the idea of this "remainder" makes imaging its outline conceptually vague. Furthermore, it is wrong to define operational risk as the remainder of the other two categories of risks. This is because there are other risks that are not included in the said three risk categories. As reputational, strategic and systemic risk are typical examples, there are others, such as business risk, liquidity risk and political risk. Indeed, there exist various individual risk components and many different combinations of these. The New Accord is, therefore, just one of the combinations. Nevertheless, it is possible to say that the combination of the New Accord is very likely to be the most popular set on a worldwide level.

From the start, the biggest concern of all financial institutions and relevant authorities has been how to calculate operational risk. Even if the same type of incident has occurred in two financial institutions, the size of the losses is unlikely to be identical: the losses are determined by each piece of circumstantial evidence, such as the size of the businesses or skill of a hacker. In reality, the Committee encourages financial institutions to develop more than one methodology to reflect their individual risk profiles[581]. Not only the methodologies but also operational risk itself is obviously under development. The perception of operational risk is also different from institution to institution or country to country. For instance, the Japan Center for International Finance conducted an inquiry on the

[579] Arthur Andersen (2001), *supra* n.562.
[580] As the examples, the Committee introduced the cases of exceeding authority, conducting business in an unethical or risky manner of dealers and officers. See 'Operational Risk Management', *supra* n.560.
[581] See 'Consultative Document, Operational Risk, Supporting Document to the New Basel Capital Accord', <http://www.bis.org/publ/bcbsca07.pdf> (print out on file with author).

New Accord. In relation to a question on operational risk and capital, there was a statement that the ratio 20% was excessive considering high accuracy in pursuing businesses and the low rate of unlawful behaviour in Japan[582]. Those facts could be true comparing other countries. However, it is impossible to determine that these phenomena could never change in the future, especially considering the financial globalisation.

It was very crucial that operational risk was involved in the New Accord. However, operational risk itself is not important in this context. The important point is introducing the concept of operational risk broadly in financial institutions, where such risks are widespread. It is not a problem that only executives have to deal with: it is very likely to be a job for an entire company since people on the floor are the ones to know exactly where, when and what type of risk could be tangible. They are also in a very good position to avoid or at least to discover a risk being tangible before it becomes disastrous. Since the issue of tackling operational risk is not confined exclusively to executives, it is crucial to involve all levels of employees. To succeed in this, training and education is imperative. As was previously mentioned, it could be helpful to employ a publicly announced incentive system, such as a reward for discovering or avoiding operational risk. It is also necessary to have a penalty, to some degree, in case of false information or fabricated cases. If this works properly, the majority of operational risk being tangible would be avoided, except any type of abrupt risks.

In regard to the factual ways of handling operational risk, there are some risk management methodologies that usually function together. Purchasing insurance policies is one of them. Other examples are to be seen in the next section.

3. The technical assistance: computer technology and security policy

Computer technology is indispensable for developing cyberspace. Without the involvement of computer technology, cyberspace would still be a fantasy. Technical innovation makes the available cyberspace services remarkably progressed, but can also, sometimes, be an irritation. To date, brand-new computer equipment is easily obtainable from a store or online, and computer skill to some degree is the basic requirement for any job. That is to say that anyone who has knowledge and equipment is potentially in a position to commit a cybercrime. It is, of course, possible to separate sever computers from networks. A closed use of computers within an office is less risky than the computer use in an open environment to cyberspace. Nevertheless, an entire withdrawal of services from cyberspace may cost a company a fantastic business opportunity. To

[582] The question was whether a financial institution believes whether it is appropriate ratio that operational risk holds 20% of capital in average. The information was obtained from the interview with Japan Center for International Finance (Japan). The author is grateful to its invaluable comments and advice.

avoid computer systems abuse, new technology has been constantly advanced. The application of biometrics is no longer fantasy: scanning a retina pattern or venous pattern on the back of a hand is possible.

In Japan, a card called "SUICA" (Super Urban Intelligent Card) was introduced in the greater Tokyo area in November 2001. This is a new rechargeable Integrated Circuit (IC) card to travel over ground railways (JR East Japan) and other private railways (such as Tokyo monorail) just by touching an automated ticket gate. The SUICA card system was widely and rapidly accepted and it is said that 90% of customers were satisfied with this card within a month's time[583]. This technology is practically applicable to electronic money (e-money). The problem is that brand-new technologies tend to be expensive, thus it is not common for all levels of financial institutions to introduce them. Considering the balance of the cost of new technology and potential size of cyber risk, they are likely to judge that potential cyber risk is not yet up to the level of introducing the expensive brand-new technologies or equipment.

Since the events of 11th of September 2001, one of the anxieties for many states is being the target of cyberterrorists' attacks. The losses or damages in cyberspace are likely to have a serious effect on the real world. In the present UK, an arrested hacker is to be convicted by either the Computer Misuse Act 1990 or the Terrorism Act 2000. When abusing public computers and networks and putting human lives in danger, the hacker is referred as a cyberterrorist[584]. In the Terrorism Act 2000, there is no specific section or subsection in relation to this. However, the abuse of the computer system falls within Section 1(1) and (2)(e)[585].

At this stage, it is unnecessary to examine how information (or data) is a crucial asset for businesses. However, it is necessary to make sure of the form of information. The Centre for Financial Industry Information Systems of Japan (hereinafter "FISC") published a guide for financial institutions in 1990 and defined the asset of information as divided into two categories: information and information systems. Information was defined in details as data or information not only recorded or kept in computer

---

[583] See 'New JR SUICA CARDs for smooth traveling in Tokyo', <http://www.tcvb.or.jp/en/hot/sizzling/0112/sizzling_12c.html> and 'Suica' <http://www.jreast.co.jp/suica/03.html> (print out on file with author).

[584] See '*Hakkā wo terorisuto toshite atsukau eikoku no shinpō* (A brand-new British Law that refers a hacker as a terrorist)', <http://www.idg.co.jp/report/security/backnumber/us_topics/200102/sec20010220_01_us.html> (print out on file with author).

[585] The Terrorism Act 2000 tells:
1(1) In this Act "terrorism" means the use or threat of action where-
(a) the action falls within subsection (2)...
(2) Action falls within this subsection if it...
(e) is designed seriously to interfere with or seriously to disrupt an electronic system.
For reference, see 'The Terrorism Act 2000', <http://www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm> (print out on file with author).

systems or any medium but also printed on papers, memorandums and the like before input into computer systems, employees' conversations and memories. Information systems were computer hardware and software as well as all equipment and facilities involved (including humans to manage the information systems) for property administration and control[586]. These sound pretty much everything, especially the involvement of employees in information systems. Nonetheless, even if an employee believes what he knows is petty, it is likely to be valuable, commercially speaking, for the other trade. In particular, the structure of computer systems is mostly a strict secret for any industry.

When discussing the issues of secured computer networks, there are two basic but critical factors: they are "integrity" and "reliability" of computer networks. In other words, the availability, confidentiality and integrity of data trafficking through computer networks. BS ISO/IEC 17799 (BS 7799-1:2000) also suggests that the preservation of these should be maintained whatsoever the form of information is[587]. To secure these factors, it is necessary that the one who actually possesses a computer or controls computer networks is responsible for implementing a sufficient level of security. If it is an individual, it is all right to employ suitable software, such as firewall and ant virus software and to keep updating them as long as the computer usage is within individual purposes. If it is for commercial purposes, companies and institutions in particular, that the situation is not that simple. This is because companies or institutions offer services to a general run of buyers. It is liability for them to ensure offering secured services to the customers to some degree. E-commerce or any service offered online is nowadays getting to be one of the popular channels in general. Ensuring integrity and reliability of computer networks is, therefore, a hot stock not only for business industries, but also for relevant authorities and even for a state.

It is essential to place importance on the quality of the entire computer security within companies. There are, however, two key factors in the ideal computer security system: introducing sufficient level of technical devise and implementing computer security policy. The former includes supplying both computer hardware and techniques. The latter suggests human involvement.

Computers and their equipment, such as printers or scanners, are popular tools in business administrations in these days. The vast majority of

---

[586] The pamphlet titled 'Information Security Policy' published by the Sumitomo Marine Research Institute, Inc, which the author obtained from the interview with Dr M Fujimoto, Consultant, Research & Consulting Department 4. The author is grateful to her invaluable comments and advice.

[587] See '*Jôhô sekyuriti seisaku jikkô proguramu, Tûsansyô* (Information security policy programme by the Ministry of International Trade and Industry)', <http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu01j.pdf> and 'BS ISO/IEC 17799:2000 - Overview', <http://www.c-cure.org/7799Overview.htm> (print out on file with author).

people would not hesitate to use them at all. However, once it comes to the issue of technical matters, they are very likely to frown and change the subject. It is true that if one uses computers, it does not always mean one understands technical matters. On the other hand, one who knows a little about computers believes that computers can do anything one wants. Those two attitudes towards computers could be barriers. The former attitude is indicative of rejection. Before actually listening to the details on technical matters, one psychologically blocks his/her mind in case anything is not understandable. In fact, technical matters of computers belong to a type of special, rather than common knowledge. It is not a disgrace if one cannot understand a technical term. The latter case is exactly the opposite of this. In this case, before trying to understand anything, the user also blocks his/her mind, believing that a computer is a magical box which can make anything possible. In general, there is a person in a specific department or section (=Information Technology manager) in charge of computer security for the whole company. Is it accepted if the IT manager and his department are only ones who understand the company's computer security system? Technically speaking, the reality is likely to be so. Nevertheless, it is preferable if the executive officers, an officer to whom the IT manager reports directly in particular, could understand to some degree. In the former case, the psychological barrier of the executive officers allow the IT manager arbitrariness. In the latter case, the attitude makes the position of the IT manager rather awkward. That is to say that the executive officers may make an unreasonable demand of the IT manager and his team. Those barriers are strengthened when the executive officers are shown the cost of implementing computer security. It tends not to be a cheap investment in plant and equipment. The more financial resources are available, the better equipment and facilities are obtainable. If this is the sole truth, it means that there is no way for small and medium enterprises to implement a sufficient level of security systems.

Strictly speaking, any company, whether a large or a small or medium enterprise, can be a target of hacking or unauthorized access. Large enterprises are likely to be targets because of their fame, whereas small and medium enterprises are likely to be targets due to an insufficient level of computer security.

When assessing the level of any computer security, there are some guiding principles prepared by relevant authorities. In Japan, the Ministry of Economy, Trade and Industry (METI), for instance, have published several standards for measures on protecting not only information security but also e-signature and privacy[588]. Amongst all standards, the standards

[588] Ministry of International Trade and Industry (MITI) reformed and changed its name into Ministry of Economy, Trade and Industry in 2001. Other standards the then MITI had published are;

* The standards for computer system audit (MITI published in 1985);
* The standards for countermeasures on computer viruses (MITI annunciation No.

for secured information system (MITI annunciation No. 518 in 1995) are for information security. The main part of the body is divided into three phases. The first phase has 100 items each for six different locations (e.g., a host computer room, an operation room and so on) to check in relation to installing computers and their equipment in the least risky environment. The second phase has 26 items each for three different types of users to check hardware and software from technical points of view. The third phase has 66 items each for three different types of users to check for practical use of information systems[589]. However, this does not seem to have a simple structure. For instance, it suggests employing encryption to avoid electronic eavesdropping. But it does not suggest any concrete example, i.e., a recommendable encryption method or the necessary equipment. Moreover, some items suggest referring to other standards that the then MITI published. There are other standards or policies published by relevant authorities in Japan.

The FISC, for example, published a handbook for financial institutions that decide on a scheme on computer security policy in 1999. The critical issue is that those policies or standards involve merely the voluntary assistance of the authorities. There is no obligation or severe penalty for any company or institution even if they do not employ any of those standards or policies. Both such institutions and the whole industry recommend employing them. Whether or not imposing a penalty on a member institution not following their rules, it depends on each industry. All standards or policies published in Japan are domestic, and none are internationally designated. This tendency applies not only to Japan but also other countries in general. However, there is an exception in the UK. Stemming from the 1993 standards, BS7799 was established as a set of standard requirements for Information security management in 1995 by the British Standard Institute — Delivering Information Solutions to Customers (hereinafter "BSI-DISC"). BS7799 consists of two complications, evidently identified as "Part 1: Code of practice for information security management" and "Part 2: Specification for information management system[590]." In essence, Part 2 explains how to apply Part 1. Part 1 of

---

429 in 1995);
* The guideline for software administration (MITI published in 1995), and;
* The standards for countermeasures on unauthorized computer access (MITI annunciation No. 362 in 1996).

See '*Hōritsu, gaidorain nado* (Regulations and guidelines)', <http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm> (print out on file with author).

[589] See '*Jōhō sisutemu anzen taisaku kijun* (the standards for secured information system, MITI annunciation No. 518 in 1995)', <http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf> (print out on file with author).

[590] Part 1 of BS7799 (ISO/IEC 17799) is the set of security controls to be the countermeasures and safeguards against information security risks. Part 2 is designed mainly for internal assessment or audit systems for security systems from a top-down perspective on the basis of establishing a suitable Information Security Management System (an ISMS). It designs a six part programme to proceed: (1) defining a security policy; (2) defining the scope of the ISMS; (3) undertaking a risk

BS7799 has ten sections including security policy, compliance and so on[591].

It is said that it works to identify, manage and minimize the risks wherein information is being targeted. In 1999, BS7799 was revised and updated in order not only to be adaptable for other countries but also to be applicable for new developments, such as e-commerce, mobile computing and the like. In 2000, Part 1 of BS7799 was published as ISO/IEC 17799 (Information Technology — Code of practice for information security management) as the International standard by the International Organisation for Standardization (hereinafter "ISO")[592]. It deals with nearly 50 issues: for instance, accountability for assets, equipment security, outsourcing, operational procedures and responsibilities and the like. In regard to Part 2 of BS7799, it has commenced to harmonise with other management system standards, such as ISO 9001 and ISO 14001. One of the attractive features of implementing ISO/IEC 17799 (or BS7799 Part 2) is to involve a third party as an accreditation body to certify that security systems are following standards literally[593].

ISO/IEC 17799 works together with other standards. The typical standard is ISO/IEC 15408 (Information technology - Security techniques -Evaluation criteria for IT security) published in 1999. Through the process of developing ISO/IEC 15408, the establishment of "Common Criteria" (CC) came into existence originally amongst some European countries and the USA. ISO/IEC 15408 provides the criteria of evaluating

---

assessment; (4) managing the risk; (5) selecting control objectives and controls to be implemented; and (6) preparing a statement of applicability. See 'The ISO17799 Security Newsletter - Issue 2', <http://www.iso17799-web.com/issue2.htm> and '7799 History', <http://www.c-cure.org/7799history.htm> (print out on file with author).

[591] See 'What is BS 7799?', <http://emea.bsi-global.com/InformationSecurity/Overview/WhatisBS7799.xalter> (print out on file with author). BS7799 has 10 sections as follows:

(1) Security policy;
(2) Organising assets and resources for the management of information security;
(3) Identifying and controlling asset;
(4) Ensuring personnel security to reduce any human involved error or offence;
(5) Physical and environmental security to prevent any physical interference to both premises and information;
(6) Ensuring communications and operations management of information processing facilities secured;
(7) Ensuring access control to information;
(8) Ensuring systems development and maintenance;
(9) Establishing business continuity management plans to avoid suffering the effects of major failures or disasters to cause business interruption, and;
(10) Compliance.

[592] BSI has its origin in 1901 but was established by the Royal Charter in the 1920s as an independent body. The standards development work of BSI is funded by the government. The Department of Trade and Industry is, in particular, in a close relationship with the BSI. See 'Funding of BSI and Standards Development', <http://www.dti.gov.uk/strd/fundingo.htm> and 'The ISO17799 Security Newsletter', <http://www.iso17799-web.com/> (print out on file with author).

[593] In the UK, c:cure was set up in 1998 as the accredited Certification Authority Scheme for BS7799. See 'c:cure', <http://www.c-cure.org/welcome.htm> (print out on file with author).

information security equipment and systems including software[594]. Like ISO/IEC 17799, it also involves a third party as an evaluation facility to ensure that rules are followed in accordance with ISO/IEC 15408.

The second typical standard is ISO/TR13569 (Banking and related financial services — Information security guidelines). This is prepared particularly for the financial service industry. It initially published in 1996 and was amended in 1998 by ISO/TC68/SC2[595]. ISO/TR13569 is technically different from other standards: as the name implies, it is a technical report (TR) for financial institutions to implement a sufficient level of information security systems. Hence, an evaluation facility has not yet been involved[596].

There are other standards published by the ISO on information security management and banking operations[597]. In general, it is appropriate for financial institutions to implement information security

---

[594] ISO/IEC 15408 consists of three sections: Part 1: Introduction and general model, Part 2: Security functional requirements and Part 3: Security assurance requirements. See 'ISO, Catalogue searched for standards', <http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=15408> (print out on file with author).

[595] ISO has Technical Committees (TC) on each relevant issue. TC68 is one of them specialised in banking, securities and related financial services. TC68 has three Sub-Committee (SC) and fifteen Working Groups (WG) underneath SCs. The main WGs of TC68/SC2 are:
TC 68/SC 2/WG 4 Information security guidelines for banking;
TC 68/SC 2/WG 5 Protection profiles;
TC 68/SC 2/WG 6 Framework for IT security for financial institutions;
TC 68/SC 2/WG 8 Public key infrastructure management for financial services;
TC 68/SC 2/WG 10 Public key infrastructure management for financial services, and;
TC 68/SC 2/WG 11 Encryption algorithms used in banking applications.
See '*ISO/TC68 Kokunai-iinkai* (ISO/TC68 Domestic Committee)', <http://www.imes.boj.or.jp/iso/gaiyou.html#soshiki> and 'TC 68-SC 2', <http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=2193> (print out on file with author).

[596] See '*Heisei 13nendo OECD Jōhō sekyuriti gaidorain ni kansuru chousa* (2001 A survey on OECD information security guideline)', <http://www.ipa.go.jp/security/fy13/report/oecd-guideline/oecd-guideline.pdf> (print out on file with author).

[597] For instance, there are several standards under TC68/SC2;
ISO 1004:1995 Information processing - Magnetic ink character recognition - Print specifications;
ISO 6234:1981 Bank operations - Authorized signature lists and their representation on microfiche;
ISO 8730:1990 Banking - Requirements for message authentication (wholesale) ;
ISO 8731:1987 Banking - Approved algorithms for message authentication;
ISO 8732:1988 Banking - Key management (wholesale) ;
ISO 10126:1991 Banking - Procedures for message encipherment (wholesale) ;
ISO 11131:1992 Banking and related financial services - Sign-on authentication;
ISO 15782-2:2001 Banking - Certificate management - Part 2: Certificate extensions, and;
ISO/TR 17944:2002 Banking - Security and other financial services - Framework for security in financial systems.
See 'Standards of TC68/SC2', <http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage.TechnicalCommitteeStandardsList?printable=true&COMMID=2193> (print out on file with author).

systems that fulfil the international standards above-mentioned. That is to say that the majority of financial institutions fulfil the same minimum level of standards at least if employing international standards prevails in the industry. It is, of course, not the obligation for each institution to employ them unless any self-regulating body or relevant authority employs them as a rule for the member institutions — there is no punishment or discipline imposed. However, profit-making corporations are likely to behave like youngsters who always follow the latest fashion. In other words, financial institutions leap at a potential opportunity to make a profit. Employing the international standard is very likely to have an impact in terms of advertising their "secure' services" to the general public.

Indeed, difficulties exist. As for financial institutions, employing such standards is not a one-time event in corporate life. Once the standards are employed, financial institutions have to maintain that level of information security system to fulfil all conditions of the standards. If the standards are amended or updated, it is necessary to follow the changes. This may cost dearly and it would be difficult for companies without financial resources to maintain the standards. As for the publishers of the standards, such as the ISO, they also have to continue amending and updating the standards to keep up with the latest technical innovations.

There is another argument. BS7799, for instance, was developed in the British culture. It may be difficult to implant it directly into another culture even though BS7799-1 had eliminated British peculiarities. Mr Iwashita analysed that BS7799 was unlikely to be popular in Japan by the end of 2000. This was because, at first, it was costly. Secondly, there were cultural reasons: information security systems are a mere part of the whole business. As was previously examined, BS7799 targets not only the physical security system but also compliance or other issues involved. Therefore, it would be unbalanced to change the specific parts of the business that BS7799 requires into British or American standards without changing the rest of the parts of the business[598]. There is a survey report to prove this. According to the survey done by KPMG Japan in 2000, only 6% out of 410 entities had implemented BS7799 and more than 35% answered they had never heard of it[599]. It is true that human viewpoints differ from east to west [600]. Therefore, there is a tendency to revise international standards in accordance with domestic circumstances. The Japanese JIS X 5080, for instance, originated in ISO/IEC 17799. However, it is doubtful to what degree domestically revised international standards are acknowledged internationally.

---

[598] The author is grateful to Mr N Iwashita, Manager, Institute for Monetary and Economic Studies, Bank of Japan, for his invaluable comments and advice.

[599] See Information Risk Management Dept. (ed) 'Information Security Survey 2000 Report' (2000) KPMG Business Assurance Japan, Tokyo.

[600] It is said that the ethical doctrine that human nature is fundamentally good is generally believed in Japan whereas the ethical doctrine that human nature is fundamentally evil is believed in the UK. See also Chapter IV.

It has been approximately ten years since the OECD initially published the Guidelines for the Security of Information Systems. It was once revised in 1997 according to the article on revision of guidelines every five years. The year 2002 was the promised year for the second revision which was achieved (as promised). The acceleration in the aftermath of the September 11 tragedies was unavoidable[601]. It places importance on specific issues in particular[602]. It is rather the framework not the guideline or standard with full of details in every single issue. However, it will have an impact on countries ratified the said guidelines to a greater or lesser extent.

In addition to protecting computer security by employment of various guidelines or standards, the Japan Information Processing Development Corporation (JIPDEC)[603] has become a certifying organisation of privacy mark since 1998. Having privacy mark shows the general public that an institution so certified has taken appropriate measures to deal with personal information[604]. The retention of privacy mark and IT standards above-mentioned are translated into good publicity for the businesses.

It goes without saying that cyberspace is unbounded and not governed by a specific rule or jurisdiction. Therefore, it is critical for every individual or legal entity to be responsible for securing the nearest surroundings at least. A computer is not a magic box. Even if it is a machine, which does not make a mistake, it is a human who operates a computer. A computer software, programmes and even computers are all written, compiled or assembled by humans, not by God. Information security systems are also the same: if one structures the security system, it is potentially very likely to be hacked by someone who has the knowledge or skills. It is important to update the information of technical innovation and to analyse the latest cyber incidents as well as to be well aware of the individual responsibility of being cyberspace.

4. The physiological assistance: resuscitating morals and ethics

Even if there are many good-natured people, a sense of justice has a hard time surviving in the real world. It is unfortunately common to see

---

[601] See 'Guidelines for the security of information systems and networks towards a culture of security', <http://www.oecd.org/pdf/M00034000/M00034292.pdf> (print out on file with author).

[602] The specific nine issues are (1) awareness of the need for security of information systems and networks; (2) responsibility for using for the security of information systems and networks; (3) response to act in a timely fashion to detect, prevent or respond to security incidents; (4) ethics to respect the legitimate interests of others; (5) democracy on implementing the security; (6) risk assessment; (7) security design and implementation; (8) security management; and (9) reassessment of security. *Ibid.*

[603] JIPDEC is a public corporation that has a close relationship with the Ministry of Economy, Trade and Industry.

[604] See '*Puraibasi mâku to wa* (What is the privacy mark?)', <http://www.kcs.co.jp/p-mark/privacy_1.htm> (print out on file with author).

daily articles about commercial crime in the press. In August 2002, the ex-CEO of WorldCom (USA) was arrested after the collapse of WorldCom. Prior to this collapse, Enron (USA) also had a dramatic collapse. The auditor of Enron, Andersen, was sued by the US Department of Justice on obstruction of justice. All three of them have been sued for damages by the relevant parties as well as being under criminal investigation[605]. In early August, it was published that the relevant financial services authorities of the USA were considering the imposition of heavy fines on some financial institutions that neglected the legal obligation to save electronic mail for three years[606]. These are, to date, not at all rare cases. Moral and ethics probably have not become extinct. However, as is shown in Chapter I, committing economic crime seems to have irresistible power to dominate a person's normal moral and ethical sense.

There is a survey conducted in Japan. It is an opinion poll amongst new employees conducted twice per year (spring and fall) throughout four years. There is a specific question as to how one would behave when a superior orders him/her to commit an injustice, or at least something where one is likely to suffer qualms but that makes profits for the company. Table 6.2 shows the ratio of the new employees who answered they would obey the order whether or not they were willing to do so.

Table 6.2: The ratio of new employees who does whatever a superior orders

	Spring survey	Autumn survey
1999	39.1%	40.2%
2000	28.8%	32%
2001	33.3%	35.1%
2002	31.1%	data not yet available

(Reference: see '*Kigyô rinri* (Corporate ethics)', <http://home.att.ne.jp/sea/tkn/Issues/Issue-Ethics.htm> (print out on file with author).

Due to the educational system in Japan, new employees join the companies on 1st April in general. As is seen, taking notice of the change between spring and autumn surveys, most surprisingly, the ratio rises within half a year. The survey result tells how companies and corporations (whether private or public) place first priority on profit making. In addition to this, six months is enough for new employees to adapt to the company's policy. It was said that this was based on the Japanese lifetime employment system. Indeed, it is somehow still true now despite the changing employment system.

---

[605] *Nihonkeizai Shimbum* dated 17th July and 2nd August 2002. In addition to these, see 'Nikkei net', <http://www.nikkei.co.jp/sp2/nt48/20020615eimi204515.html> and '*Funsyoku kessan* (a window dressing settlement)', <http://www.hi-ho.ne.jp/yokoyama-a/funshoku.htm> (print out on file with author).

[606] *Nihonkeizai Shimbum* dated 3rd August 2002.

On the other hand, extreme corruption cases are often caused by the executive officers. The Guinness and Maxwell cases in the UK are good examples of this. Hence, there are ethics of two different internal controls to straighten: a company itself and its executive officers. The former is taken care of by implementing compliance exhaustively. The latter is by having rigid corporate governance. Compliance is understood as a form of behaviour to run businesses complying with laws, ordinances and moral precepts that a company ought to follow[607]. Corporate governance is the control of the decision making process and the audit systems for realising soundness and effectiveness of businesses. Bill Witherell, OECD Director for Financial, Fiscal and Enterprise Affairs, addressed it at the IOSCO 2002 conference as "good corporate governance ensures transparency, fairness, and accountability with respect to shareholders and other stakeholders[608]." The critical difference between compliance and corporate governance is that corporate governance was originally initiated on shareholders whereas compliance is more focused on corporate responsibilities as a member of society. However, corporate governance has currently moved its approach to this direction in the general form of stakeholders and has four main aims:

* Effectiveness and efficiency of operations;
* Reliability of financial reporting;
* Compliance with laws and regulations, and;
* Safeguarding of assets[609].

Employing both compliance and corporate governance are inseparable and inevitable for pursuing sound economy. In reality, some types of operational risk are avoidable by implementing compliance and corporate governance. Moreover, the vast majority of information security standards involve them as the important factors.

The history of internal control goes back to the 1987 Treadway's Report of National Commission on Fraudulent Financial Reporting in the USA after a series of window dressing settlements and bankruptcies. It was believed that substantial internal control was inevitable for preventing further dishonest financial reporting. After the Consideration of the Internal Control Structure in a Financial Statement Audit (AICPA SAS55) being published in 1988, the committee of sponsoring organizations of the Treadway Commission (COSO) published a landmark report on internal control called the "COSO report" in 1992. It is said that the COSO report

---

[607] See '*Risuku to konpuraiansu* (Risk and compliance)', <www.zenginkyo.or.jp/pub/pamph/pdf/dp1-7.pdf> (print out on file with author).
[608] See 'Corporate Governance and the Integrity of Financial Markets: Some Current Challenges', <http://www.oecd.org/pdf/M00029000/M00029848.pdf> (print out on file with author).
[609] See 'Corporate Governance', <http://www.cpaaudit.co.uk/pages/corpgovernance.html> (print out on file with author).

is the de facto standard of the theories and methods of effective internal control[610]. The COSO report has defined internal control as follows:

> "Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> * Effectiveness and efficiency of operations
> * Reliability of financial reporting
> * Compliance with applicable laws and regulations[611]."

They seem to involve all levels of employees, with the executive officers, to a greater or lesser extent. In other words, internal control is to give an impact on a corporate culture itself.

Looking at the UK, the Committee on the Financial Aspects of Corporate Governance was set up in accordance with the proposition of Financial Reporting Council and Institute of Chartered Accountants in England and Wales (hereinafter "ICAEW"). This Committee, chaired by Sir Adrian Cadbury, published the report in 1992 placing importance on controlling the board of directors, reporting functions and the role of auditors. The report included the Code of Best Practice — that complying with it became the condition of being listed on the London Stock Exchange (hereinafter "LSE") — in July 1993 in accordance with the Committee's request. After the Greenbury Report in 1995, the Committee on Corporate Governance was chaired by Sir Ronald Hampel, which published the Combined Code in 1998. This code was also adopted by the LSE in December 1998. The Combined Code remained uncertain to some degree. The ICAEW set up the Internal Control Working Party chaired by Nigel Turnbull and it established a report called the Turnbull Guidance in 1999[612]. This placed importance on implementing internal control and conducting risk management. Since December 1999, the compliance with the Turnbull Guidance has been obliged to the member companies of the LSE. Compliance with the Turnbull Guidance leads companies not only to be listed with the LSE but also to promise sound business practices[613].

---

[610] In February 1999, another report called Report of the Blue Ribbon Committee - Improving the Effectiveness of Corporate Audit Committees was also published by the Blue Ribbon Committee. See '*Gabanansu* (Governance)', <http://home.att.ne.jp/sea/tkn/Issues/Issue-Governance.htm> (print out on file with author).

[611] See 'Key Concepts', <http://www.coso.org/KeyConcepts/index.html> (print out on file with author).

[612] See K. Gotô, '*Kigyô-keiei no saidai-kadai to natta risuku manegimento* (Risk management, the crucial key factor of business management)' (2001) 4 Songai hoken kenkyû 62, at 38-41.

[613] Some western European countries also had published reports on corporate governance since 1997. The OECD also published the OECD Principles of Corporate Governance in 1999. See '*Kigyô risuku jôhô* vol.9 (Corporate risk information vol.9)', <www.irric.co.jp/library/management/risk_info09.pdf> (print out on file with author).

Japan is far behind them compared to the Britain and the USA. There is a report that shows evaluations of the corporate governance of each country published by Davis Global Advisors, Inc. According to the 1999 report, Japan got 3.5 points whereas the UK got 8.3 and the USA got 7.0 (Table 6.3). Japan has conducted further research and revised the relevant legislation to take the most effective approach.

Table 6.3: Corporate governance evaluation

Indicator	Japan	The U.K.	The U.S.A.
1.1 Best Practice Codes	2	7	9
1.2 Non-executive Directors	1	6	8
1.3 Board Independence	0	3	6
1.4 Split Chairman/CEO	10	9	1
1.5 Board Committees	3	10	10
21 Voting Rights	10	10	8
2.2 Voting Issues	4	9	1
3.1 Accounting Standards	1	9	10
3.2 Executive Pay	3	10	10
4.1 Takeover Barriers	1	10	7
Overall Score	**3.5**	**8.3**	**7.0**

(Reference: see '*Gabanansu* (Governance)', *supra* n.*595*)

Considering corporate governance in Japan, it is impossible to avoid mentioning *sôkaiya*. Nakajima concisely defined it as "general meeting fixers... extort money from companies by threatening to disrupt their annual general meetings [614] .' Until 1997, successive deplorable corporate scandals disturbed Japanese society. The typical example was payoff scandals involving *sôkaiya* who mostly have strong relationships with *yakuza* (also known as the Japanese mafia). The Japan Federation of Economic Organizations became apprehensive about falling credibility from payoff scandals and the like. Hence, it published the proposal to suggest member industries, companies and the government take constructive action preventing further corporate scandals, particularly the cases involving *sôkaiya*[615]. In practice, *sôkaiya* seem to be less involved in the traditional type of a general meeting however they are not yet entirely retired from the stage. To date, an online general meeting of shareholders has been considered. It will be possible for *sôkaiya* being involved in an online general meeting only if a company gives assistance. Considering the nature of cyberspace, it will be most probably difficult for the relevant authorities to detect their online attendance or to find the proof of their attendance. This issue has not yet been realised and will remain to be

[614] C. Nakajima, 'Conflicts of Interest and Duty' (1999) Kluwer Law International, London, at 54.
[615] See '*Toumen no sôkaiya-nado heno taiousaku ni-tsuite* (The urgent countermeasures against *sôkaiya* issues and the like)', <http://www.keidanren.or.jp/japanese/policy/pol142.html> (print out on file with author).

seen.

Implementing both compliance and corporate governance aims to control a corporate body internally by complying with the relevant laws and regulations, disclosing corporate information, or using audit systems. They are not aimed to detect a criminal offence, a dishonest act or an error being committed as their principal task. Their real purpose is to suggest means to conduct businesses more effectively by preventing or minimising potential risks. It is possible to materialise only if a whole company is involved. Therefore, to pursue successful compliance and corporate governance systems, it is necessary to take steps to enhance the totalitarian project of the company. One of the effective means is to give an opportunity for employees to purchase shares, as being a stakeholder of the company one works for is very likely to be a good incentive.

5. The other type of assistance 1: applying outsourcing

Outsourcing is considered to be one of the solutions to reduce risks. Information security in particular is said to be suitable for applying outsourcing. As is known, there is a variety of information technology. Gardner, for example, suggests the application of outsourcing to avoid choosing inappropriate technology or methods[616]. It is possible to judge business lines whether or not they are appropriate to deal with internally. Information technology, in particular, is apparently a specialised area. If a company designs security systems, there are some problems and issues to solve.

1. Never ending innovation of technology;
2. The deficiency of resources;
3. Difficulties to integrate the different types of systems all over the company;
4. Inflexibility of solutions;
5. Insufficiency of infrastructure;
6. Insufficient but highest level of technology, and;
7. A goal that is hardly possible to see[617].

Indeed, as it is not necessary for financial institutions to be familiar with the area, it has potential for outsourcing. Examining the application of outsourcing, there are some advantages:

1. Core competency;
   Outsourcing enables a company to concentrate on its main business without any ancillary component, which it was supposed to spend on

[616] See '*Dai-4-kai Chokumen-suru omona kadai to taisaku Part. II* (4. The major problems and countermeasures Part. II)', <http://www.unisys.co.jp/outsourcing/column/column4.htm> (print out on file with author).
[617] *Ibid.*

an IT department.

2. Efficiency (including cost effectiveness);
   With well-established outsourcing services, it is unnecessary for a company to spend money, human resources or time.
3. Being provided with professional IT services and experiences;
   It is likely to be strong and sustainable security systems and it avoids taking cyber risk rather than the self-established security system.

It is also privilege for a company to research, analyse and choose the most suitable outsourcing services amongst many competitors[618].

However, it is hard to say that outsourcing always leads to those advantages. It is not necessary for outsourcing service providers to have a brand-new technology or equipment. They are very likely to utilise their existing skills and machineries rather than employing a brand-new but not well-tested technology [619]. Furthermore, it has disadvantages. Introducing outsourcing services itself can be risky. Hence, it is critical to assure some points before actually introducing outsourcing services:

1. Pursuing enough research, analysis and evaluation when choosing an outsourcing service provider;
2. Pursuing a constant check of quality of the services;
3. Establishing the alternative or contingency plan in the event of any accidental breakdown or failure;
4. Establishing a regular communication method with a service provider;
5. Confirming the provisions in relation to the payment of an indemnity in case of being sued as a result of an accident. This should be clearly written in a contract form[620].

6. The other type of assistance 2: using Alternative Risk Transfer

It is said that there are various definitions of Alternative Risk Transfer (hereinafter "ART"). It is generally considered as a non-traditional risk management approach[621]. ART tends to relate with

---

[618] See 'uk, outsourcing, reduce business operating costs ', <http://www.outsourcer.co.uk/core-competency.htm>, <http://www.outsourcer.co.uk/efficiency.htm>, <http://www.outsourcer.co.uk/cost-effectiveness.htm>, <http://www.outsourcer.co.uk/freedom.htm> and '*Autosôsingu* (Outsourcing)', <http://www.dtcg.tohmatsu.co.jp/serviceline/outs.html> (print out on file with author).

[619] See 'Dai-4-kai Chokumen-suru omona kadai to taisaku Part. II (4. The major problems and countermeasures Part. II)', *supra* n.601.

[620] See '*Kinyû-kikan gyoumu no autosôsingu ni saisite no risukukanri* (Risk management on outsourcing services in financial services industry)', <http://www.boj.or.jp/seisaku/01/sei0112.htm> (print out on file with author).

[621] There is a similar to ART but different risk management method called 'Finite', which also enables companies to deal with a big risk that is traditionally judged uninsurable. See 'Risk Transfer Programs: An approach to greater risk control', <http://www.chubb.com/businesses/art/> and 'Finite', <http://www.ace-insurance.co.jp/risk/risk08.html> (print out on file with author).

insurance since it initially has a close relationship with reinsurance[622]. ART makes it possible to hedge specific risks that have not been accepted in traditional insurance products, such as catastrophe risk[623], by distributing risks in the money market. Morimoto employed Schanz' classification method: (1) Alternative Solutions; (2) Alternative Risk Absorbers, and; (3) Alternative Sales Channels. The typical examples are, holistic covers (also known as integrated risk management or balance sheet protection), contingent capital, insurance linked securities, and derivatives[624].

Low frequency and high severity are the keywords. It is widely believed that cyber risk is potentially very likely to cause an extreme loss. It is the common understanding that no grave case has yet occurred thus far. Indeed, cyber risks fulfil two conditions of being targeted by ART. They are similar to the risk of earthquakes. For instance, Japan sits upon a volcanic zone and it is true (if including unnoticeable quakes) that there are frequent earthquakes. Even if one luckily does not suffer from earthquakes, one cannot entirely be indifferent since it is announced by the mass media as soon as a significant earthquake is registered somewhere within Japanese territory. However, earthquake insurance is not popular. Japanese know earthquakes can be felt anytime but do not believe (or do not want to believe, more precisely) that the strong earthquake attacks will occur in their own vicinity. Cyber risks are in exactly the same position as this. "A hacker attacks someone's computer; but not at MY company!"

Utilising cyber risks by ART, it is possible for financial institutions to raise funds. Securitising cyber risks is a good example. By possessing captive, the profit is obtainable if no incident happens.

Compared with other risk management methods, employing ART methods is yet unique and therefore it seems to be difficult for financial institutions to decide to use ART methods at this moment. Whether this becomes popular or not depends on where the recognition and perception of cyber risks in each company and institution changes.

7. The other type of assistance 3: using Alternative Dispute Resolution

In the case of a company having a civil action brought against it by another party, it is sometimes possible to seek a resolution outside the court which both parties agree upon[625]. This is called Alternative Dispute Resolution ("ADR") and has broadly two different meanings: mediation and

---

[622] N. Hiyoshi, '*Daigaeteki risuku iten* (Alternative Risk Transfer)' (2000) Hoken Mainichi Shimbumsya, Tokyo.
[623] Catastrophe risk is to be low frequency and high severity.
[624] See '*Kinyû to hoken no yûgô ni-tsuite* (Uniting finance and insurance)', <http://www.imes.boj.or.jp/jdps99/99-J-13.pdf> (print out on file with author).
[625] It is possible to arrive at reconciliation as a result of trial. In this context, ADR is the resolution to be sought outside the court.

arbitration[626]. Mediation is the procedure wherein a mediator assists two private parties as a neutral intermediary to reach a mutually satisfactory settlement. This is a negotiated settlement, not adjudicative. Arbitration is a binding dispute resolution by an arbitrator or a tribunal of several arbitrators. If the parties concerned do not come to a settlement by mediation, it generally leads to arbitration. An arbitrator or mediator in this context means a third party, who has fulfilled the requirements and was chosen by a relevant authority. There are governmental or non-governmental organisations for ADR. Some advantages of entrusting ADR are, firstly it is possible to nominate an arbitrator by the parties depending on subjects. Secondly, the process and the judgement of ADR is behind closed doors. Thirdly, it takes a much shorter time compared to the court procedure. Fourthly, due to the existence of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (also known as the New York Convention), arbitration provides an enforceable power[627]. Apart from an international convention or treaty, ADR has its own legal assistance in each country. For instance, the institutional rules of the London Court of International Arbitration are supported by the 1996 English Arbitration Act[628].

ADR is basically available for international commercial disputes. However, it is hardly possible to say that it is popular for any subject. The most popular subject ADR is employed for is disputes on intellectual property rights, with domain name disputes in particular. The World Intellectual Property Organization (WIPO) has established the WIPO Arbitration and Mediation Centre in 1994 as a standing institution, especially for cases involving intellectual property[629].

Indeed, domain name disputes are certainly appropriate to seek the resolutions at ADR. However, it is difficult to say that employing ADR is the most appropriate resolution for other cyber cases at this moment. This is because the vast majority of cyber cases are supposed to be more complex compared to domain name disputes, therefore it is unlikely to be successful in investigating and verifying the cases under the present circumstances. If a hacker is one of the parties concerned, it is almost impossible to settle a case at ADR.

---

[626] Conciliation and early neutral evaluation are also involved. Conciliation is sometimes considered to be synonymous with mediation.

[627] Furthermore, UNCITRAL Model Law on International Commercial Arbitration adopted by United Nations Commission on International Trade Law (hereinafter "UNCITRAL") is adopted by many countries and states.
See '*Chûsai no tokuchô* (The characteristics of arbitration)', <http://www.jcaa.or.jp/arbitration-j/kaiketsu/t-3.html> and 'Arbitration and Mediation Centre', <http://arbiter.wipo.int/arbitration/arbitration-guide/index.html> (print out on file with author).

[628] See 'The London Court of International Arbitration', <http://www.lcia-arbitration.com/lcia/lcia/> (print out on file with author).

[629] See 'The WIPO Arbitration and Mediation Centre', <http://arbiter.wipo.int/center/background.html> (print out on file with author).

8. The other type of assistance 4: miscellaneous

There are varieties of risk management methods. In regard to the issues of computer security, the upshot of the matter is a contest of wits between companies and offenders. It is crucial how effective and quick the response to a brand-new risk is. Without employing urgent new equipment, it is possible to entrap a wrongdoer by using exactly the same equipment a company already has. This trap is especially called the "honeypot" project. By preparing a server computer or network with a relatively weak security system separate from the essential server computer and network, a hacker is very likely to be led into the "honeypot". To analyse what the hacker does against the honeypot, one is able to discover the behaviour and technical skill being employed. The honeypot project generally introduces some specific products and tools to camouflage, such as ManTrap, Specter, Vmware and the like, rather than physically duplicating the servers and network. However, this is not the perfect solution. It has potentialities to aggravate hackers and the honeypot could be exploited to attack the essential server computers[630].

Zero Knowledge Systems based in Montreal published in 2000 that they could assure one's personal characteristics without inputting personal information online. The chief scientist of the company stated that "it prevents people from compiling dossiers". The application of this technology would assist e-commerce as well as e-money. Contrary to this, there was a view that this would be a "repeat" of DigiCash's mistakes[631]. It is true that this technology potentially makes it easy to abuse the privacy of users of the services [632]. Furthermore, this type of technology is mainly prepared for the end users not the intermediary institutions, in other words, financial institutions. Indeed, financial institutions are not in a position to order all account holders to install extra software or employ a new technology to reduce their potential risks.

To avoid taking a risk of damages being claimed, it is vital for financial institutions to prove that they have not neglected the duty of care. It is not acceptable to employ any technology, equipment or skill that covers all risks except one specific risk. However, it is a fact that there is no perfect solitary solution to avoid or minimise cyber risks. Hence, the reality is to implement the assortment of various types of risk management methods to deal with each risk individually. It is most probably practical to establish an effective knowledge management system of a company to find out what type of risks exist, what resources (including human

---

[630] See '*Hani potto wo riyou-shita nettowâku no kikikanri* (Crisis management of computer network by using the honeypot project)', <http://www.atmarkit.co.jp/fsecurity/special/13honey/honey01.html> (print out on file with author).

[631] In relation to e-money and DigiCash, see Chapter VIII.

[632] See 'A New ID-Less ID System', <http://www.wired.com/news/print/0,1294,34477,00.html> (print out on file with author).

resources) are available and the like, as the first step.

Chapter VIII: An Application of Cyber Risk Management for the Account Aggregation Services

1. Introduction

As a great number of different types of services and products exist in the financial markets, so too do almost the same numbers of risks. "Risks" do not always cause damage. While there is a grey area, risks can turn into either profit or loss. "Account aggregation" services are very likely to be defined as a risk in this grey area.

The services have actually been making profits for some aggregation vendors whereas their history in business dates only since 1999[633]. It is a simple explanation that '[the account aggregation services] consolidate customers' online accounts into a single web page, allowing them to view all their accounts from a variety of institutions. Customers would be able to view details of their bank and credit card account balances, share trading accounts, managed funds and loyalty reward programs under only one password and personal identification number[634].' Each secure website, such as banks, stockbrokers, credit cards or even airline companies, requires a specific login name and password to access. The services simplify customers' processes and save time by checking all one's accounts using a single login name and password[635]. Some account aggregation services (hereinafter the "aggregation") also provide financial advice for customers. The services seem to be very useful from the customers' point of view. Nevertheless there are some issues and problems with them.

Aggregation is defined as a brand-new type of cyber risk. By the applications of the analyses conducted in Chapters I to VII, these issues will be examined at length.

2. The Background and its Players

By October 2001 there were more than 20 financial institutions and/or aggregation vendors providing services in the USA[636]. The services had been developed as part of the worldwide trend, such as in

---

[633] Internet banking services started between 1995-1996, however it was not until 1997-1998 that these services became the focus of public attention. See '*Beikoku akaunto Agurigêsyon sâbisu saishin doukô* (The latest trend of the account aggregation services in the USA)', <http://www.sw.nec.co.jp/finance/Special/Aggregation/FSFair401.html>, (print out on file with author).

[634] See 'CBA leads charge for all-in-one bank sites', <http://globalarchive.ft.com/globalarchive/articles.html?id=010809001851&query=account+aggregation>, (print out on file with author).

[635] See 'NATIONAL NEWS: One-stop money e-shop to open NEWS DIGEST', <http://globalarchive.ft.com/globalarchive/articles.html?id=010821000823&query=account+aggregation>, (print out on file with author).

[636] *Ibid.* By October 2001, there were about six account aggregation software vendors. For example, Corillian, Digital Insight, eBalance, 724 Solutions, Teknowledge and Yodlee. See *also* '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', <http://www.nttdata.com/usinsight/8Report1-1.htm>, (print out on file with author).

Japan and the UK. There are mainly four players in aggregation at present:

- Customers (individuals)
- Data providers [637] (such as the financial institutions and airline companies who originally make a contract with customers)
- Aggregators (who actually provide aggregation to the customers)
- Aggregation vendors (who develop the software and provide technology for aggregators)

The following industries have announced their candidacy as aggregators; the portal sites (e.g., MSN, AOL, Yahoo), banks including virtual banks, credit sales companies (e.g., American Express) and securities firms (Table 7.1)[638].

In Japan, however, industries other than the above mentioned have taken action to set up these businesses. For instance, Nomura Research Institute, Ltd. and NTT Data Corporation announced their agreement to run an aggregation business in early 2001. Information Services International-Dentsu, Ltd., Hitachi, Ltd. and Softbank Technology Holdings Corp. have also set up a joint enterprise Account One Co., Ltd., in October 2001. Account One has been expected to turnover three hundred million yen (equivalent to 1.8 million pounds sterling)[639]. In the UK, companies such as Citibank, Virgin and Egg have aroused interest in this business. There are more than 60 banks and 35 stockbrokers who have already started purchasing financial services online, regulated by the FSA. One in ten British adults have purchased online financial services and the UK is expected to be the big target market for aggregation next to the USA[640]. The significant news is that Yodlee, the outstanding aggregation vendor, announced plans to set up a data centre in the UK in 2001. This data

---

[637] The word 'data provider' is used in 'Best Practice Aggregation Guidelines', <www.apacs.org.uk>. (print out on file with author).

[638] The 'portal' sites can be defined as 'Websites that serve as starting points to other destinations or activities on the Web.' See 'NetLingo Dictionary of Internet Words', <http://www.netlingo.com/lookup.cfm?term=portal>. and also '*Beikoku ni-okeru akaunto agurigêsyon sijô no kibo* (The size of the account aggregation market in the USA)', <http://www.sw.nec.co.jp/finance/Special/Aggregation/FSFair403.html>. (print out on file with author).

[639] See 'Japan's First Aggregation Service (Next-generation B-to-C Service) to be introduced', <http://www.nri.co.jp/english/news/2001/010313.html>. and also '*ISID, Hitachi Seisakujo, Sofutobanku-Tekunorojî ga agurigêsyon-jigyoukaisya wo setsuritu (ISID, Hitachi and Softbank Technology set up aggregation joint enterprise)*', <http://www.watch.impress.co.jp/internet/www/article/2001/0911/acount.htm>. (print out on file with author). The exchange rate: £1 equivalent to approximately 170 yen.

[640] See 'Getting to grips with e-risk', <http://www.fsa.gov.uk/pubs/press/2001/066.html> and 'Citibank misses its deadline for online service', <http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT302R0E5RC&live=true&query=aggregation>. (print out on file with author).

centre is the first outside the USA[641].

Table 7.1: The US Players

Financial Aggregators	Vendors	Launch Date	Brand Name
BANKS			
Bank of America	Yodlee	February 2001	Perspectives on Planning
Chase Manhattan	Yodlee	Fall 2000	Chase Online Plus
Citigroup	Yodlee	July 2000	My Citi
City National Bank	Yodlee	February 2001	My Accounts
First Union	Yodlee	Planned for 2001	N/A
Wells Fargo	VerticalOne	August 2000	
INTERNET BANKS			
E*Trade Bank	Yodlee	Planned for 2001	N/A
NetBank		December 2000	Online Consolidation
BROKERAGES			
Fidelity Investments	Yodlee	January 2001	Full View
Merrill Lynch	Yodlee	February 2001	My Financial Picture
Morgan Stanley	Yodlee		
Dean Witter	Yodlee	October 2000	NetWorth
CREDIT CARDS			
American Express	Yodlee	February 2001	Account Profile
PORTALS			
America Online	Yodlee	July 2000	My AOL
Intuit	Yodlee	April 2000	MyAccounts
MSN		May 2000	MoneyCentral
Yahoo	VerticalOne		

*VerticalOne had been merger into Yodlee. (Reference: '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621 and also TowerGroup, 'Aggregation for the Little Guys', <http://www.banktechnews.com/btn/articles/btnaug01-4.shtml>, (print out on file with author).

The social background of aggregation's greeting in the USA is rooted in the prosperous development of Internet access. The more popular online banking services became, the more various type of services and information became available online. Commercial websites were inundated one after another, as if having a website was indeed a proof of doing proper business. Unlike Japanese people, US citizens were

[641] See 'Yodlee strengthens UK presence', <http://www.yodlee.com/company/pressreleases/uk.html>, (print out on file with

accustomed to investing their assets. It was natural for individuals to try to find the best choice for investments from a large number of financial products. As a result of that, the number of accounts for individuals increased, and incidentally, the number of login names and passwords increased, and then aggregation finally gave a first cry[642].

The initial account aggregation services were provided by Yodlee,Inc. in 2000. The company itself was established since 1999 and it succeeded in getting their first client, Citigroup, in July 2000[643]. Aggregation was for accounts excluding the financial matters in the first instance. Aggregating non-financial accounts into a single page is as good as making a snapshot of the information a customer wants. It makes it possible to abstract the necessary information, satisfying one's parameters out of various information categories. This service is not very different from gathering information by using search engines. The significant differences are:

1. Specific parameters/query words for searching information remain and the updated searched results are always visible (but not time-consuming);
2. More than two different types of information can be shown on a single screen[644].

For example, one could obtain entertainment information if one's favourite film star 'Brad Pitt' performs as well as property information within one's budget on the same screen[645]. The Financial Services Authority of the UK explained aggregation as:

> "Account aggregation lets you see the information from all your online accounts on one website. This could include your current account, savings and investments, mortgage, credit cards and personal loans and reward schemes such as supermarket reward points or air miles[646]."

The concept of e-commerce had primarily been "B to C"(a single business to plural customers), one-way only. However, aggregation

---

author).

[642] See '*Kinyû akaunto agurigêsyon* (The financial account aggregation)', <http://www.sw.nec.co.jp/finance/N_Souken/Article/200107-3.html>, (print out on file with author).

[643] See 'Aggregation for the Little Guys', <http://www.banktechnews.com/btn/articles/btnaug01-4.shtml>, (print out on file with author).

[644] The services are available not only via the Internet, but also via web-enabled mobile phones. See '*Beikoku ni okeru akaunto Agurigêsyon no shinten* (The latest progress of the account aggregation services in the USA)', <http://www.nri.co.jp/report/sihonsijo/01_spring/04-04_004s.htm>, (print out on file with author).

[645] The account aggregation trial website is 'Spyonit', <http://www.spyonit.com/>. Spyonit is technically assisted by one of aggregation vendors, 724 Solutions Inc.

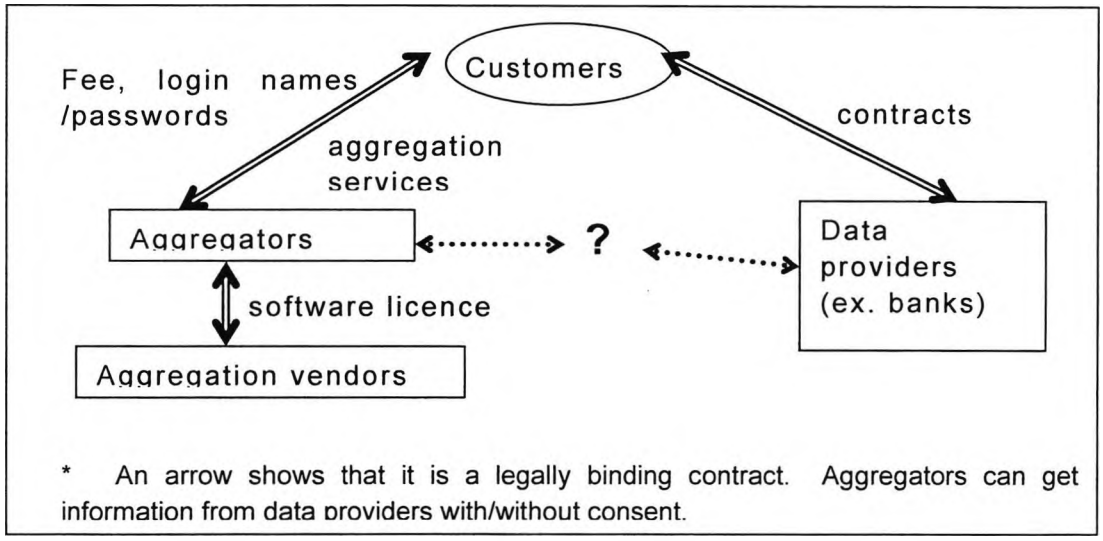
[646] See 'fsa, what's new, e commerce', <http://www.fsa.gov.uk/consumer/whats_new/updates/e_commerce/mn_aggregation.html>, (print out on file with author).

changes it into plural businesses to plural customers or possibly, the other way around. It is not always necessary to have a login name and password if one gathers the above-mentioned information. In 2000 OnMoney.com started the financial service, followed soon after by many financial institutions [647]. Since then a lot of financial institutions have been involved. Furthermore, aggregation extremely increased the importance of financial institutions, rather than any other industry, as a data provider. So it is possible to say that aggregation is very likely to be recognised as a part of financial services.

All financial services' and membership accounts require an individual login name and password. So the third advantage of aggregation appeared to be revealed as:

3. By entering a solitary set of login name and password issued by the aggregator, a customer is able to check all of his/her accounts on a single screen.

Table 7.2: The players of the account aggregation



The most noteworthy point, in the first place, was that it is unnecessary to have an agreement or consent between data providers and aggregators [648]. (Table 7.2) The technology called "screen scraping" made it possible to get information from the data providers' website without their cooperation. In reality the role of data providers had been

[647] See '*Kinyû-gyôkai ni jisedai-BtoC sâbisu tanjô. Agurigêsyon-sâbisu niyoru kokyaku-kakoikomi ha seikousuruka*? (The account aggregation, the new service for the next generation BtoC, has now arrived in the financial market. The question is will it prove a success in ensuring customers?)', <http://www.atmarkit.co.jp/fitbiz/keyword/aggregation/keyword7.html>, and also '*Beikoku akaunto Agurigêsyon sâbisu saishin doukô* (The latest trend of the account aggregation services in the USA)', *supra* n.618.

[648] See '*Kinyû akaunto agurigêsyon* (The financial account aggregation)', *supra* n.627.

diminishing for a while. This was largely related to the most remarkable point of the services. Aggregation contains many aspects, but the service's centre of attention is in controlling customers' login names and passwords. The more secure websites one accesses, the more long and meaningless the required password. Many secure websites, such as for online banking, normally require eight digits for a login name. There is sometimes more than one password required to access a website[649]. Furthermore, people are very likely to have several accounts, for which each need an individual login name and password to access, such as Internet banks, securities firms, airline companies and supermarkets. It is sensible in cyberspace to have a different login name and password for each account. However, it is only natural to choose either an easy or a single-word login name and password for all accounts. Nowadays one's name, birthday, telephone and any simple easily-guessed words or numbers (such as 1111 and 1234) are sometimes automatically rejected, due to security reasons, when opening an account. The FSA of the UK published tips on online services for consumers in June 2001. It recommended not only choosing login names and passwords carefully but also trying to remember all of those without writing them down[650]. No one would feel comfortable about committing all-different, no-clue-to-remember, many names and numbers, to memory. To be provided aggregation, a customer has to register for the services by informing the aggregator of all login names and passwords for his/her accounts. Then it issues a brand-new solitary set of login name and password instead. A customer uses this unique set of login name and password to access the services. However, these providers, in reality, only substitute for the customers. It means the providers automatically get access to the websites and gather information by using the informed login names and passwords when a customer uses a solitary login name and password. Regardless of whoever uses a proper login name and password issued by financial institutions in the first place, there is no mean to know whether one is really their customer or not[651]. On account of this issue, the short history of aggregation seems to be dramatic.

One presently finds well-known institutions and firms taking part in aggregation, such as Bank of America, Chase Manhattan, Citibank, and

---

[649] It is mainly banks that issue more than one password for different directions of use or purposes.

[650] See 'New FSA help for consumers on making the most of the internet', <http://www.fsa.gov.uk/pubs/press/2001/065.html>. (print out on file with author).

[651] Even by manipulating up-to-date technology it is hardly possible to identify who gets access to the websites, due to the lack of the system of global addresses. In the future if the global addressing system (so-called 'IPv6' system) becomes available, it will then be possible to allocate a unique Internet Protocol Address (IP address) for an individual computer on a worldwide level. This system will make identifying a customer possible by the computer used. However it will be unreliable to assume that a customer always uses the same computer. Furthermore, checking an IP address without informing the customer is likely to infringe privacy. The author obtained this information from the interview with an IT consultant. Here the company remains anonymous by the company's request. The author would like to thank the company for its frankness.

Wells Fargo on the one hand; AOL, Intuit, MSN and Yahoo on the other. However, in December 1999, the very first year of aggregations' debut in the market, First Union Corp. brought a lawsuit against the Paytrust unit of Secure Commerce Services Inc. in regard to providing services by gathering information from First Union's website without its approval. In the end, the case was settled for the Paytrust unit to heed the guidelines prepared by First Union Corp. This is only one of the many examples. Some would say that the financial institutions had been hostile against the aggregators. If it is an overstatement, it is not too much to say that they had been very reluctant to introduce aggregation and/or had loathed to ignore the services' provided for their own customers by the aggregators[652]. However, the mood of the financial institutions against aggregation was suddenly mitigated and even became amicable in 2000. The reasons and grounds for this will be discussed in depth later.

Online banking services themselves have since flourished. The biggest reason is a high rate of interest compared to the traditional "bricks and mortar[653]" banks. For instance in the USA, it was said to that there were about 113,000 customers in NetBank by September, and about 2.3 million customers in Wellsfargo.com by October 2000. A report was published that the number of online banking customers had reached 23 million customers (1.7 % of all households) in 2001. In Europe the Internet is only the third means in banking communications, whereas about 27 million Europeans are expected to engage in mobile banking, with about ten million for Digital-TV banking by 2005[654]. Egg in the UK had 1.5 million customers by 2000[655]. Both NetBank (USA) and Egg (UK) provide banking services online only. The customers are, at first, very likely to open an online banking account in the main "brick and mortar" bank, with which they have had a bank account for a long time. So, the total number of online banking customers could be unimaginable. If that is the case, to what extent has aggregation spread over the Internet? In the USA, the most prosperous place of this business worldwide, there have been about 600,000 customers in 2000 and the market growth can be expected to

---

[652] See 'American Banker-The Financial Services Daily, While Others Quail At 'Screen Scraping,'Fleetboston Will Embrace It on New Site', <http://www.yodlee.com/company/news/articles/amerbanker_services.html> and '*Beikoku akaunto Agurigēsyon sābisu saishin doukō* (The latest trend of the account aggregation services in the USA)', *supra* n.618.

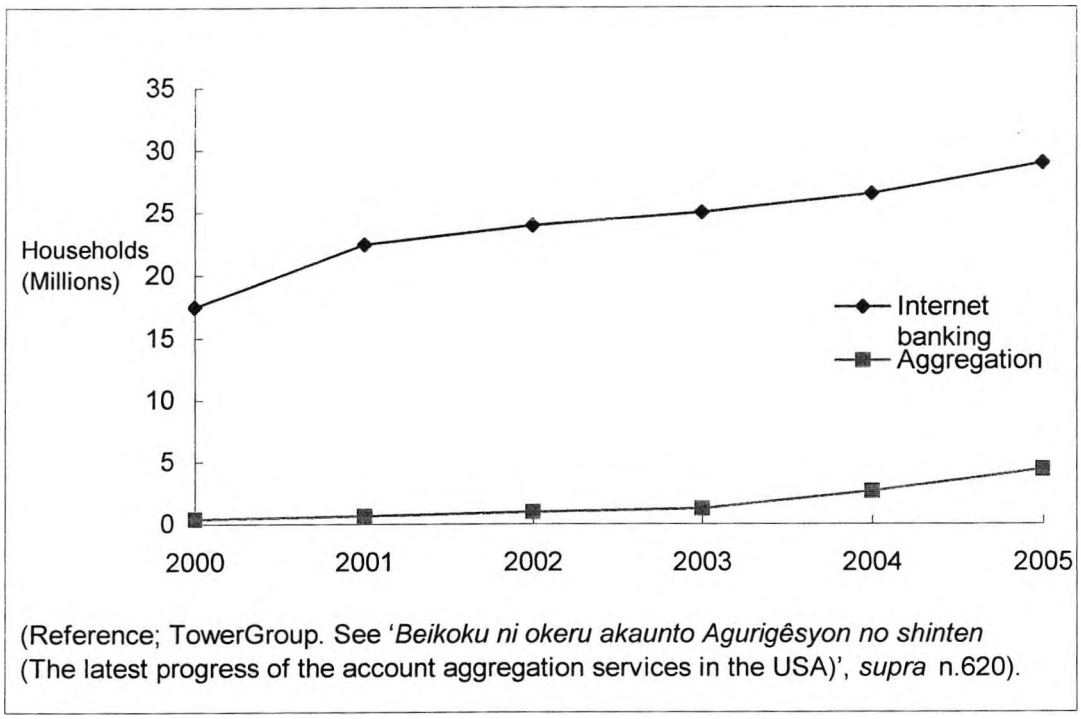
[653] "Bricks and mortar" is defined as a traditional banking business running in a store only. An antonym of this is "Click and mortar" meaning a mixed business with the Internet and a store. See 'CNET Japan', <http://japan.cnet.com/Help/manual/0911.html>, (print out on file with author).

[654] A report was published on online banking strategies in Europe, 'Looking ahead', <http://www.fstech.co.uk/thebigfeature.htm>, (print out on file with author).

[655] See '*Beikoku ni-okeru akaunto agurigēsyon sijō no kibo* (The size of the account aggregation market in the USA)', *supra* n.623. *The Financial Times* dated 20th February 2000. The article is also available on its website, 'Egg remains confident of breaking even BANKS OUTFLOW OF CUSTOMERS SLOWS IN FOURTH QUARTER BUT ANNUAL LOSSES INCREASE TO Pounds 155M', <http://globalarchive.ft.com/globalarchive/articles.html?id=010220001157>, (print out on file with author).

reach 35 million customers in 2004[656]. It seems that about 3% of US online customers have received the blessing of aggregation. (Table 7.3)

Table 7.3: Size of the Market in the USA



(Reference; TowerGroup. See '*Beikoku ni okeru akaunto Agurigêsyon no shinten* (The latest progress of the account aggregation services in the USA)', *supra* n.620).

The other survey estimated the growth from about one million to ninety million by 2005[657]. There is a statement to support this upward tendency of aggregation. According to the report published by McKinsey & Co (USA), US$1,700 (equivalent to £1,188) per a year can be saved by using the services[658]. It is, however, true that there are anxieties that undermine the financial institutions' optimism. To trust in aggregation, to some extent, when considering the issues and problems will be discussed in the later section.

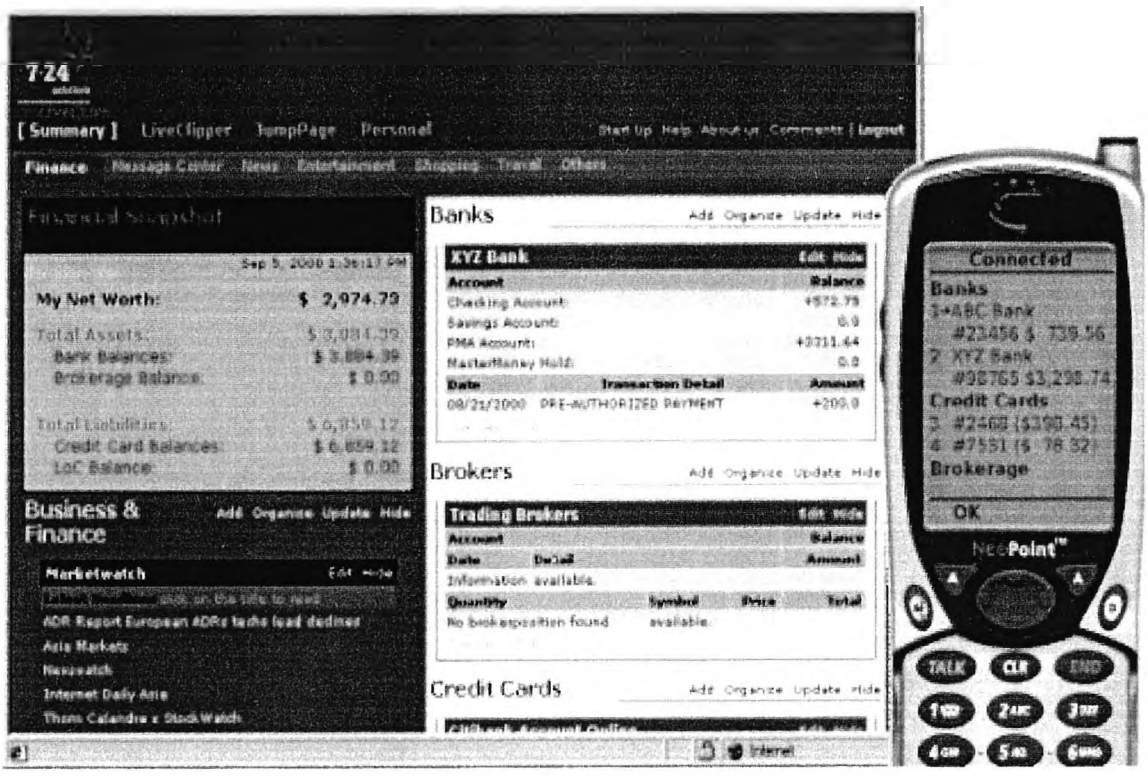
3. The Services and Customers' satisfaction

There are mainly three technical methodologies engaged in aggregation. The first methodology is called "screen-scraping". It

[656] See '*Kinyû akaunto agurigêsyon* (The financial account aggregation)', *supra* n.627.
[657] See 'Wells Fargo revs up account aggregation wagon', <http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2001/01/22/newscolumn2.html>, (print out on file with author).
[658] *The Financial Times* dated 28th July 2001. The article is also available on its website, 'UK gets new one-stop site', <http://globalarchive.ft.com/globalarchive/articles.html?id=010728001043&query=account+aggregation>, (print out on file with author).

literally scrapes information off from various websites. To be specific, an aggregator has been given all login names, passwords and website addresses for all online accounts of a customer whilst the customer receives a solitary login name and password to access the aggregator's website (hereinafter "destination site"[659]).

Figure 7.1: The example of Account Aggregation



(Reference: 724 Solutions, '*Kinyū-gyôkai ni jisedai-BtoC sâbisu tanjō. Agurigêsyon-sâbisu niyoru kokyaku-kakoikomi ha seikousuruka*? (The account aggregation, the new service for the next generation BtoC, has arrived in the financial market. Will it prove a success in ensuring customers?)', *supra* n.632.)

Suppose a customer originally has made contracts with six different online accounts; two national banks, one each for overseas bank, stockbroker, airway for mirage and supermarket reward programme. The aggregator gets access to six registered websites by using six login names and passwords as impersonating its identity. Once getting access to the targeted institution's website (hereinafter a "host website"), it then pulls the account's information and downloads it into its website. The information downloaded is parsed to extract required data only, and then finally it is

[659] Destination sites are defined as "the websites on which aggregated data is presented to users" in 'BEST PRACTICE AGGREGATION GUIDELINES', *supra* n.622.

saved onto a /or in a database to redirect it as consolidated data for the customer. (Figure 7.1) As the correct login names and passwords are used, it is impossible for data providers (such as online banks) to distinguish a subject contracted from an aggregator. Moreover, this is the reason why aggregation enables an aggregator to commence services without consent of the data providers. Thus, this screen-scraping method seems to be easy for an aggregator to apply for. However, it involves some disadvantages. Firstly, data accuracy is not guaranteed one hundred percent. Layouts of some host websites are intentionally changed frequently and this is very likely to mislead data presentation. To fulfil data accuracy, it is necessary to monitor these host websites. Secondly, efficiency in performance is low so that constant maintenance is necessary[660]. In relation to maintenance, security is maintained by an aggregator in employing screen-scraping. This security evidently costs greatly. If the data integrity is doubtful, it is obliged to say that this methodology is unsuitable to deal with financial information. Thirdly, the issue as to when the accounts should be aggregated must be considered. At the very least it is critical to aggregate a customer's accounts on a daily basis. Needless to say, timeliness is the most crucial issue for the financial services. As little as an hour makes a substantial difference for financial transactions, as supposedly they happen after a customer checks information in the aggregated screen. Therefore, whether or not an aggregator aggregates customers' accounts on an overnight basis should be reconsidered[661]. Furthermore, screen-scraping does not employ any standard, so it has been scrutinised.

The second methodology being used in aggregation is called "permissive aggregation", which was developed after screen-scraping to overcome its weak points. Data is actually fed by financial institutions themselves using techniques called Interactive Financial Exchange (IFX) or Open Financial Exchange (OFX). All data is automatically provided in real-time in cooperation with data providers in this methodology. This is said to be almost the same model engaged with Automatic Teller Machines in banks. Unlike screen-scraping, data is controlled by data providers in the host websites and security is maintained by them. Permissive aggregation supports transactional websites and personal financial software and streamlines the process of financial institutions. OFX is adopted as the standard for online banking transactions[662]. As it is indispensable for permissive aggregation to be understood and supported by data providers, this is not always available for an aggregator.

The third methodology is called "Desktop' aggregation". The

---

[660] See '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621.
[661] See 'Account Aggregation: Consolidate, or be Consolidated?', <http://www.unisysfinancial.com/events_news/publications/articles/account_aggregation.asp>. (print out on file with author).
[662] *Ibid.*

biggest difference to the first two methodologies is that the software for aggregating information is installed in a customer's computer. In this methodology, login names and passwords remain in a customer's hand as being encrypted. However, the technique engaged in this methodology is, in reality, screen-scraping. So its shortfalls still remain, except for the issue of login names and passwords[663].

In regard to a model of the business, there are two different ways to offer aggregation. One is outsourcing; aggregation is offered by an aggregator as an Application Service Provider (ASP). The other one offers an in-house service. The former case is basically offered by 724 Solutions, Advent Software, ByAllAccounts and Yodlee, the latter examples by CashEdge and Teknowledge. Outsourcing could save time to start the business although it would not be possible to have any speciality of an aggregator. On the other hand, an in-house service would be time-consuming to develop as a system harmonised with the other systems. Thus it is comparatively expensive. An aggregator's advantages could also be utilised in the service. Furthermore, aggregation is under its control without any third party; the less parties involved, the firmer security[664]. This would distinguish the service from rivals' services and give an impact of advertising the service towards customers.

Aggregation basically contains four different services;

1. Aggregating accounts' service
2. Aggregating web contents' service
3. Messaging service
4. Advising service

The first and the second are self-explanatory. Aggregating accounts' service make one's multiple accounts displayable by using a solitary login name and password. Aggregating web contents' service consolidates all information one requires from the Internet and updates it. In other words, the first two services enable a customer to have the sole financial port to control all transactions. This means that it conclusively causes transparency on financial transactions; it allows a customer to find a false transaction, discrepancies or even frauds more easily than ever. Customers are likely to check their accounts frequently. The more familiar one is with one's accounts, the quicker one detects frauds[665]. The third service is to alert a customer, by emailing, on the aggregated

---

[663] See 'APACS publishes best practice guidelines for account aggregation', <http://www.apacs.org.uk/downloads/aggregationpr2.pdf>. (print out on file with author).

[664] See '*Akaunto agurigêsyon no kinou* (The functions of the account aggregation)', <http://www.sw.nec.co.jp/finance/Special/Aggregation/FSFair402.html>. (print out on file with author).

[665] See 'Account Aggregation: Consolidate, or be Consolidated?', *supra* n.646 and *infra* n.652, and 'Account Aggregation - Consumers' Questions Answered', <http://www.europathway.net/newsresult.asp?ID=53>. (print out on file with author).

account's website and/or sending text messages to a mobile phone, the latest information which meets preset parameters a customer has given. The parameters could be anything; from weather forecasts to share price's information[666].

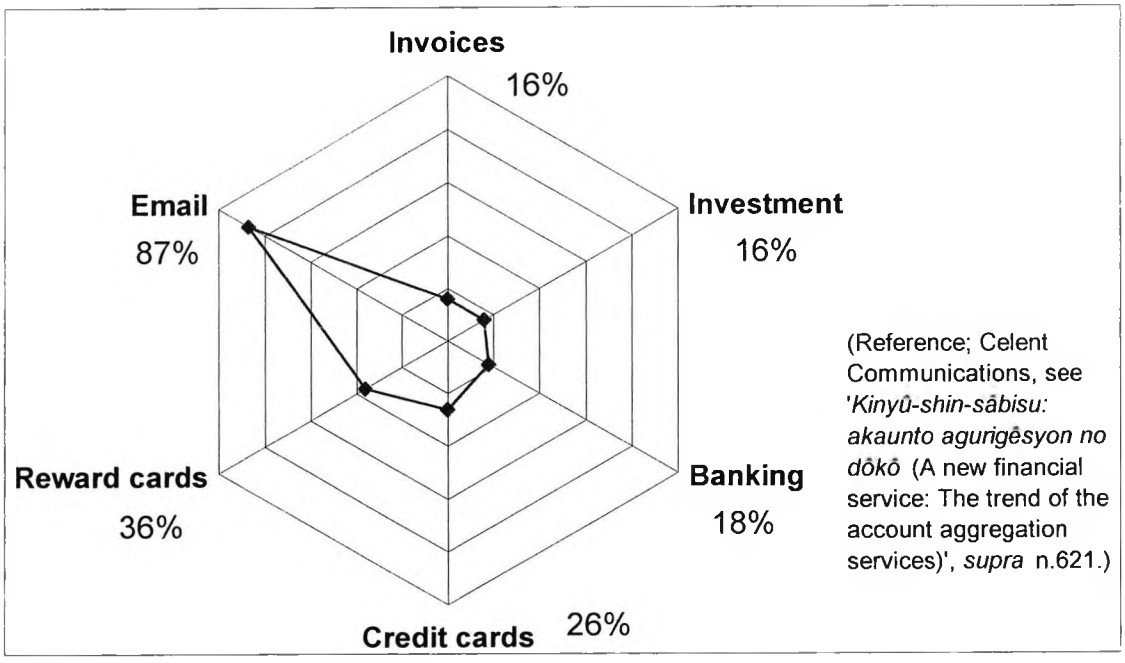
The fourth service is to give advice, especially financial advice, to the customers on the aggregated website. Financial products and services will be custom-made if this service works properly. This is, however, not offered by all aggregators at present. In some aggregation cases, giving financial advice is available only for selected customers (such as an affluent class). But there is a possibility that it may be available for all customers in the future. All four services ultimately give customers an opportunity for total assets' management. This will indirectly enhance the market's competitiveness, so that a wide range of financial products and services will be available for customers[667].

What could be the most valuable service for customers? Yodlee,Inc., for instance, aggregates information from approximately 2,000 institutions. Then 800 out of 2,000 (40%) are related to financial matters/institutions to a greater or lesser extent[668]. Therefore, the useful services frequently utilised by aggregation services' customers tend towards the financial services (Table 7.4). Some potential customers may misunderstand that it is possible to transfer money one to the other within aggregation. However, it does not have bank transfer functions at present. So if one wants to transfer money from *A* bank to *B* bank, one has to get access to *A* bank's account separately after logging off from aggregation service.

---

[666] See 'Japan's First Aggregation Service (Next-generation B-to-C Service) to be Introduced', *supra* n.624.
[667] See 'Account Aggregation: Consolidate, or be Consolidated?', *supra* nn.646 and 650, and 'Account Aggregation - Consumers' Questions Answered' , *supra* n.650.
[668] See '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621.

Table 7.4: The Customers' Focal Utilities



(Reference; Celent Communications, see '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621.)

In regard to a charge for aggregation service, the services are offered mostly free at this stage[669]. "FTyourmoney" (operated by accountunity Ltd.) and "My Accounts" (provided by Citibank) are concrete examples in the UK. My Accounts aggregates more than 2,500 sites including Goldfish, Stocktrade, Bank of Scotland and Egg[670]. The possible reason for offering free aggregation service is explained thus: the aggregators, especially financial institutions such as banks, are much keen to take a promising opportunity in the future[671]. That is to say that aggregation seems to have recognised itself as profitable, therefore, its subsidiary works to bring a gain. Incidentally, if the financial market tends to offer aggregation services free of charge, charging a commission could let customers go by. However, the idea of free service is not yet settled at present; whether free or not depends on the aggregators' decisions.

Considered overall, there remains doubt whether aggregation is really useful for customers or not. It is, in essence, helpful to aggregate

---

[669] Some aggregators offer aggregation service for specific customers who fulfil certain conditions. The conditions could vary, for example, customers who have bought shares more than once in the past six months, etc. See '*Kojin-muke ni 3-taipu no agurigêsyon-sâbisu teikyou-kaishi* (Three different types of aggregation services are available for individual customers)', <http://www.nri.co.jp/news/2001/011025.html>, (print out on file with author).

[670] See 'Aggregate to accumulate'' <http://www.moneyextra.com/features/2001/f011004_investment_84.html> and 'FTyourmoney launches online "financial dashboard"', <http://uk.biz.yahoo.com/011219/66/cm3og.html>, (print out on file with author).

[671] See 'Aggregate to accumulate', *supra* n.655.

information one needs; the services simply save time and also money as a by-product. But it still takes time when one signs off from the aggregated site after checking the accounts, then logs in on each account for transactions. The benefits and anxieties of aggregation will be mentioned later; security is the highest priority and the centre of attention in this business. Whether one takes convenience (plus time and money saving) then registers aggregation, or considers security more important than any advantages and refrains from using it, the choice is for the customer to make.

4. The Benefits and Anxieties for the Aggregators

As has already been mentioned, aggregation service is free. Contrary to this, the service providers incur a high business cost. There is an example that an aggregation vendor charges about US$400,000 to 2 million for licensing its software, and furthermore adds between $10 and 18 as an annual fee for each customer. One stated that it costs $53 per a customer for the first year's implementation of aggregation[672]. Suppose all of Egg's customers (1.5 million by 2000 as mentioned earlier) have registered for aggregation, a vendor charges $400,000 for licensing, and $12 as an annual fee per person. The total annual fee could be more than $18 million! It would not be an enormous amount of money for large institutions and companies, whereas it is obviously a far greater financial obstacle for small and medium-sized enterprises. In reality they ought to have their own websites to offer the services for customers before anything else although constructing websites for business costs a fortune. According to the survey done by Unisys, the truth is that 94 out of 400 leading banks worldwide have not had their own websites[673].

Even for large enterprises it could be a big risk if the invested business did not bring a gain. If that is the case, what could be the benefits for the aggregators? The possible benefits for the aggregators are as follows:

Aggregation service enables data providers to:

1. Guide customers to an aggregator's own website often; this enhances customers' familiarity with their products and services[674] ;
2. Ensure customer loyalty (i.e., prevent customers being drawn to other rival institutions[675] ;

---

[672] See 'Aggregation: An Untouched Opportunity For Financial Institutions', <http://www.microbanker.com/artarchive02/hallcreditlendAggregationAnUntouchedOpportunityFor121501bts.html>, (print out on file with author) and also 'Aggregation for the Little Guys', *supra* n.268.

[673] See 'NEC solutions, Weekly Topics Vol. 105', <http://www.sw.nec.co.jp/column/backnum/11/115.html>, (print out on file with author)

[674] See '*Kinyû akaunto agurigêsyon* (The financial account aggregation)', *supra* n.627.

[675] K. Katayama, '*Beikoku ni-okeru akaunto agurigeisyon no sinten* (The Development

3. Charge for providing a service in the future[676] ;

The three benefits above are fundamentally available for any type of party who is interested in being a data provider. It is, however doubtful whether other industries (except financial institutions) would benefit from the said three standpoints. In addition to this, they are able to enjoy another benefit as follows:

4. Grasp customers' financial standing to enable presenting the best and most appropriate products corresponding to each customer's need;

To pursue the benefits from providing aggregation services, the new online market would be developed as well as competitive advantages found. Furthermore, customer satisfaction and loyalty would be built up[677]. As mentioned earlier, financial institutions showed hostility against aggregation until it suddenly became amicable in the middle of the year 2000. The change was said to be astonishing even for the individuals concerned. The reasons for this change were closely connected with the above-mentioned benefits. The financial institutions might have recognised that aggregation was the market's trend, or customer demand. They most probably considered developing aggregation as a potential business opportunity. In addition to these, in financial institutions one serious obsession must augur that both potential and existing customers would be fascinated and lured away by rival institutions unless one launches aggregation service[678]. Indeed, it could be a real business opportunity if the potential benefits of aggregation are borne out. Unfortunately, it could be possible to say that being involved in aggregation business, in the beginning, could have been a desperate or negative decision for financial institutions. Why? Because financial institutions should be cautious regarding security and privacy. On the other hand, aggregation is available for any industry to offer. While banks refuse to be involved in aggregation on the grounds of placing importance on security and privacy, disintermediation, especially of non-bank services, could be another threat[679]. What makes the situation even worse is that the legitimacy of aggregation business has not yet been well defined.

---

of Account Aggregation in the USA)' (2001) Capital Market Quarterly Spring, Nomura Research Institute, at 35-49. It is easy to understand this in the case of credit cards. When issued with a new credit card, one needs to register one of the bank accounts. After one begins to use that credit card, it is most unlikely that one will change from the registered bank. As a result, financial institutions will hold onto more of their customers.

[676] See '*Kinyû akaunto agurigêsyon* (The financial account aggregation)', *supra* n.627.

[677] See 'Aggregation: An Untouched Opportunity For Financial Institutions', *supra* n.657.

[678] See '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621.

[679] See 'Lack of Regulation Increases Insecurities', <http://www.erisk.com/news/analysis/news_analysis2001-05-22_01.asp?>, (print out on file with author)

There have been neither guidelines adopted nor announced as to who the relevant authority could be in any country. Aggregation hastily started before it had been fully considered from every angle in the USA. It should be possible to say that it was natural enough to be started there; and that such a business would never have succeeded within Japanese culture and tradition even if the business model had originated there.

5. Unsolved Issues

5.1 In general

According to a survey done by Forrester Research, Inc., aggregation hardly makes a profit at this stage due to low customer adoption, high vendor costs, and firms' inability to mine the data although 51% of financial institutions responding to the survey answered that they believed in aggregation's profitability [680]. On the contrary, there is a bright view for the aggregators and their cooperative data providers that customers are very unlikely to switch from an aggregator once they register. Having entered all accounts information and personal details in applying for aggregation, it would take time and is trouble. So it is said that they hardly bother themselves to re-register for another aggregator. Some aggregators rushed into a business for this reason[681]. Another survey supports this theory that only 3 % of life insurance and 2 % of brokerage customers consider to switching institutions. It added "Financial products are not impulse purchases"[682]. However, it does not change the fact that aggregation is not a highly profitable business at present. In reality, another survey disclosed that only 7 % out of all Internet connected households in the USA were interested in aggregation. It is also said that online banking develops its market very slowly as opposed to other parties involved in this business. It cannot be avoided in the economic circumstances of late that people generally may prefer to be a conservative and not to take a risk[683]. Many criticisms are still inevitable against aggregation. If that is the case, who is this 7%? What does a real customer for aggregation at present look like? A study revealed a portrait of the customers as follows:

- 63% are male;

---

[680] See 'Consumer Account Aggregation Won't Deliver ROI For Most Financial Firms, According To Forrester Research', <http://www.forrester.com/ER/Press/Release/0,1769,609,00.html>, (print out on file with author).

[681] See 'Aggregation for the Little Guys', *supra* n.268 and *infra* n.668, and '*Beikoku akaunto Agurigêsyon sâbisu saishin doukô* (The latest trend of the account aggregation services in the USA)', *supra* n.618.

[682] See 'Consumer Account Aggregation Won't Deliver ROI For Most Financial Firms, According To Forrester Research', *supra* n.665.

[683] See 'Aggregation for the Little Guys', *supra* nn.268 and 666, and 'Categorization Plus Syndication Does Not Necessarily Equal Viability', <http://www4.gartner.com/DisplayDocument?id=334188&acsFlg=accessBought>, (print out on file with author).

- The average age is 36 years old. 64% of aggregation customers are between 25 and 39 years old;
- The average number of the aggregated accounts is 5, of which 41% are financial accounts;
- 81% have incomes between $50,000 and $149,000[684]

As the survey shows, less than half of the total financial accounts are aggregated. What makes people relinquish an interest in aggregation? It is because of security and privacy issues. Customers lose interest when they realise they have to disclose all accounts details, especially some of accounts finances participate in, to an aggregator[685].

Security is always a central issue in any business connecting with a computer network. One of aggregation services advertised that its service was secured from Internet hackers, unlike its rivals, owing to storing information on a customer's computer, not disclosing login names and passwords[686]. Is it true that using aggregation is safe if login names and passwords are kept inside an individual computer? It is, unfortunately, not always true. Any computer security can be breached from anywhere although it could be possible to say that the potential risk in this methodology is a little less than screen scraping and so on.

In particular, customers are very likely to have no doubt that financial institutions are liable as to whatsoever may happen to their accounts. In reality customers would not check to see if their computer systems are truly highly secure. In other words, customers involuntarily put their confidence in financial institutions. This gravely influences running a business from financial institutions' viewpoint. To sustain and prosper businesses, therefore, they are responsible to respond to their customers' tacit claim, proving the security system is highly maintained to the greatest degree. Aggregation, however, has had an impact upon not only customers, but also financial institutions themselves, to reconsider. Having a solitary login name and password definitely increases risk. If one uses online banking without aggregation, and if a hacker successfully uncovers one's login name and password, one's potential financial loss would be restricted to a deposit in the online bank account. In case of hacking, for one who has five financial accounts (with just one solitary login name and password for aggregation) it is simple mathematics that the potential financial losses would be five times or even more. From customers' point of view, their anxiety is whether their accounts are surely secured against internal and/or external offences. The issue is who would be responsible and compensate for their losses in case of any shortfall caused by a failure, an error or offence. It must be clear who customers should rely on.

---

[684] See 'Account Aggregation: Consolidate, or be Consolidated?', *supra* n.646.
[685] See 'Consumer Account Aggregation Won't Deliver ROI For Most Financial Firms, According To Forrester Research', *supra* n.665.
[686] See 'FTyourmoney launches online "financial dashboard"', *supra* n.655.

Speaking of security, internal attacks are, however, not of concern to a greater or lesser extent due to the said reasons[687]. As it was mentioned earlier, security systems are maintained by data providers if there is consent between two parties. If not, it is supported by the aggregators. The former case could be simple. Two parties have agreed about this issue when they made a business contract. Considering external offences, financial institutions would probably assure customers that their computer security is perfectly secure. In fact they have been very likely to introduce the toughest security compared to any other industries in the interest of keeping good reputation and winning customers' confidence[688]. The latter case could not be that simple. Financial institutions are concerned that they might be liable for losses when hackers attack even if there is an inadequacy, error or a loophole in the aggregators or aggregation vendors[689]. If an aggregator implements screen scraping without a consent from data providers, is it necessary for a customer to check the availability of an aggregator's financial assets before signing aggregation for filing a suit against the aggregator?[690]. Although Corillian International stated that a financial institution would compensate for losses in case of any event to avoid "brand damage", customers cannot play for high stakes[691]. One could say that 7% of the US aggregation customers are challenger!

The next issue is that aggregation may infringe customers' privacy. This is because aggregation collects personal information such as individuals' financial status, contact addresses and so on. It is possible for aggregators to sell this personal information database to a third party, who may want it for marketing purposes. If not for that, they are able to email certain selected customers, who meet conditions, to advertise a product or service on behalf of a third party as a part of business. In some services, the aggregators have declared in their websites not to disclose or use personal information for any other purpose. Some aggregators stated they would not disclose any personal information unless customers agree to do so[692]. In principle, there is a box in both an online application or a paper form to check to show a preference if a customer does not want personal information to be disclosed or used for marketing.

---

[687] An "internal offence" in this context means any offence being committed by an employee(s) of a financial institution.

[688] See '*Kinyû-gyôkai ni jisedai-BtoC sâbisu tanjô. Agurigêsyon-sâbisu niyoru kokyaku-kakoikomi ha seikousuruka*? (The account aggregation, the new service for the next generation BtoC, has arrived in the financial market. Will it prove a success in ensuring customers?)', *supra* n.632.

[689] See '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621.

[690] See 'Account Aggregation - Consumers' Questions Answered', *supra* n.650.

[691] See 'UK gets new one-stop site', *supra* n.643.

[692] See '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621, and '*Akaunto Agurigêsyon wo shitteimasuka?* (Do you know the account aggregation services?)', <http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20011220/1/>. (print out on file with author).

It must be clear enough to attract a customer's attention, and also customers themselves must be careful when signing an agreement.

The greatest fear for financial institutions is aggregation causing them trouble whether they run aggregation by themselves or are involved with aggregators. It is not, strictly speaking, either a security or privacy issue. That is, primarily, either aggregation is a legitimate or illegal business. Secondly, it is how and by whom it could be regulated if it is defined as a legal business. In the UK, regarding the first issue, Virgin published the statement that it felt that introducing aggregation might conflict with the Data Protection Act 1998 and the Copyright and Rights in Databases Regulations 1997 in relation to the access to personal information. There is a view that the aggregators could breach the contracts and/or intellectual property rights between a customer and a data provider including criminal liability under the Computer Misuse Act 1990[693]. Disclosing a login name and password would also breach the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contract Regulations 1999[694]. In reality, FSA most surprisingly says that a customer may not be protected by the Financial Ombudsman Scheme or the Financial Services Compensation Scheme. Its Managing Director announced on 15th of May 2001 that:

> "...The FSA will have no powers to regulate the provision of account aggregation. This activity will fall outside the jurisdiction of the FSA and, as a result, we cannot guarantee you [customers] the protection of the regulatory system if something should go wrong... "

It suggested for institutions under its supervision to pursue a fair business on legal, security and systems and controls issues as well as to meet minimum standards, which the FSA expects. The FSA has no power over unregulated firms, unless they provide services such as investment advice, dealing facilities or arranging deals[695]. Furthermore, Barclays bank has announced that disclosing individual information to a third party invalidates an online anti-fraud guarantee for a customer. Like this financial institution, if terms and conditions of any institution refer to aggregation as a breach of contract between a customer and an institution, this customer could be liable for any offence that happens against an account[696].

---

[693] Applying screen scraping is likely to infringe Intellectual Property Rights because it uses Java applets. Virgin also claimed that "Virgin blamed problems with 1997 database law, which makes it [=aggregation] illegal to re-arrange information from another database." See 'Account Aggregation: Consolidate, or be Consolidated?', *supra* n.646, and 'Citibank misses its deadline for online service', *supra* n.625.

[694] See 'Account Aggregation - Consumers' Questions Answered', *supra* n.650.

[695] See 'Account aggregation', <http://www.fsa.gov.uk/consumer/whats_new/updates/e_commerce/mn_aggregation.html>. and 'New online 'account aggregation' service will not be regulated, warns the FSA', <http://www.fsa.gov.uk/pubs/press/2001/057.html>. (print out on file with author).

[696] See 'Aggregation Is The New Buzzword - Aggregation Will Allow',

In the USA, the Office of the Comptroller of the Currency published guidance for the bank-provided aggregations although the non-bank provided aggregations are outside its scope unless they offer financial transactions under the provisions of the Gramm-Leach-Bliley Act. However it is a customer's decision to choose which service he/she would receive. In fact 33 % out of a thousand aggregation customers answered that they preferred to receive services from non-bank institutions, portals, such as Yahoo[697].

In Japan there is no statement published by the Financial Services Agency (JFSA) in relation to aggregation. However, the Japanese Bankers Association, a premier financial organization, stated that it, as an attorney of banking customers, approved of aggregation as a legitimate business [698]. It seems all industries and authorities involved in aggregation have studied what would happen in a different jurisdiction prior to taking a next step.

Another potential problem is the territorial issue. Because of its nature, aggregation will be easily extended to transnational or international accounts. There is no doubt that not only all issues heretofore mentioned but also unexpected brand-new issues will be raised[699].

5.2 A Dilemma: Legal issues

It is worthwhile examining the legal issues more closely, comparing Japanese and British legislation from the viewpoint of a party (=a data provider) who is involved in aggregation without giving its own consent. That is to say that two issues would be discussed: whether aggregation would be identified as having unauthorized access to a computer, and if so, what type of remedies a data provider could receive and what could be a penalty on an aggregator.

It is important to attempt to extend the observation from different angles. First of all, a matter of consequence is in view of an action — in other words, whether a business act executed under the name of aggregation could be illegal or not. The focus would be on "unauthorized computer access" rather than "hacking". This is because unauthorized computer access is the first offence, which precedes hacking. The relevant legislation would be criminal law and relevant special law on a specific crime. Secondly, it is vital to place importance on information. The legislation involved in this focus is law relating to data protection or

---

<http://globalarchive.ft.com/globalarchive/articles.html?id=010713016979&query=account+aggregation> (print out on file with author) and 'Account aggregation', *ibid.*

[697] See 'Lack of Regulation Increases Insecurities', *supra* n.664.

[698] See '*Kouza jyôhô syûyaku sâbisu* (aggregation services)', <http://www.fin-bt.co.jp/comment9.htm>, (print out on file with author).

[699] See 'Account Aggregation: Consolidate, or be Consolidated?', *supra* n.646.

privacy. Although other types of legislation might be infringed by aggregation, such as the Unfair Competition Prevention Law, it still remains to discuss the first two points, which are considerably important and cover most possible issues.

Getting right to the point, aggregation seems to be identified as unauthorized computer access in both Japan and the UK. In Japan the Unauthorized Computer Access Law (UCAL) came into effect on 13th February 2001. This prohibits unauthorized access itself. In addition to this fact, tangible damage needs to be proven to ask assistance of the existing law (as a result of a crime being committed), whereas the UCAL did not adopt that concept. Evidently aggregation is not the services to alter, damage or erase data when an aggregator gets access to a host website. The UCAL prohibits unauthorized access to a computer in Article 3 at first. It explains the details as the access to a computer using someone's identification code. "Identification code" means, in other words, a login name and password in this context. The details are defined in Article 2 and aggregation falls within one of three items explained:

> "(Clause 1 Article 2)
> A code the content of which the access administrator concerned is required not to make known to a third party wantonly[700]."

It describes in Article 3 that, as the access to a computer with the approval of an access administrator (=data provider) or an authorized user (=customer) is not identified as unauthorized computer access, it is necessary for an aggregator to get the approval from both parties. In fact, almost all banks are very likely to notify a customer in their terms and conditions, that the use of the services are restricted to a person who enters into a contract with a bank[701]. This is not only for online banking services but also ordinary banking services. So aggregation is illegal if the business is conducted without consent from all parties involved, mainly in case of applying for screen-scraping methodology. Then if aggregation is found guilty of being a business based on unauthorized computer access, an aggregator will be punished and sentenced with either a fine or penal servitude as criminal liability[702]. Then an aggregator will have a civil action brought against them. The possible civil liability to be imposed would be compensation and suspension of a business.

---

[700] In this context, "the access administrator" is the data provider and "a third party" is an aggregator. See 'Unauthorized Computer Access Law (Law No. 128 of 1999)', *supra* n.227.

[701] As an example, see 'Tokyo Mitsubishi Direct', <http://direct.btm.co.jp/kiyaku/index.htm>. (print out on file with author).

[702] The fine is limited to no more than 500,000 yen (equivalent to £2,941, £1 equivalent to approximately 170 yen) or imprisonment with labour (not exceed one year). See 'Unauthorized Computer Access Law (Law No. 128 of 1999)', *supra* n.227.

Incidentally neither the Criminal Law nor Unfair Competition Prevention Law of Japan is effective in dealing with aggregation. This is because of the rule that a crime with physical damage against a victim or victim's property is an absolute minimum[703]. In regard to the viewpoint of privacy and personal information, the Personal Information Bill has been shelved since 2001. It is said that it will require informing individuals (at least) when a business utilises their personal information[704]. Another applicable law is Copyright Law. The point is whether an aggregate of personal information is possible to be identified with a database. It defines "database" as:

> "(x*ter*) 'databases' means an aggregate of information such as articles, numericals or diagrams, which is systematically constructed so that such information can be searched for with the aid of a computer[705]."

It proves an aggregate of individual's information as a database, and thus, this database is recognised as independent works being protected under Copyright Law. The potential rights of a victim institution are the right of demanding cessation and compensation and measures for restoring of honour (Article 112 to 118). This possible criminal liability is either a fine or penal servitude (Article 119)[706].

In the UK, the "Computer Misuse Act 1990" (CMA) is in force. It penalises three particular offences;

- Unauthorized access to computer material;
- Unauthorized access with intent to commit or facilitate commission of further offences, and
- Unauthorized modification of computer material (Section 1 to 3)[707].

To be criminalized for an act under the said three offences, firstly, a subject intentionally gets access to a computer, secondly this access is done without any consent or permission, and finally this subject knows it is unauthorized access to a computer. It is clear that an aggregator, applying for screen-scraping methodology, has not been given consent from the data provider. In regard to an aggregator's intention, it is unnecessary to prove it. The possible criminal liability is imprisonment, fine or both on summary conviction[708]. Civil remedies would be given

---

[703] For details, see Chapter II.
[704] See *Mainichi Shimbun* dated 28th March 2001. It is also available in its website, 'New privacy law easy on media', <http://www12.mainichi.co.jp/news/mdn/search-news/846176/diet20data-0-2.html>. (print out on file with author).
[705] See 'Copyright Law of Japan', <http://www.cric.or.jp/cric_e/clj/cl1.html>. (print out on file with author).
[706] *Ibid*. The fine is limited to no more than three million yen (equivalent to 17,647 pounds sterling, one pound sterling equivalent to approximately 170 yen) or imprisonment with labour (not exceed three years).
[707] See 'Computer Misuse Act 1990 (c. 18)', *supra* n.255.
[708] *Ibid*. The fine is not more than level 5 on the standard scale or an imprisonment

separately after the offence is identified as computer misuse.

How could Data Protection Act 1998 (hereinafter "DPA") work upon aggregation? At first "data" is defined as information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68 (Section 1)[709].'

Furthermore, "personal data" is defined as information of a (living) individual, which makes possible to identify this subject:

" (a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller[710]."

To understand clearly, it must be noted that the target information being protected by the DPA in aggregation is personal information, such as name, address and so on. Within the said perimeters, the targeted information database of aggregation is able to be identified as "personal data", which must be protected by the DPA. Section 55 explains that;

" (1) A person must not knowingly or recklessly, without the consent of the data controller-
(a) obtain or disclose personal data or the information contained in personal data, or
(b) procure the disclosure to another person of the information contained in personal data. ...[Omissions]...
(4) A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).
(5) A person who offers to sell personal data is guilty of an offence if-
(a) he has obtained the data in contravention of subsection (1), or
(b) he subsequently obtains the data in contravention of that subsection.
(6) For the purposes of subsection (5), an advertisement indicating that personal data are or may be for sale is an offer to sell the data."

---

does not exceed six months.
[709] Section 68 defines the meaning of 'accessible record' such as a health or an educational record. See 'Data Protection Act 1998', <http://www.hmso.gov.uk/acts/acts1998/80029--a.htm>. (print out on file with author).
[710] *Ibid.*

Aggregation falls in subsection (1), and if an aggregator sells information to a third party as a result of providing aggregation, the aggregator would be found guilty under subsection (4) to (6). The possible criminal penalty is a fine[711].

The CRDR is another possibility to regard when considering the legitimacy of aggregation. This was enacted to amend the Copyright, Designs and Patents Act 1988 (CDPA). In the beginning, Copyright is a property right (Section 1 of CDPA). To consider what database is in this context, an initial compiler of the database is a data provider. An aggregator extracts information from a host website and complies with a different database. If a copyright of the initial database is infringed, the second database must be recognised as an unlawful product. The owner of the initial database has the first owner of database right as well as being protected under the CRDR whereas the second database is outside the legal protection. According to the CDPA supplemented by the CRDR, "literary work" includes a database (Section 3). It means "a collection of independent works, data or other materials which:

(a) are arranged in a systematic or methodical way, and
(b) are individually accessible by electronic or other means.[712] "

It also must be original. As a conclusion, the initial database made by a data provider is judged to be protected under the CRDR and CDPA. Hence for a data provider, the copyright owner, all remedies are open, for instance, compensations, injunctions and so on (Section 96 to 103 of CDPA). As for imposing criminal liability, an aggregator would be more likely to be sentenced a fine, imprisonment or both[713]. If it sells the database, the sentence would be a fine, imprisonment or both either on summary conviction, or on conviction on indictment (Section 107 of CDPA)[714].

6. The Future of Aggregation

It seems that all legislation, both in Japan and the UK are against aggregation. That is to say that it is criminalized under the special laws without exception. In spite of the facts shown, why has aggregation survived in the market? It is initially because of a party involved, in the strict sense of the word, a customer who discloses login names and

---

[711] *Ibid.* A fine on a summary conviction is not more than the statutory maximum.
[712] *Ibid.* See also 'Copyright, Design and Patents Act 1988 (c. 48)', <http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_2.htm>. (print out on file with author).
[713] *Ibid.* The fine is not more than level 5 on the standard scale or an imprisonment does not exceed six months.
[714] *Ibid.* A fine on a summary conviction is not more than the statutory maximum. An imprisonment on conviction on indictment does not exceed two years.

passwords to a potential defendant, an aggregator. Before accusing an aggregator of unauthorized computer access or infringement of copyright, it is a breach of contract that a customer discloses information which is supposed to be strictly confidential. However, customers probably had not been aware of any risk being contained in aggregation in the early stages. Moreover, an aggregator was unlikely to mention risks of the services to its customers. Data providers, on the other hand, hesitated to bring a suit against either of them, owing to watching for a business chance. As a conclusion, aggregation survives in the market holding disadvantages inside. That is why issues and problems are still tangible and aggregation does not quite make the grade. After two years since aggregation joined the market, SunTrust Banks Inc., who "pulled in" introducing aggregation, stated it was a wise decision[715].

After First Union's case, no party involved seems keen to take an action against aggregation. Although the FSA in the UK announced that it does not have authority to regulate aggregation business, it does not show any indication of criminalizing the business. The JFSA has not published any statement on it, either. Furthermore, when the Electronic Banking Group of Basel Committee mentioned aggregation in its white papers, it confined itself to stating "EBG will identify and promote the implementation of sound industry risk management practices for critical or emerging areas, such as technology outsourcing, security issues, and aggregation activities[716]." Regulators also have not shown any loathing against aggregation. The second promising reason is that they focus on the possibilities that aggregation would expand the e-banking market further and faster. Even if there is no wonder that aggregation is very likely to be judged as an offence, the aim of aggregation is positively and unmistakeably restricted within business and commercial. They would not try to regulate or ban the business unless its risks go higher than its market value or when parties involved in the business rush into regulators to petition. That is why aggregation exists in the grey area, and why aggregation cannot go further without being regulated since it holds high risks to run business.

If law or regulators do not affect very much for/against aggregation, what is necessary in the financial market to pursue a sound stable economy? If no one regulates the market, it is desperately necessary for data providers and customers to prepare measures to control the risks

---

[715] *The Financial Times* dated 5th March 2002. The article is also available on its website, 'Scraping Phobia Yields To Business-Case Merits', <http://globalarchive.ft.com/globalarchive/article.html?id=020305001872>. (print out on file with author).

[716] The FSA of Japan published a translation of Initiatives and White Papers, published by Electronic Banking Group, Basel Committee, which mentioned aggregation. For the whitepaper itself, see 'Basel Committee Publications - Electronic Banking Group Initiatives and White Papers - Nov 2000', <http://www.bis.org/publ/bcbs76.pdf#xml=http://search.atomz.com/search/pdfhelper.tk?sp-o=2.100000.0>. (print out on file with author).

attached to aggregation. The sole and effective solution is to establish self-regulation. In regard to aggregation, many parties are involved both inside and outside the financial market. Thus, building up the system of self-regulation of aggregation needs mutual cooperation amongst parties. One useful method is to introduce a standard or guidelines either domestic or international.

As the US firms have taken the lead on aggregation, the first achievement in researching this business was also marked in the USA. BITS, the Technology Group for the Financial Services Roundtable was launched in 2000. One of the working groups, called the BITS Aggregation Services Working Group, specialises in aggregation to take an initiative aiming at providing a framework referring to Regulation E (of the US Federal Reserve Board) and the Gramm-Leach-Bliley Act. Voluntary Guidelines were published in April 2001. It has launched a new phase to develop a secured model of aggregation[717].

The UK also demonstrated its own achievement. The Best Practice Aggregation Guidelines was published by the Association for Payment Clearing Services (APACS) in 2001 after the FSA announced its remit. It is, however, confined to some issues, such as the data collection, storage and so on. It aims to protect consumers and maintain confidence in both aggregation and e-banking and includes security issues as well as customer education. To list some crucial key factors, the principle APACS introduces is that aggregation should be based on the consent amongst the parties. It also strongly suggests meeting the BITS Security Guidelines. This impacts standardised security measures at least between the UK and USA. Unfortunately, the Best Practice Aggregation Guidelines are not obligatory for the parties involved in this business. Nonetheless it is said that parties would follow them to appeal to both existing and potential customers to emphasize their reliabilities on aggregation[718].

In terms of computer security, data integrity, confidentiality and availability must be ensured. These three key factors have been assigned in the Guidelines for the Security of Information Systems published by Organization for Economic Cooperation and Development (OECD)[719]. Technically it is prerequisite at the minimum for financial institutions to deliberate on encryption, secured communications and physical security;

---

[717] The Financial Services Roundtable is originated with the Association of Reserve City Bankers in the USA in 1912. See 'Account Aggregation: Consolidate, or be Consolidated?', *supra* n.646, 'The Financial Services Roundtable', <http://www.fsround.org/>, and 'BITS', <http://www.bitsinfo.org/aggregator.html>, (print out on file with author).

[718] See 'Aggregation guidelines receive cautious welcome', <http://www.onwindows.com/news/2001/December/241201.htm>, (print out on file with author).

[719] It described as "Security of information systems is the protection of availability, confidentiality and integrity." See 'Guidelines for the Security of Information Systems', <http://www1.oecd.org/dsti/sti/it/secur/prod/e_secur.htm#11>, (print out on file with author).

not only applying highly powerful encryption and security systems to detect and prevent unauthorized access but also enforcing a thoroughgoing check of identities to access both computer systems and its physical location. To support a series of security measures, it is necessary to publish a security policy and implement it in an institution practically[720]. It is also provident to prepare the computer security of a financial institution for international standards and/or guidelines published by international organisations or the competent authorities in respective countries. Will it be totally secured if a financial institution has implemented the best (presently) security system? It is open to debate.

Risks are always involved in financial institutions. Aggregation, however, should be a brand-new type of risk, which was born outside their business boundary. Therefore, financial institutions have been nonplussed to deal with it. It is a fact that aggregation has not chosen its direction, nor its value yet been clearly measured. In other words, it could be possible to say that aggregation has not had a real punch to wield influence over the market. If a new service of aggregation is developed, it may distinctly change the present situation. The potential new service would be to enable financial transactions on an aggregated screen. It is clearly useful if it is available amongst accounts although this service holds serious security and privacy issues to resolve. In one example, the Royal Bank of Canada has tied-up with CashEdge to develop aggregation with this value-added service[721].

A useful service for a customer does not always make a profit for a service provider, such as financial institutions. The aggregators believe it is profitable for them, whereas financial institutions do not immediately agree on this although they do not deny a possibility of aggregation being a subsidiary to attract their customers. It is hard to say that aggregation has fully considered its risks in early stages, or that its problems and issues have been yet resolved. It is necessary for financial institutions to examine carefully not only aggregation itself but also the market's trend and customers' interests to make a judgement on expanding the business. There are some means available to control risks. The important thing is to ascertain whether a certain risk is worth to take and if so which is the best option to control it. Aggregation will never be incriminated; but it depends on the decision financial institutions make whether aggregation will be able to survive or not.

---

[720] Possible solutions are introducing 128-bit SSL (Secure Socket Layer) for communications between customers and a server, 3DES for database in a server and itself to be encrypted. Building up firewalls and intrusion detection system are also crucial. See '*Kinyû-shin-sâbisu: akaunto agurigêsyon no dôkô* (A new financial service: The trend of the account aggregation services)', *supra* n.621.

[721] *Ibid.*