Cyber Security Information Sharing in the United States: An Empirical Study Including Risk Management and Control Implications 2000-2003

Volume One of Two

by

Michael Keith Lavine

March 2007

In Partial Fulfillment for Doctor of Philosophy Degree from Sir John Cass Business School, City University, London, UK

Table of Contents

List of Tables

List of Figures

Abstract

A tremendous amount of change in traditional business paradigms has occurred over the past decade through the development of Electronic Commerce and advancements in the field of Information Technology. As lesser-developed countries progress and become more prosperous, traditional 'first world' countries have migrated to become strong service oriented economies (Asch, 2001). Supporting technologies have developed over the past decade which has exploited the benefits of the Internet and other information technologies. While Electronic Commerce continues to grow there is a corresponding impact on computer software and individual privacy (Ghosh and Swaminatha, 2001). Recently, the U.S. National Institute of Standards and Technology (NIST) found that software bugs cost the U.S. economy approximately $59.5 billion, or .60% of the annual Gross Domestic Product (U.S. Department of Commerce, 2003). In addition, we have witnessed a rise in the strength and impact of Denial of Service and other types of computer attacks such as: viruses, trojans, exploit scripts and probes/scans. Popular industry surveys such as the annual Federal Bureau of Investigation/Computer Security Institute (Gordon, Et. Al., 2006) confirm the growing threats in the Information Assurance field. In addition to these concerns our increased reliance on the Internet enabled systems (Loudon and Loudon, 2000), E-Commerce systems and Information Technologies an integrated suite of risks which must be managed effectively across the public and private sectors (Backhouse, Et. Al, 2005, Ghosh and Swamintha, 2001, Parker, 2001, Graf, 1995, Greenberg and Goldman, 1995).

Previous research (Rumizen, 1998, Haver, 1998, Roulier, 1998) examined Inter-Organisational, Web Information Systems and Government Information Systems in order to assess how companies and other organisations can effectively design these information systems such that maximum benefits can be achieved for all participating organisations. Furthermore, Davenport, Harris and DeLong (2001) and Davenport (1999) explained that collaboration is central to the results of a knowledge management system in which open, non-political, non-competitive entities are involved in environments to achieve optimal individual and collective results. Before this memorable event, some related programmatic initiatives were already in-process at that time. The United States government built upon its active leadership in the areas of computer security and information assurance when it launched a number of important efforts to manage information security threats. This was clearly evident when President Clinton made the U.S. National Infrastructure (NII) a major national priority in the 1990s. One critical development occurred in 1998 when the National Infrastructure Protection Centre was established to be the central point for gathering, analysing and disseminating critical cyber security information and built upon the previous success of the national Computer Emergency Response Team (CERT).

Earlier research (Rich, 2001, Soo Hoo, 2000, Howard, 1997 and Landwher, 1994) addressed various aspects of information security information and incident reporting. Also, Vatis (2001) addressed some research considerations in this area while investigating foreign network centric and traditional warfare events primarily through Denial of Service and Web Site Defacement attacks. However, areas for new exploration existed especially as they related to U.S. critical infrastructure protection (Karestand, 2003, Vatis, 2001, U.S. General Accounting Office, 2000, Alexander and Swetham, 1999). Finally, Information and Network Centric Warfare (Arens and Rosenbloom, 2003, Davies, 2000, Denning and Baugh, 2000, and Schwartau, 1997) are increasing national security issues in the War on Terrorism and Homeland Security in general.

Acknowledgements

Undertaking a Ph.D. is a major career opportunity which is filled with many inherent constraints and practical challenges. My efforts to pursue this research degree began nearly seven years ago when I completed a second MSc. degree at Johns Hopkins University. Perhaps, more accurately the beginnings of this effort actually began in 1994 when I had the opportunity to study for a MSc. in Internal Auditing and Management at City University Business School (former name of Cass Business School). I have always found the learning environment at Cass Business School to be exactly what I was (and have remained) interested in.

Quite simply, this degree would not have been possible without the help of a number of important people. All of my family members have always supported my educational efforts; even when it has meant considerable time away from home and additional time spent in the office and library. I am immensely grateful for the love, support, patience and understanding they have given me throughout my life.

My supervisor, Professor Georges Selim, has been an incredible source of inspiration to me since the first time we meet over twelve years ago. Serving as an advisor for part-time research students must be a very challenging and often frustrating position. At every single stage, he has patiently guided me over six years of study, constructively evaluated my work, and supportively nurtured my academic and professional development. Much like a father who guides his son through life, Georges has always stayed with me. He has been a truly wonderful advisor and role model, as well as a superb mentor and very close friend. I wish him, Sally, Emma and Claire the very best that life has to offer.

In addition, Dr. Rob Melville, Senior Lecturer of Management has always been a wonderful teacher, colleague and good friend. He has also been very supportive and encouraging of my diverse teaching and research interests. I am very grateful for your friendship and advice over the many years.

Also, I am also indebted to Mr. Vince Rowe, Former Editor of the CyberNotes newsletters and currently at the Federal Bureau of Investigation National Headquarters for his help in providing me with the data for this project. Since my original request in 2002, he has always been willing to assist me, listen to my suggestions and review my results.

In addition, Dr. Bradley Trinkle, Assistant Professor of Accounting at the College of Charleston has taught me a number of important lessons about research design and statistical methods. He has been a true colleague and friend.

Finally, to all of those that I have not been able to mention by name; I thank you and hope that I have also made you proud.

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 acknowledgements.

Chapter One - The Introduction

1.1 An Introduction

Businesses and other organisations have long sought to use Information Technology (IT) to gain competitive advantage. The present E-Business business environment is entrenched in a model of continual exploitation of IT (Rayport and Jaworski, 2001; Loudon and Loudon, 2000). There is a vast array of available technologies that allow businesses to automate previously manually intensive business processes, help gain advantage over competitors and otherwise expand their activities in the competitive global marketplace. Furthermore, with the explosive growth of the Internet and the E-Business paradigm place society in a time of tremendous change with a variety of complex set of IT risks and an increasing reliance on IT to support and advance our business and personal lives (Backhouse, Et. Al, 2005, Dutton and Shepherd, 2004, Jackson, Allum and Gaskell, 2004, Riggins and Rhee, 1998).

Since the beginning of modern society people have been involved in the buying and selling products and services using mediums of exchange (i.e. U.S. Dollars, Euros and British Pounds). Traditionally, this has been conducted on a face-to-face or in person. Yet today's technologies have changed the ways in which we are able to conduct business. From a purely utopian point of view, IT should enable business organisations and individuals to operate more efficiently and effectively. However, with the growing use of emerging technologies; companies are simultaneous faced with the need to maintain control over these technologies.

Controlling technologies is often done through the use of other technologies that are often newer. However, this may not be optimal since the organisation balances the need for IT Security with the ease of use for end-users (Backhouse Et Al., 2005, Schou and Trimmer, 2004, Pfleeger and Pfleeger, 2002 and Schneier, 2000).

The first approach to IT Security grew out of the centralised, mainframe computing platform and military security principles. Limiting physical access was emphasised in large data processing centres. By controlling physical access through such rudimentary measures as locked doors, employee identification cards and security personnel, organisations grew confident that all valuable computing resources were adequately safeguarded. Not withstanding the fact that individual user privileges were limited on a 'need to know' basis.

In other words, computer system rights were given only for what was determined necessary for the accomplishment of an individual's job tasks and responsibilities.

In the early mainframe environment of the 1970s through to the mid-1980s, the number of computer users relative to the organisation's entire workforce was relatively small. We could also classify computer users of this era into two distinct groups: highly technical computer services personnel and task-oriented employees that primarily performed data entry and retrieval tasks on 'dumb terminals'. In the next generation of computing, companies tried to leverage their investments in computer systems by moving to client server architecture. In the 1990s, these changes required creative and dynamic new approaches to IT and general business risk management.

Distributed computing and client/server architectures have put computers and related technology into the hands of exponentially more people than existed in the mainframe environment. Local Area Networks (LANs), Wide Area Networks (WANs), Virtual Private Networks (VPNs). Furthermore, the persuasiveness of the Internet drastically increased the use of IT in the everyday lives of a large portion of the population in many countries around the world. Some researchers have referred to today's society as being network centric (Jones, 2001, Ghosh, 2001, Cantwell and Santangelo, 1999). This concept is based on the fact that the Internet and its corresponding security requirements have become a central part of our personal and business lives. From this premise it is important to discuss the main aspects of security with the context of information technology as a whole.

Information technology security has four primary objectives. These principles guide the development and application of IT Security. Specifically, these are:

> ***Confidentiality*** – ensuring that only authorised individuals have access to the information they require in order to successfully complete their job responsibilities. Often, this is also commonly referred to as privacy, it relates to the military concepts of 'need to know' and 'least privilege'.
>
> ***Availability*** – requiring that information be available when it is required to be so to the user(s).
>
> ***Integrity*** – determining that data is accurate, complete, valid and unadulterated.

Non-Repudiation – validating that the user is who they claim to be. In essence, authenticating the user based on pre-determined criteria.

(Adapted from Bosworth and Jacobson, 2002)

Networking technology has continues to have a steady increase in functionality (e.g. features, usability, availability and performance) together with a simultaneous decline in unit costs. Today's IT products are faster and more powerful than ever while also being less costly. Currently, we are expanding into a new era of wireless technology; which is a good example of how next generation technologies can change our lives. A fundamental concept in the field of IT which address the rate of advancement is known as Moore's Law named after one of the founders of the Intel Corporation. This concept was originally based on microprocessors and the accelerated rates of advancement and simultaneous decreasing costs (Loudon and Loudon, 2000). Today, this principle has been accepted as being applicable to most of IT as a whole.

While federal government agencies were some of the largest users of mainframe systems there was no significant active role of national governments in protecting their respective citizenry. Some early U.S. initiatives were directly related to the Morris Worm incident in 1988 (Rochlis and Eichen, 1989). Now, in the post–911 world, we have seen many new government efforts to combat terrorism and improve the collaborative efforts between the public and private sectors. This position had some rationale given the fact that other than tampering with confidential data the average citizen did not perceive a large impact of how the government was protecting them from IT related risks. The mainframe era was also the time of communism, the Cold War and potential nuclear conflicts. All of which can be considered as primarily as physical threats from known adversaries. Therefore, governments were largely *lassie-faire* in terms of how involved they were with regard to external IT security issues. On the one hand, it was commercial enterprises and industry groups that were left with the responsibility of addressing and handling internal, but not external IT security threats.

From a corporate perspective, those companies that maximise the effective use of technology can create true competitive advantage. This general business principle compels companies to seek to maximum exploitation of technology by increasing operational performance, combating global competitors and meeting shareholder expectations (e.g. profits, dividends, performance).

IT is not completely unique in terms of the need for risk management practices. Other functional areas require such initiatives due to the inherent risks involved in business processes and outside threats that can cause the enterprise to be vulnerable in various ways. Damage can often be measured in terms of financial losses, personnel hours, consulting fees, and the lack of continuity of operations (Ayets, 2004, Weber, 2000 and Gollman, 1999). There is also an additional group of risks that must be identified and managed for organisations to ultimately be successful in meeting their objectives. An enterprise cannot expect to completely eliminate all risks given their practical cost and resource constraints. Rather they can take a variety of risk management approaches (Parker, 2001 and McNamee and Selim, 1998).

The current E-Business environment in the United States has millions of host and client computers connected to the Internet all the time (United States Critical Infrastructure Assurance Office, 1999). New dependencies between the public and private sectors have developed with various political, military, legal and economic perspectives (Brinson, Et. Al, 2001, Olson, 2001, Vatis, 2001, Palmer, 2000, United States Presidential Decision Directive No. 63, 1998). While important and necessary, safe commerce and the protection our physical and economic welfare is an increasingly important issue in the Information Age. Enemies can take various forms such as non-state and state actors (Kiefer, 2001, Davies, 2000, Fischer-Hubner, 2000, Rathnell, 2000, Furnell and Warren, 1999, Kovacich, 1999). Furthermore, it is sometimes unclear exactly who the enemies are and where they physically are located. This is due to the use of advanced Internet technologies such as proxy servers and anonymisers; all of which have security functions but also serve as tools for enemy combatants. To further complicate this situation, government authorities may have no jurisdiction in the nation state where the attacker physically resides due to a lack of legal treaties and political factors. Therefore, in its totality there are many inherent challenges and externally imposed problems in the field of IT Security.

1.2 Need for the Study

The need for this research study is based on a number of critical observations about the disciplines of: IT Security, Risk Management. National/Homeland Security and Electronic Commerce. This study builds on a grounded theory research approach and incorporates a detailed literature review from various disciplines. It is also based on the fact that traditional risk management practices including auditing and information sharing are necessary to counteract the various costs of IT Security. For instance. the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce. calculated in 2002 that software bugs costs the U.S. economy about $59.5 billion annually. or 0.60 percent of the American Gross Domestic Product (U.S. Department of Commerce. 2003)

Justification can also be highlighted by the fact that one of the natural by-products of this study will be its direct application to the field of IT Security. This is in terms of advancing the current knowledgebase and applying its results in terms of meaningful recommendations to the profession and society as a whole.

First and foremost, IT is a growing part of our business and personal lives. Technological innovation is an evolutionary process. Personally. the researcher also finds IT to be interesting, intriguing and powerful. while simultaneously challenging, confusing and risky. Secondly, there are inherent challenges to the field of IT Security. Specifically. the researcher chose to examine these particular challenges in the context of today's Internet economy.

Some of these obstacles include: technology itself. primitive legal frameworks, and resource constraints. By no means are these minor issues to address. In fact. even in the early years (e.g. prior to 2000) of programmatic development the United States alone has spent roughly two billion U.S. Dollars per year to combat the threats to IT security related to the country's critical information systems infrastructure (U.S. General Accounting Office. 2000).

There is a new mode of cooperation between the government and private sectors in IT Security. This includes partnerships between different independent organisations with competing objectives. Specifically. national government organisations (e.g. funded with taxpayer finances) have historically focused on enforcement of laws and regulations versus business organisations that strive for profit realisation, stock price appreciation and customer perfect service. Inherently, there should be conflict between these two discrete groups with competing individual objectives. Simultaneously, the field of IT Security must have information sharing mechanisms between the public and private sectors.

Nevertheless, our future as human beings will be impacted by the ways in which we can adequately protect ourselves, and the information technologies that support us. In order to support the need for a Ph.D. dissertation, a number of important considerations need to be justified. To help prove that this project will make a contribution to the literature and knowledge, it will be useful to identify the limitations and gaps perceived from other studies. This is summarised in the following table, as follows:

Table 1.1 – Perceived Limitations and Gaps in Previous Studies

Researcher	Date	Description	Limitation(s) and/or Gap(s)
Computer Security Institute/Federal Bureau of Investigation	2000-2006	Annual practitioner based survey on covering information security trend analysis and impacts.	Annual anonymous survey that included estimated financial impacts of threats and vulnerabilities. Security technologies used in industry and government identified and forecast growth.
Vatis	2001	Case study analysis of non-U.S. regional military conflicts.	Emphasis was on non-U.S. countries involved in regional military conflicts. No analysis of national information infrastructure.
U.S. General Accounting Office	2001	Follow-up audit (to 2000 audit; listed below).	Re-emphasised the need for additional resources and congressional support of this organisation.
U.S. General Accounting Office	2000	Initial large scale review of NIPC activities.	Operational audit of government entity. Focused on availability of resources and overall effectiveness of organisation. Identified critical success factors of the organisation and related gap analysis.
Howard	1997	Ph.D. research involving the main activities of CERT.	Solely focused on the work of CERT and information security trends related to Internet growth.

Ultimately, the researcher has incorporated some of the suggestions for future research into a few of the study hypotheses from prior work by Howard (1997).

Further support for demonstrating the need for the study can be shown by explaining the benefits that this project will yield. These have been divided into five rational categories: general benefits, specific benefits to the NIPC organisation, benefits to the profession practice of IS security, personal benefits to the researcher and other benefits. Each of these areas is discussed separately below.

1.2.1 General Benefits

The need for this research study is based on a number of personal, theoretical and technological observations. These items cover the areas of IT Security, E-Commerce and National Security. Justification can also be highlighted by the fact that one of the natural by-products of this study will be its direct application to the field of IT Security; in terms of advancing the current knowledge base and applying the expected significant results of this study to government agencies, the IS profession, the research community and society as a whole.

1.2.2 Specific Benefits to the NIPC

The researcher is optimistic that the project will assist the National Infrastructure Protection Centre in carrying out its responsibilities. Technology is particularly evolutionary and dynamic. Therefore, it is important for the NIPC to be able to: 1) obtain and analyse security information quickly, 2) share information quickly and efficiently and 3) address the general and specific information needs of various stakeholder groups; all in a user-friendly format. This organisation faced formidable obstacles including: technology itself, primitive legal frameworks, and resource constraints (Alexander and Sweetnam, 1999 and U.S. General Accounting Office, 2000 and 1998).

The United States is investing billions of dollars, to combat IT security threats related to the country's critical infrastructure. Limited government resources must be used efficiently minimising the risk of duplication and waste. It is hoped that through this project, the overall effectiveness of the organisation will be improved, even in a small way.

1.2.3 Benefits to the Information Security Profession

There is an emerging mode of operation that includes partnerships between different independent organisations. This includes sharing of information about information security vulnerabilities and exploits between the public and private sector. More specifically, national government organisations are supported by taxpayer finances, and historically focus on the enforcement of laws and regulations. Whereas private business organisations strive for profit realisation, stock price appreciation and customer perfect service. Furthermore, the Internet and electronic commerce have created a new inter-dependence between these two sectors (Vatis, 2001, Ciborra and Hanseth, 2000, Ellison, 1999, U.S. General Accounting Office, 1998). This is discussed in more detail in Chapter Two: Literature Review.

1.2.4 Personal Benefits to the Researcher

Firstly, the researcher has a number of personal reasons to further justify the pursuit of this study. Strauss and Corbin (1998) identify this as an important component of research activities. A personal interest in this area has developed over more than twelve years of professional practice as an information technology and internal auditor.

During this time, a keen interest in information sharing with regard to information security vulnerabilities developed. When a transition to full-time academic employment commenced in 1999, the desire to make a contribution to the research arena began to synthesise. Through this synthesis, the interest, curiosity and intrigue began to gain momentum. In 2001, during the unprecedented terrorist activities against the United States further motivation developed since there is a strong possibility that this research will directly help the NIPC and its successor organisations in accomplishing its strategic objectives (General Accounting Office, 2001 and 2000).

1.2.5 Other Benefits

This study also has other possible benefits. In today's Information Age. some of these protective measures include technologies that support our safety and security on a national and regional level. From a moral perspective, our future as human beings will be impacted by the ways in which we can adequately protect ourselves. In the twenty-first century. computer security and information assurance are critical aspects of our modern society.

1.3 Objectives of the Study

In this project, the researcher developed a set of research hypotheses in the context of a major U.S. government sponsored IT Security organisation. Particular emphasis is placed on gathering empirical data provided by the FBI. Furthermore, it is necessary to go beyond the limitations of prior research studies, and make a unique contribution to the IT Security knowledgebase and literature.

Critical to the accomplishment of this goal is designing a sufficient scope for this research study. At the foundation of this project is an analysis of how different groups (i.e. federal governments, private enterprises, professional organisations and individuals) seek to promote IT security. In particular, focused research is made of leading initiatives in this regard, as well as, what technologies are being used as countermeasures to IT security threats. As such, four specific objectives were developed.

The first objective is to investigate whether there is a correlation between general cyber security information and what is determined to be critical by the NIPC. To probe this question, this was organised using two categories of CyberNotes data (e.g. Bugs and Viruses) and related information from government and non-government sources.

The second objective is to examine changes in Internet growth and the reporting by the NIPC. The premise behind this aspect of the research was that the Internet is continuing to become an attractive target for hackers, criminals and terrorists as more individuals connected to the Information Superhighway and the E-Commerce business paradigm expands. The study variables related to: software bugs, viruses, Exploit Scripts, Trojans and Probes/Scans were utilised.

The third objective is to study a variety of macro-economic factors and see if these variables are associated with the five variables of critical cyber security information reported by the NIPC. A range of publicly available stock market indices are used, as are the government's reporting of CPI, GDP, Inflation and Unemployment figures.

The fourth objective is to explore the potential associations between military and political events with the NIPC's CyberNotes reporting using an event window methodology which is a common research design in finance, advertising, public policy and communications. Using the advice of other academics in these fields; five military events and four political events were analysed. Specifically, the military events are: 1) the attack on the USS Cole Battleship, 2) the War in Afghanistan, 3) September 11th Terrorist Attacks, 4) U.S. Invasion of Iraq, and 5) U.S. Military Intervention in Liberia. The political events are the: U.S. Presidential Election, Western States energy crisis, severe winter weather storms, and Northeast Blackout.

In addition to these results, another benefit of this project is that additional ideas for further research emerged. It is my passionate desire to develop new, original discoveries. The researcher was able to pursue a legitimate and significant need for this particular research study.

1.4 Limitations of the Study

There are a number of crucial limitations to this research study that must be acknowledged. It is important to note that these individual limitations are not presented in order of direct significance to the research study itself, but rather are shown in the aggregate to ensure a proper understanding of the various constraints encountered.

Firstly, the amount of financial resources that can be expended is limitation to the study. This research was not funded by any grants, scholarships or other support. Therefore, the researcher had to rely solely on personal financial resources. Over the course of my Ph.D. studies at City University, I estimate that the total direct costs amounted to 50,000 Pounds Sterling inclusive of registration fees and course materials.

Secondly, technology itself is also a limitation to this study. This study is not based on basic or scientific research, or a testing methodology that analyses individual technologies or vendor specific products. Excluding this type of testing is important since the researcher could not test the effectiveness of any of the thousands of IT Security products. While this type of applied, hands-on research is very interesting: it is not in keeping with the research methodology employed.

Thirdly, the emerging nature of IT Security/Information Assurance is a partial limitation on this study. The primary reason for this is that new information systems emerge on a steady, regular basis. As such, the researcher did not believe that this study can predict what types of new technologies will emerge from academia and industry. Accordingly, as new generations of existing technologies are made available, there will surely be new product enhancements; some of which will include security features and mechanisms. These will likely be the result of: continual product development, software engineering, regulatory, industry and legal advances.

Fourthly, the amount of time dedicated to this research project was limited by professional and personal commitments such as university teaching, consultancy and family responsibilities. As a Ph.D. student, I was very fortunate to pursue my research project on a part-time basis while first working at Towson University as a Senior Lecturer in Accounting and later as a faculty member at the Johns Hopkins University Information Security Institute. This was in addition to leading some consultancy projects, originally for the Operational and Systems Risk Management (OSRM) practice of PricewaterhouseCoopers, LLP. Without a doubt, a Ph.D. degree is a very serious professional and personal undertaking. The associated opportunity costs are numerous and difficult to calculate in definitive financial terms.

Clearly, all of the limitations described above are considered noteworthy. Yet, after assessing the aggregate impact of these limitations together with the scope of this research project there is adequate and sufficient basis for a thorough examination of the research questions described in the following section of this chapter.

1.5 Structure of the Study

In accordance with University guidelines, the structure of the study is organised in the traditional format of a research based, Ph.D. dissertation project. There are six distinct chapters in this study, and each chapter itself represents a main component of the project.

Chapter One is the introductory chapter and serves as the initial overview of the entire research study. A general introduction to the research project and related sub-topics is provided along with an analysis of the overall scope of the project. Additionally, the need for the research project is examined in detail in order to demonstrate the justification for pursuing such a project at the Ph.D. level. Also, a variety of limitations of the research project are delineated, so that the research project can be portrayed in the proper context subject to the constraints involved. This chapter is concluded with a brief summary section.

Chapter Two focuses on a review of the related research literature. This process involved an extensive literature review and an examination of prior research studies, government publications and public policy initiatives in the diverse fields that directly and indirectly impact the scope of this project. Particular attention in this analysis is paid to analysing prior journal articles, conference papers, books, and post-graduate research projects. This was done intentionally to provide a broad basis for framing this project. During this stage, the researcher was also able in order to identify some key recommendations for further research which were suggested by other researchers. In its totality, the literature review provided an excellent background and overview to build the research model used in the next section of project using a strong academic research methodology.

Chapter Three addresses the project's research methodology as a complete analysis. This includes information about how the research model was designed and executed. Beginning with a discussion of the advantages and disadvantages of various overall research approaches. Then, the chapter continues with an analysis of various research methodologies used in the field of Social Science research in general; and more specifically in the fields of Internal Auditing, Management and Information Systems. Various aspects of quantitative and qualitative research are presented. Next, all research questions are presented together with their associated research hypotheses; all of which were approved by the project advisor before proceeding to Chapter Four. In all, the overall objective of this segment of the study is to provide sufficient analysis of the research techniques employed and utilised.

Chapter Four includes a descriptive analysis of the various data sets which were collected and analysed. This chapter begins with a brief presentation describing the data accumulation, collection and analysis techniques employed during the project. Of special importance and focus are the five main data categories of the CyberNotes newsletters: 1) Bugs, Holes and Patches, 2) Viruses, 3) Exploit Scripts, 4) Trojans, and 5) Trends. It details a variety of high-level presentations related to frequency distributions, data aggregation summaries and other analyses. Also, a variety of secondary data sets are presented. For the secondary data, a limited presentation of the frequencies and trends is also included. Various descriptive statistical summaries are presented throughout this chapter with a primary focus on frequency and trend analyses. All of which is prepared according to the five major research questions of the project.

Next, Chapter Five presents a detailed testing sequence for each of the research hypotheses presented earlier in Chapter Three. This part of the study is focussed on proving these hypotheses which is done by explaining the specific detailed tests using correlation techniques and other statistical methods that were performed as well as the limitations and generalisations observed during the study. Also included in this chapter is a discussion of the research results and answers to the research hypotheses are explained.

Finally, Chapter Six provides a summary and conclusion on the research project. It also presents six specific recommendations for future research. The last section of this chapter contains some final thoughts on the research project as a whole.

1.6 Final Thoughts on Chapter One

The ever changing nature of computer and IT security threats pose many challenges to both industry and government organisations. Software bugs, computer viruses, Trojans, exploit scripts and network probes force government and non-government organisations alike to identify, manage and share information about protection and mitigation strategies. Essential to the effectiveness of this process is the overall cooperation and sharing of information amongst these diverse constituencies (Tope, 2005, Lavine, 2004 and Tribodeau, 2000).

Today, hackers, criminals, terrorists and industrial espionage agents use a variety of cyber attacks to perpetuate their deeds. These groups put critical infrastructures across and within countries and individual companies in various sectors at great risk. Denning (2003) and Schwartu (2002) present views about cyber terrorism and information warfare which have been shared through various landmark commissions and Presidential Executive Orders in the United States. However, there remains a vast amount of work to do in order to prevent, detect and recover from such events. The National Infrastructure Protection Centre was one of the most important U.S. government agencies in charge of this very challenging task.

This project continues with Chapter Two which focuses on an extensive examination of the literature. The work in this area forms the theoretical basis for the project's research questions and study hypotheses.

Chapter Two - Literature Review

2.1 General Introduction

Today is a very exciting time in the field of information technology and business. New technologies continue to emerge and more organisations are entering the domain of electronic commerce. With this excitement comes caution and concern about the various risks that individuals, companies and government organisations face. These risks come in different forms – predominantly human and technical. Hackers, cyber terrorists, social action groups and rogue nations are all realistic threats to our country (Taylor, 2004, Tippett, 2002, Alexander and Swetnam, 1999). Software flaws, computer viruses, worms and denial of service attacks can cost over seven billion dollars per incident (Ohlson, 2000). Early growth forecasts indicated that the United States would nearly double its Internet usage of 1994 by the year 2004 (OECD, 2000). In addition, the fact that our society is increasing our dependence on information systems more as time goes on. Therefore, each citizen should be concerned enough to understand what the government and private industry are doing to protect the well-being of society.

This section begins with a presentation of changing economic paradigms. It is from this base that a story unfolds about the major information technology advancements of the twentieth century. Individual technologies are discussed only as they particularly related to the fields of information systems security and electronic commerce. Particular emphasis has been placed on information sharing and dissemination through inter-organisational, web and government information systems. The U.S. government initiatives in these areas are highlighted. Also, a discussion of the opportunities and risks, controls and threats, and secondary issues related to computer security are presented. Throughout this chapter a wide variety of previous research studies are used to illustrate the key theoretical underpinnings of this project. In the end, a wide and thorough foundation is presented and discussed as a foundation for the research study.

2.1.1 Changing Economic Paradigms

A tremendous amount of change in the traditional, geographic business paradigm has been occurring over the past two decades. The modern world has made huge technological advances in the way trade is conducted across the globe. For centuries, the economies of the western world were based almost entirely on land and other natural resources; this formed what economists considered a predominantly agrarian society.

Over hundreds of years, through the Industrial Revolution society slowly moved to a manufacturing environment. Major city centres developed around factories that produced consumer and commercial products that enabled large-scale growth in the general economic strength of 'first world' countries. This situation continued until the middle part of the twentieth century, and remains in a state of continuous change.

As lesser-developed countries progress and become more prosperous, traditional first world countries are migrating to become strong service oriented economies (Asch, 2001). Currently, this situation is causing a dramatic shift in the way young professionals pursue education and employment opportunities. Furthermore, today's economy is faced with rapid advances in science and technology that exponentially affect our business and personal lives. The most dramatic technological innovation that our generation has been fortunate to witness is the Internet.

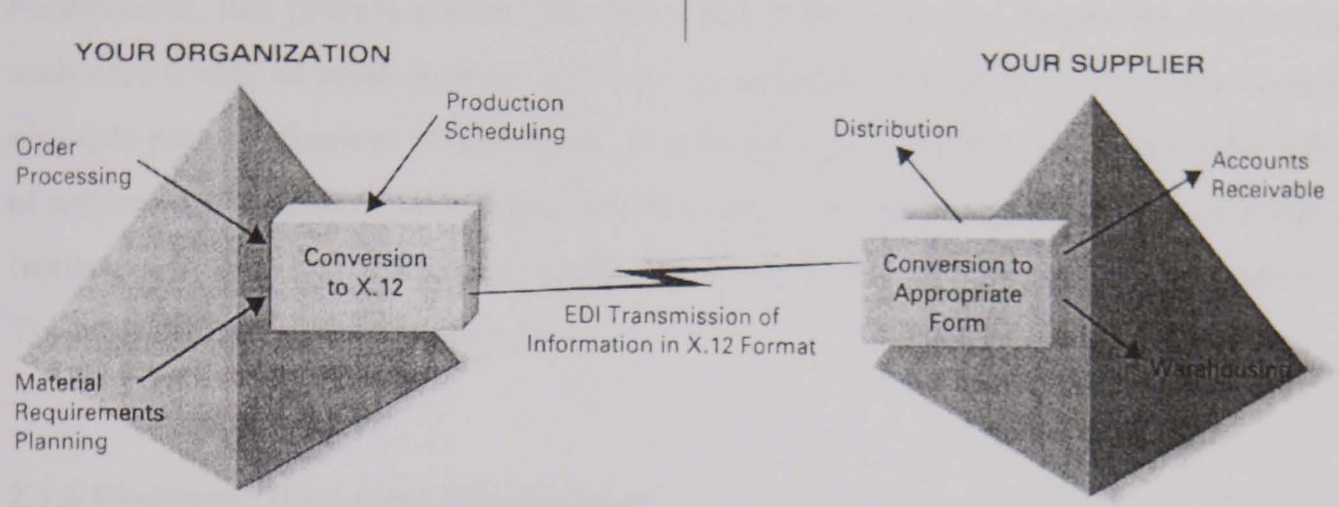
2.1.2 Electronic Mail

The first and most primitive method of Electronic Commerce is electronic mail (commonly referred to as e-mail). This technology provides a very simple and lost cost method of communication (Rayport and Jaworski, 2001). It is a highly effective method for a purchaser to communicate order information to their suppliers. For instance, this can be done over a basic dial-up account to the supplier's electronic post office or via an Internet supported e-mail account with an Internet Service Provider (ISP). While this is fundamentally a sound way of communication it is definitely the most elementary. A subsequent technology to EDI and Electronic Mail is Electronic Data Management.

2.1.3 Electronic Data Interchange

The second method of EC is Electronic Data Interchange (EDI). American Hospital Supply Corporation first implemented this technology in the late-1970s, as a method of allowing large hospitals to order medical supplies and pharmaceuticals over a dedicated computer line. In its time, this was considered a major advancement for the healthcare industry. This information system allowed healthcare providers to increase the overall management of inventory control; which today has allowed many organisations to implement Just-In-Time (JIT) systems. This is described in more detail in the following figure:

Figure 2.1 – Overview of Electronic Data Interchange



Source: Loudon and Loudon, 2000

A specific application of EDI is Electronic Funds Transfer (EFT). For illustrative purposes, assume that Customer 1 at Bank A can transfer money to Customer 2's account at Bank B. This technology allows buyers and sellers in one country or in different countries the ability to promptly negotiate many common business transactions such as the payment of common vendor invoices and installment commercial loans. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is an association of financial institutions and commercial bank networks that provide the technology infrastructure and network management tools for most banks offering EFT services. Today, most industry observers consider EDI to be a mature technology.

EDI services have expanded and diversified over the past twenty years. Today, this technology incorporates the following key operating characteristics:

- Direct application-to-application interchange,
- Well-defined, tightly specified message formats,
- Batch orientated, asynchronous operation,
- Interactions based on pre-existing contractual relationships between the business partners,
- Primary use is between trading partners in a specific industry, for example manufacturing or healthcare, and

- Frequently a required initiative of one of the trading partners (e.g. the buyer) to achieve operational improvements.

Source: Adapted from Marcella, A.J. Jr., Stone, L. and Sampias, W.J., 1998

Furthermore, this process enables the buyer and seller to realise significant cost savings in such core overhead areas such as; purchasing, materials management, inventory control and accounts payable/finance. Additionally, this technology is further enhanced by the influence of national and international standard setting bodies such as the American National Standards Institute (ANSI) and Electronic Data Interchange, For Administration, Commerce and Transport (EDIFACT), respectively.

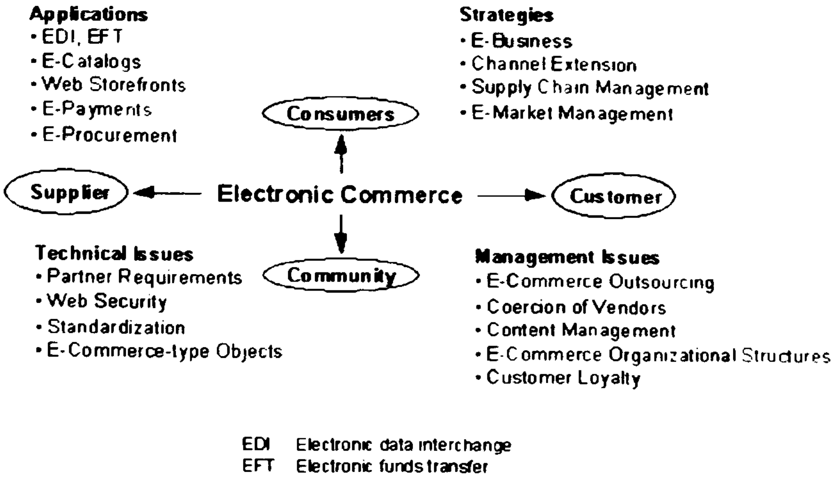
2.1.4 Electronic Document Management

Electronic Document Management (EDM) is a natural outgrowth of the traditional electronic data interchange model. This medium facilitates the electronic transfer of data normally included on paper-based documents such as payroll timesheets, purchase orders and vendor invoices. Cost reductions and time- savings on behalf of those administrative areas that normally did a lot of 'paper shuffling' were able to see noticeable improvements in their underlying performance. As well, EDM also increases overall integrity and reduced error rates since documents are transmitted electronically and are subject to various edit checks and other validation procedures.

2.1.5 Early Electronic Commerce

Fully integrated Electronic Commerce can be viewed as a natural outgrowth of EDM. Electronic Commerce is now the method of choice for some businesses and consumers. A formal definition is as follows, "Electronic Commerce is the involvement of two or more individuals and organisations in the completion of electronic business transactions" (Rayport and Jaworski, 2000, p. 12). Figure 2.2 below provides a framework for modern Electronic Commerce.

Figure 2.2 – Framework of Modern Electronic Commerce



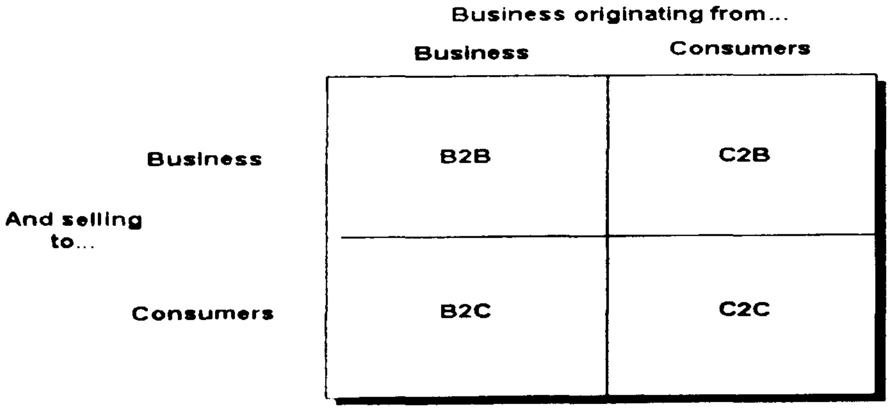
Source: Gartner Group, 1997

In the early development of electronic commerce, there were only two prevailing business models; Business to Business (B2B) and Business to Consumer (B2C). Over time, this has changed to incorporate two other business models.

2.1.6 Contemporary Electronic Commerce

Contemporary Electronic Commerce has evolved fairly rapidly over the past few years. While new business models (i.e. Business-to-Government (B2G) and Government-to-Consumer (G2C) have been initiated. The most prevalent four Electronic Commerce categories are shown in Figure 2.3 below:

Figure 2.3 – The Four Primary Categories of Electronic Commerce

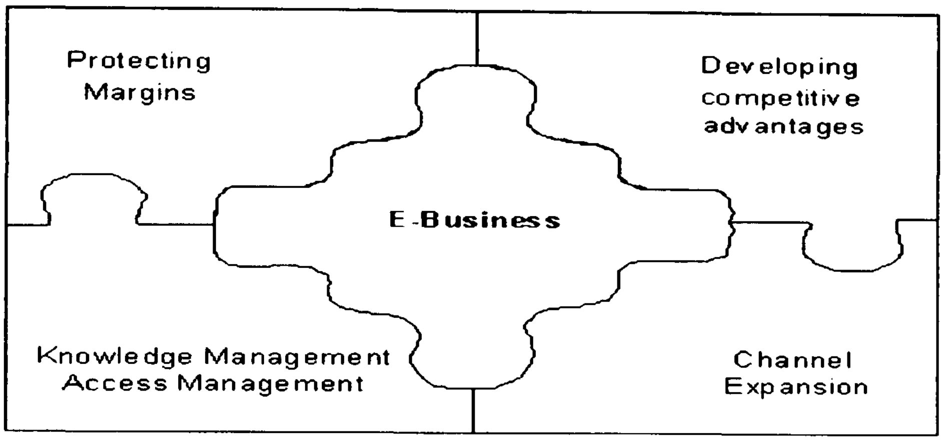


		Business originating from...	
		Business	Consumers
And selling to...	Business	B2B	C2B
	Consumers	B2C	C2C

Source: Rayport and Jaworski, 2000, p. 15

At present, the overall electronic commerce environment is witnessing a convergence of the two original, basic frameworks. Nevertheless, there is one fundamental question that must be answered, Why do organisations seek to engage in Electronic Commerce? In fact, this question has multiple answers, which are best represented in the following diagram of EC Motivators:

Figure 2.4 – The Electronic Commerce Motivators


Protecting Margins
Developing competitive advantages
E-Business
Knowledge Management Access Management
Channel Expansion

Source: Gartner Group, 1997

A number of leading consulting organisations have completed research studies which highlight the dramatic growth of Electronic Commerce. In an earlier study, business-to-business electronic commerce was expected to reach 220 billion U.S. Dollars and consumer to business electronic commerce to hit 140 billion U.S. Dollars in 2003 (Rayport and Jaworski, 2001, p. 24).

With these types of predictions it is important to address a number of important issues in this research study. First, there are a variety of information technologies that have enabled electronic commerce to evolve rapidly. Second, within information technology there are various important security issues. Third, in the United States the federal government has launched a number of important initiatives that help protect society from various types of threats. The current convergence of these three issues creates an important area for research. Especially, in terms of the recent efforts the U.S. government has made in this area; such as information sharing with regard to serious vulnerabilities to the cyber infrastructure.

2.2 Enabling Electronic Commerce Technologies

One of the most interesting and simultaneously challenging aspects of Electronic Commerce is the fact that it is so multi-faceted. This is true in terms of business processes, external environment technologies. Section Two describes the main technologies that enable today's Electronic Commerce environment. Due to the new developments in the areas of programming languages and manufacturer specific products, these areas have been deliberately excluded from the analysis. However, application development is discussed in Section Three, hereafter.

2.2.1 Mainframe Computing

Computing as we know it today, began with a very large physical machine capable of manipulating data and processing business transactions. The first mainframe computer was developed by International Business Machines (IBM) in 1953 and was known as Model 701 (PricewaterhouseCoopers, 1998, p. 482). In today's terms, mainframes might seem to be primitive, but in the beginning of the computer age these machines were genuine scientific inventions.

With a mainframe computer, businesses were capable of processing large amounts of business data. This provided evidence that information technology was capable of replacing mundane, but necessary administrative tasks, in a more efficient and lower cost manner. In its original design, access to mainframe resources was physically limited because an electrical (e.g. copper wire) connection was required for effective communication. For instance, large Cathode Ray Tubes (CRTs) or 'dumb terminals' were used by data entry personnel, clerical staff and computer operators for their respective daily job tasks.

In 2007, mainframes are still very popular and with the advent of newer, more powerful technologies this computing platform has been re-named 'the supercomputer' - a rather befitting term. Perhaps the most major advance in information systems over the past twenty years is the development of computer networks.

2.2.2 Computer Networks

Computer networks allow physically dispersed personnel to share data and other system resources. This is especially important due to the nature of modern day work where employees are often located in different offices, buildings and cities. Technology needs to support their work functions. There are a variety of computer network configurations (Pfleeger and Pfleeger, 2002 and Black, 2000). These are outlined in Table 2.1 below:

Table 2.1 – Popular Configurations of Computer Networks

	Type of Network
1.	Local Area Network (LAN)
2.	Wide Area Network (WAN)
3.	Metropolitan Area Network (MAN)
4.	Global Area Network (GAN)
5.	Internet
6.	Intranet
7.	Extranet
8.	Virtual Private Network (VPN)

All of these different network configurations allow end-users to share, transmit and data files, while also sharing other computing resources such as print, fax and World Wide Web services. However, there are some important limitations of computer networks.

Networks need to be properly configured, installed, managed and monitored. Typically, they are constrained by such physical factors as: user access, bandwidth, congestion, and a variety of technological/engineering variables. Because of their tremendous impact on Electronic Commerce types of specific networks such as the Internet, Intranets, Extranets and Virtual Private Networks are discussed in subsequent sub-sections of this section. Additionally, every network is dependent on a telecommunications protocol in order to transmit and deliver data. This subject is specifically discussed further in Section 2.6.

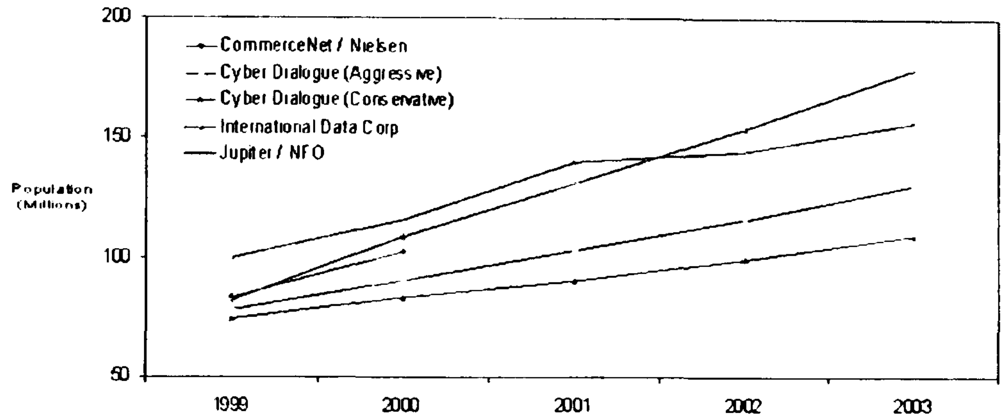
2.2.3 The Internet

The Internet was originally used to share research and educational information throughout the government and academic communities in the United States. The original ARPANET model facilitated the interchange of this information to and from various local area networks based on military installations and university campuses. Today, while many individuals still use the

Internet for educational purposes; the commercial benefits of this medium are being vastly expanded for the benefit of all types of organisations (e.g. educational, commercial and government etc.).

After the Public Switched Telephone Network (PSTN), the Internet itself is the next largest network in the world (Loudon and Loudon, 2000). It represents an ever-increasing number of connected organisations. Figure 2.5 below illustrates the rapid growth of U.S. Internet Users over a five-year time period.

Figure 2.5 – U.S. Internet User Growth from 1999 to 2003



Source: Rayport and Jaworski, 2001, p. 42.

While the abilities of the Internet itself cannot be underestimated there are also a wide variety of networks that take serve different purposes in today's business environment. An Intranet is the first of such networks.

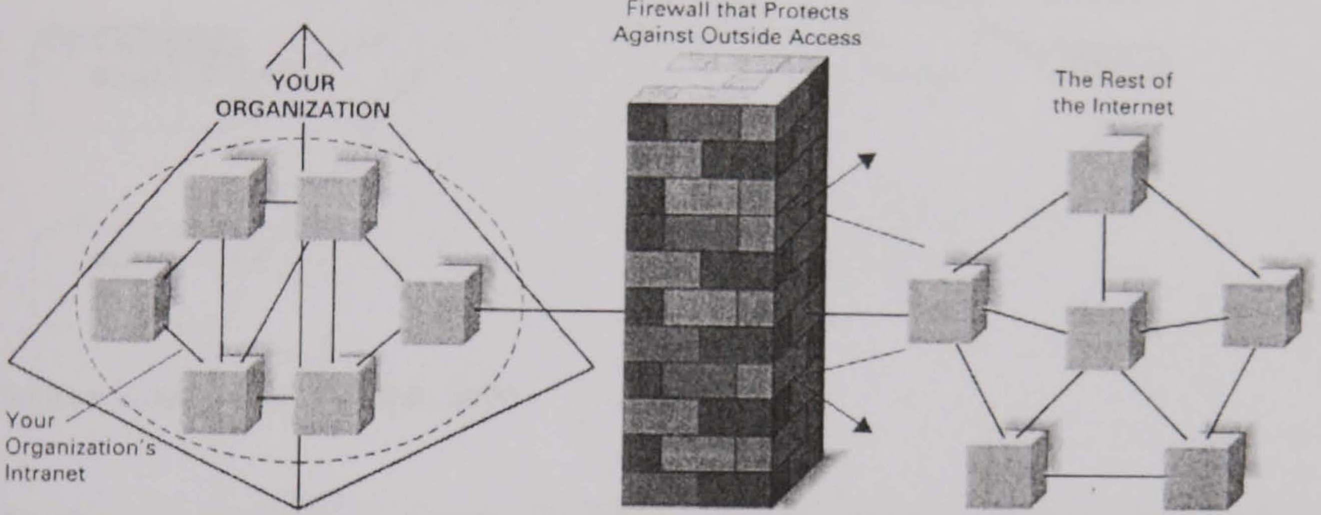
2.2.4 Intranets

Intranets provide a valuable method of sharing information throughout the modern enterprise. By incorporating the technological fundamentals of the Internet and Local Area Networks, businesses can provide authority- based access to company information resources. In the strictest sense, an Intranet employs LAN technology, Internet protocols, Graphical User

Interfaces (GUIs) and web browsers to obtain information that they normally would have required in a paper format.

Specific examples include: organisational policies and procedures that would be traditionally be kept in a three-ring binder on a shelf in an office and health insurance forms that might be physically stored in a Human Resources Department. With an effective company Intranet these items can be accessed on an 'as needed' basis from the employee's computer. Figure 2.6 below illustrates a typical Intranet configuration, as follows:

Figure 2.6 – Standard Commercial Intranet Configuration


Firewall that Protects Against Outside Access
YOUR ORGANIZATION
The Rest of the Internet
Your Organization's Intranet

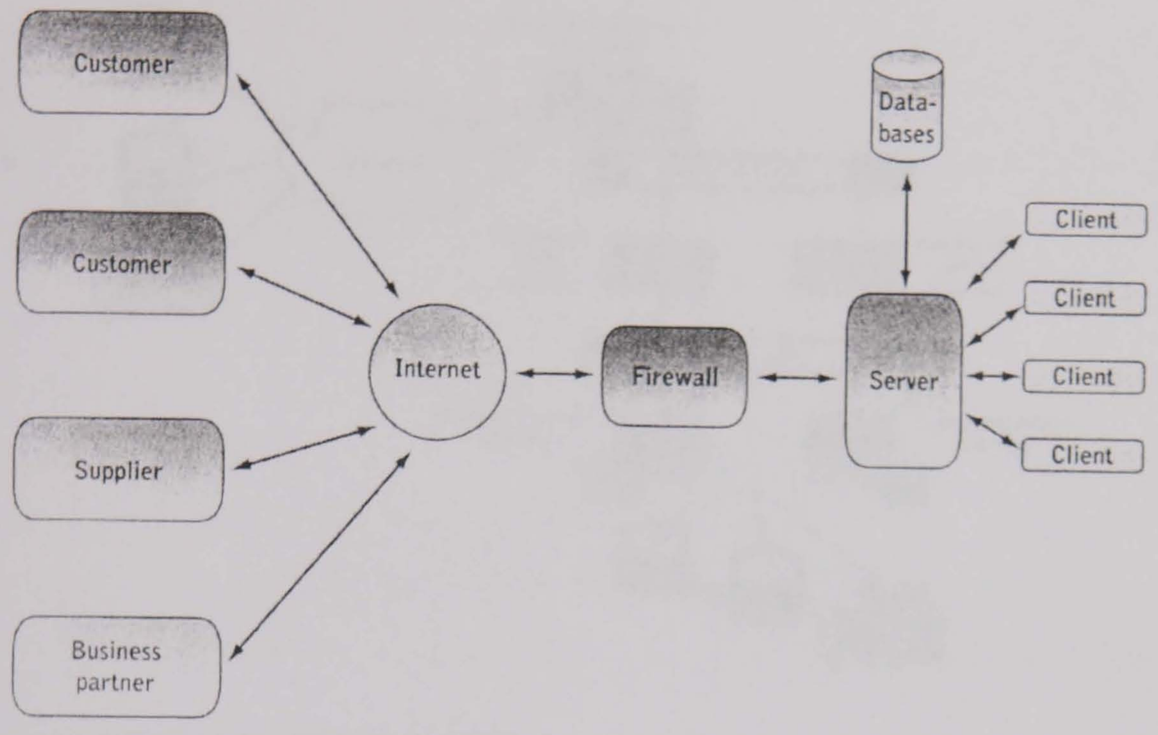
Source: Loudon and Loudon, 2000

From a management control standpoint, the Intranet is an access point that requires proper permission and sufficient monitoring. Since by definition an Intranet is limited to an internal environment, a natural by-product of this technology is the Extranet; which extends the reach of Intranet technology and related data stores (i.e. information systems, databases etc.) to external parties.

2.2.5 Extranets

An Extranet is a network technology that allows business partners to trading share information. One of the main capabilities of this technology is that it allows access to information in an automated and timely manner. Typically, over an Internet connection with special firewall and access control considerations one organisation is allowed to view the data on another organisation's information system. A normal business scenario would be where a product supplier can view inventory levels of selected products on their customer's system. This example is illustrated in more detail in the following figure.

Figure 2.7 – Standard Extranet Configuration



Source: Loudon and Loudon, 2000

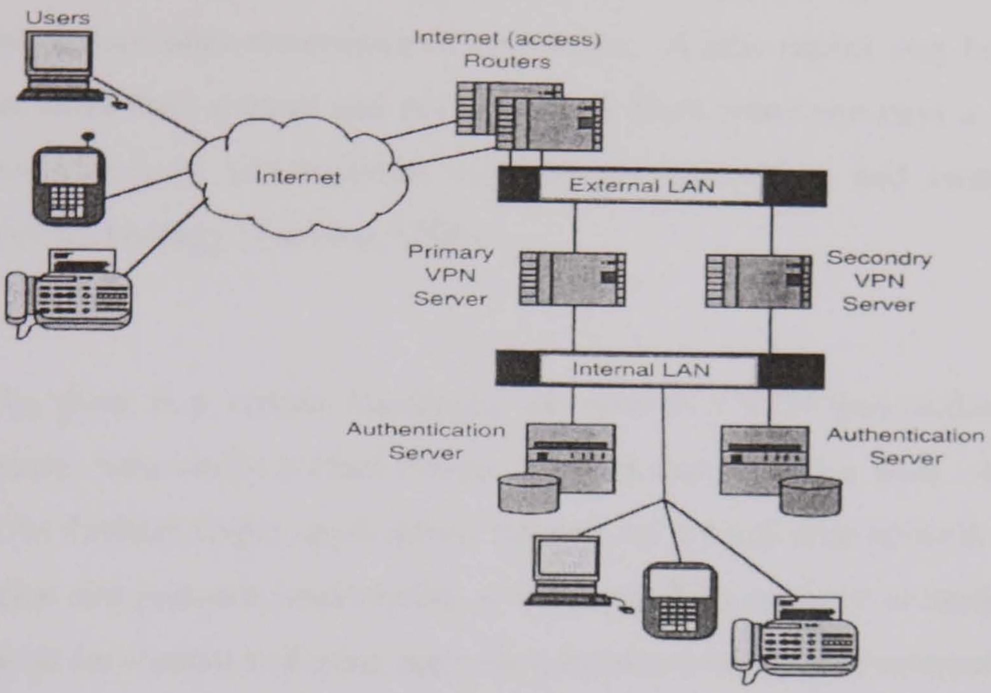
Another way of thinking of an Extranet is as a private WAN. Additional parties that might have business reasons to access an Extranet include customers, contractors and other business/trading partners. Since the technology used to establish and maintain an Extranet is ostensibly similar to a WAN and VPN this system has gained great popularity in recent years.

2.2.6 Virtual Private Networks

Today, a Virtual Private Network (VPN) is one of the most popular and cost-effective EC technologies. This technology allows an organisation to use the Internet, the largest public network available to transmit and receive data in lieu of a dedicated private line.

In recent years, the Virtual Private Network has become a very successful method for commercial enterprises to conduct business over the Internet. It is highly likely that this technology will become one of the most popular, fundamental tool for enabling Electronic Commerce. VPNs have a number of distinct and significant advantages that make this platform very appealing (Glass, 1996). It is important to note that although VPNs do, in fact, prove successful for most businesses there are a number of operational hurdles that must be addressed. Figure 2.8 below provides an associated network diagram:

Figure 2.8 – VPN Network Diagram



Source: Pfleeger and Pfleeger, 2002

The first main advantage of VPNs is from the economical perspective (Glass, 1996). VPNs are much more economical in terms of remote access telecommunications costs. Prior to VPNs, a typical system user would need to directly dial in to the company's network over an expensive leased long distance line. This situation created a high on-going operating cost to the business; particularly to physical dispersed companies. A VPN allows the company to arrange for services with a local Internet Service Provider (ISP) that provides the local connection to the Internet and then use a Managed Service Provider (MSP) such as British Telecommunications, AT&T, or Sprint to manage traffic directly to the corporate network server. While MSPs are actively seeking to manage these services on behalf of large organisations the reduction of telecommunication costs remain the key driver for implementing a VPN.

In addition to remote access costs there is also an operational requirement for such services. Over the past ten years, society has witnessed a dramatic increase in number of people working from home and other non-traditional offices. This situation is largely seen as an important factor for employees looking to achieve a work-life balance and not opting for dedicated office space. These telecommuters and 'road warriors' form what some industry observers have termed the virtual enterprise, in other words, one without exclusive offices and workspaces. For example, such arrangements frequently appeal to new parents returning to the workplace after maternity/paternity leave. A new parent may be able to arrange for childcare three days a week and prefer to work from home two days a week. Therefore, in order to effectively communicate with his/her co-workers and customers a VPN is a supportive technology (Terhune, 1998).

Secondly, there is a certain transparent element to a VPN thus making it a user-friendly architecture. One single Virtual Private Network can provide a wide variety of services that used to be limited single applications running on a local area network. By increasing the application and protocol functionality, a VPN user does not have to muddle through a variety of methods for sharing and using resources, thereby streamlining communication.

Thirdly, source code does not require modification when using a VPN for securing legacy applications. This is a security enhancement in the main Internet Protocol. With IPv6, VPN technology allows for a secure transmission stream between an authenticated client and a secure server.

While VPNs have their distinct advantages there are also a number of important disadvantages. One of which is the relative immaturity of the technology itself. Since this is a new method of telecommunication it is not as proven and robust as other, older technologies. With new vendors selling new products on a regular basis; new technologies typically are very deficient in security capabilities. This situation can be easily exploited by computer hackers and other groups.

Another disadvantage is interoperability. This affects the way one or more networks communicate with each other. In the past, organisations were dependent on having the same hardware and software vendor(s) to effectively communicate between each location/entity. Using a common vendor such as 3Com or Cisco was the only easy way of doing business.

This situation continues to plague the industry today, and while there are numerous de facto standards; it is critical that common open systems become the norm for this technology to continue to succeed (Terhune, 1998 and Glass, 1996). The final disadvantage relates to client side technology.

Virtual Private Networks typically require some modifications to the existing information technology environment. This situation can be both costly and time consuming. Software must be installed on each client device to provide communication to the VPN. Unfortunately, the high costs of such a role-out can lead to a delayed implementation.

2.2.7 Information Technology Protocols

The Internet is not absolutely necessary for Electronic Commerce, since two parties could generate transactions over two inter-connected Wide Area Networks (WANs). The Internet and telecommunication protocols are an essential component of effective Electronic Commerce since protocols provide a mutually agreed upon method of sending and receiving data (Black, 2000).

This systematic and methodical approach is critical in order to maintain uniformity, integrity and security throughout the entire communication process. While telecommunication protocols have existed for some time and have been used effectively in X.25, FDDI, ISDN and ATM networks there are new challenges that are inherent in E-Commerce. IT protocols are essential for the overall efficiency, effectiveness and security of data transmission through a computer network (Black, 2000). All of these protocols provide a pre-determined method for delivery, transport and receipt of data, which is normally most critical when doing so between two or more parties under different controlling organisations. Essentially, one could consider this to be the most fundamental process mode of operation in the telecommunications industry.

All IT protocols should be viewed in context with the Open Systems Interconnect (OSI) reference model. This framework was developed by the International Standards Organisation (ISO) in 1974, and provides seven separate layers that cover all processing functions for an information technology environment. Table 2-2 below provides a high-level summary of this important conceptual approach.

Table 2.2 – The OSI Reference Model

Layer	Key Functions
Application	Where applications on a network reside
Presentation	Application data encoding formatting
Session	Adding of extra functions to assist in data transport
Transport	Establishment of a reliable communication stream between systems
Network	Computation of links and packet switches across the network
Data Link	Delivery of a piece of information across a single link
Physical	Delivery of unstructured items across the telecommunications link

Source: Kaufman, Perlman and Speciner, 1995, p. 24

It is important to note that this model is not specific to any software or hardware; rather, it assists vendors and users in understanding the purposes of the different functions encompassed in data and voice networking.

2.2.8 Mobile Commerce

In many ways, Mobile Commerce is the next generation of Electronic Commerce. As information technology becomes more powerful and less expensive, individual consumers and business professionals can take advantage of Personal Digital Assistants (PDAs), smart phones, mobile phones, palmtop computers, and wireless networks. These technologies allow people to keep in very frequent contact with e-mail, stock market information and other items of interest. Furthermore, with the globalisation of industry, people tend to travel more than what was common only two decades ago.

Ghosh and Swaminatha (2001) discuss the impact of the growth of mobile commerce and its impact on software security and privacy. Citing industry forecasts for 600 million Internet subscribers and a $200 billion mobile commerce market they categorise the related risks, as either platform/operating system risks or software application risks. Platform risks arise primarily out of the failure of vendors to provide basic security features such as: memory protection, file access control, differentiation of user rights and biometric authentication in their products. Software application risks primarily focus on flaws in programming logic, weaknesses of low-level programming languages and inherent issues in script technology. Another risk in mobile commerce is the inability to precisely track the physical location of the attacker. In the aggregate, the threats within mobile commerce provide further justification for increasing each person's understanding of general computer security exposures.

By utilising the new technologies, business activities can take place while walking to the office, taking a taxi to a business appointment or flying on an airplane. While today's technology makes these items reality, it is important to acknowledge that the technologies are still in the early stages of development and adoption. Fundamentally, similar to the way other emerging technologies develop there is a high likelihood that there will be considerable security issues. As such, these security and control issues are also just beginning to be explored.

2.2.9 Composite Electronic Commerce Systems

Electronic Commerce systems are a composite of the aforementioned systems. These core systems plus peripheral computing devices such as printers, plotters, and scanners give the modern E-Business a solid technological base from which to operate. As technology evolves over time, existing technologies become faster and less expensive, following the traditional product life cycle.

Of critical importance are the issues of information technology security to all parties in Electronic Commerce. These groups include, but are not limited to private enterprises, individual consumers and government organisations. For the specific purpose of this research study, what will be investigated in-depth is the important role of federal governments in Electronic Commerce. National governments such as the United States, United Kingdom, and Canada, and others are primarily interested in protecting the good of society and enforcing laws and regulations.

2.2.10 Recent E-Commerce Developments

With the expansive nature of the Internet and the ubiquitous nature of modern computing we have witnessed a further expansion of E-Commerce developments over the past few years. For example, new business models such as Government-to-Business. Government-to-Government, and Government-to-Consumer have now become popular in the USA and other countries. Simultaneously, new technologies have enabled further connectivity and utilisation of wired, wireless, and mobile devices which has resulted in an expanding need for WWW and Internet technologies. In fact. some researchers most notably. Hoffman. Novak and Venkatesh (2004) have argued that the Internet now might be considered an indispensable technology. Today, we can look back at original U.S. Advanced Research Project Agency's efforts to develop the Internet as a research and academic infrastructure which now must continue to support new commercial and public purposes as well. Some of these necessities include: increased bandwidth (e.g. capacity) for large file transfers, multimedia applications, and two way voice and video conferencing (Mutch and Ventura, 2003). Further expected outcomes include the potential delivery platform whereby 100 Megabits per Second of capacity can be delivered to all home networks to support such activities as movie delivery and other web content services.

According to Fithcard (2003) this is why researchers supported by the U.S. National Science Foundation are developing a fundamental redesign of the Internet's network architecture which was primarily based on the old telephone network design. To make these technical developments possible, a very important project, Internet 2 was launched in 1996 to improve upon the original design and delivery platform of the Net. The project has the following four major goals: improved bandwidth, advanced networking applications, new network performance (including the implementation of protocol IPv6 which has enhanced security features over earlier versions), and development of important middleware applications (Matlis, 2006).

Additionally, Web 2.0 is the dynamic and ongoing development of the WWW and is often referred to as the Semantic Web. In this regard, information stored on the WWW can be stored, accessed and analysed using a variety of mechanisms such as traditional natural languages as well as advanced software agents. Some of the many advantages of this project include more efficient and effective knowledge exchange, information retrieval and universal application of this advancing technology. Furthermore. machine-to-machine communication will further enhance this suite of advancements to incorporate the use of a Resource Description Framework developed by the Worldwide Web Consortium. This technology is based on underlying logical expressions, linguistics and commonly accepted meanings (i.e. including those used in pre-WWW mediums). Two examples of this are zip/post codes and abbreviations for states and provinces (World Wide Web Consortium. 2007).

In order to accomplish this formidable task this effort a major philosophical change together with new system design principles and collective working group activities is needed. If this is successful then we can expect to see new technologies continue to emerge for such tools as web searching, mark-up and retrieval languages as well as web indexing and publishing techniques.

Finally, as these new technologies have occurred. so to has the array of threats and risks that commercial businesses, individual consumers and home computer users face. New threats from computer and related systems such as spyware, phising schemes and denial-of-service attacks continue to threaten the security of computers and other information technologies (Neumann, 2007 and Materson, 2005). In a recent study, Moore Et. Al. (2006) highlighted the complex nature of preventing, detecting and recovering from this common type of network attack. Specifically, the researchers highlight the broad nature of Internet security threats to all web sites regardless of their size, Internet Service Provider and other variables. In the end, as IT, the Internet and the WWW continue to evolve, so to must our knowledge, experience and capabilities in the areas of cyber security, risk management and auditing.

2.3 The Software Development Process

Application development and software engineering are two related areas that have a direct impact on the field of computer security. While this field is fairly mature it is also important to understand, in terms of what has been done over the past ten years to help with the security and reliability of computer applications. In one aspect, the field of software development has established a number of important methodologies that help streamline the development process itself. Due to the fact that many applications are developed in a commercial setting for multiple customers.

Survivability is an important characteristic for all information systems especially for those that are deemed critical in an organisation. Ellison Et. Al. (1999) provided an analysis of the necessary qualities of such systems; which in today's environment are often comprehensive and networked. In terms of system survivability, it is noteworthy to consider that a distinction between attacks, failures and accidents are not particularly important. Rather, the unbounded computing environment is found to exhibit the following characteristics:

1. It encompasses multiple administrative domains with no central authority;
2. It lacks global visibility;
3. Interoperability between administrative domains is determined by convention;
4. Systems are widely distributed and interoperable;
5. Users and attackers can be peers in the environment; and
6. It cannot be partitioned into a finite number of bounded environments.

(Adapted from Ellison Et. Al., 1999)

Their research also found that survivable systems must have four key attributes. First, these systems must be resistant to attack. Second, they must be capable of recognising attacks. Third, they must provide for complete recovery after an attack. Lastly, they must adapt and evolve after attacks to reduce the impact of future attacks. In late-2001, research lead by the U.S. CERT/CC began to develop new methods to evaluate the survivability of systems (Feigenbaum, 2002). This new area of information systems security research is likely to be highly valuable to many organisations.

The field of systems analysis and design has also impacted application development and software engineering. Popular development strategies such as the Systems Development Life

Cycle (SDLC), Joint Application Design (JAD), Rapid Application Development (RAD), Prototyping and Object-Oriented Analysis and Design provide a structured approach to the systems development process. These development approaches are quite diverse in their individual processes, but they nevertheless supply a structured framework to systems development which in turn creates better functioning and more reliable information systems.

Computer Aided Software Engineering (CASE) can assist organisations in developing more robust systems and achieve high levels of organisational change (Hoffer, Geroge and Valacich, 2002 and Orlikowski, 1993). A few of the main advantages to adopting CASE include the regeneration of programming code, automated testing and system generated and maintained documentation. For small organisations, CASE tools can be cost prohibitive, however, in large software development companies they are commonplace. In addition to automated tools, there are software development (e.g. process-based) frameworks that work in conjunction with CASE tools.

The Capability Maturity Model (CMM) developed by the Software Engineering Institute (SEI) and is a popular methodology for software development. The CMM focuses on building a process infrastructure that continually advances the effectiveness of software engineering and management practices. Included in the CMM are five levels of software process maturity: initial, repeatable, defined, managed, and optimising (Parzinger and Nath, 2000 p. 357). With initial characteristics few organisational processes related to application development are defined and this situation leads to applications being developed ad-hoc and the ultimate success of the project is highly variable. Repeatable characteristics include tracking of project management variables such as cost, schedule and functionality. Defined components cover documentation of a systems development methodology. Managed criteria allows for detailed measures of the software process and product quality are maintained and controlled and with optimising a further continuous improvement process is implemented.

Bakersville (1993) researched the implications of information systems security for information systems development. The first generation approach discussed by the researcher is the use of checklists that were used in systems development. Specifically, it is noted that three primary checklists had between 790 and 954 total items, with various individual items related to security (Bakersville, 1993, p. 382). The second generation approaches to computer security (primarily in the 1980s) have four primary assumptions. First, the requirements impacts of the security system elements will be complex and interconnected. Second, the exact controls could be unique and ideal. Third, the feasible solution set is not bounded. Lastly, a well-understood and well-documented security design leads to efficient security maintenance and modification (Bakersville, 1993, p. 400).

In the 1990s, with the third generation approach five broad assumptions relate to computer security models. These are:

1. The ideal security solutions will be the result of a broad understanding of the security problem(s);
2. Second, abstract models clarify the organisational problems, and more effective controls will result;
3. Designs founded on such models will prove flexible, adaptable and consequently longer lived;
4. There are few universal problems; and
5. Controls place constraints on information systems (Bakersville, 1993, p. 408).

Landwher Et. Al. (1994) surveyed the relationship of flaws within computer programs in order to develop a possible taxonomy and operated on the probable assumption that if someone knows how a system failed than that information can help us build more resistant systems in the future. Computer security flaws are defined as "any conditions or circumstances that can result in denial of service, unauthorised disclosure, unauthorised destruction of data or unauthorised modification of data" (Landwher Et. Al, 1994, p. 211). Early approaches to these issues dealt with 'patching' of software programs. However, early research in the 1970s and 1980s indicated that fixing software was not always an ideal situation. This was due to the fact that additional exposures were often discovered and some vulnerabilities might not be easily repaired. Furthermore, seven categories were used to establish the types of operating system security flaws as indicated below:

1. Incomplete parameter validation;
2. Inconsistent parameter validation;
3. Implicit sharing of privileged/confidential data;
4. Asynchronous validation/inadequate serialisation;
5. Inadequate identification/authentication/authorisation;
6. Violable prohibition/limit; and
7. Exploitable logic error.

While a taxonomy could not be statistically validated in this study, the root causes mentioned above have later lead to additional research in this area. Software flaws are considered in

Chapter Three-Research Methodology as one of the key variables that will be analyzed in this research project.

Further research by Parzinger and Nath (2000) studied the relationship between total quality implementation factors and software quality. In addition to the CMM, these researchers also used ISO 9000-3 guidelines. Their study found a positive relationship between TQM implementation factors and the indicators of software quality.

Three costs of quality related to software application development were cited. Failure costs arise when fails before or after it is released, this can be related to requirements and coding that needs further analysis, debugging, testing or re-installation. Appraisal costs primarily cover quality assurance and testing. Prevention costs include training and utilising continuous quality improvement to achieve optimal performance. While it appears difficult to directly correlate these costs to individual information security issues, they are important considerations that software development organisations consider throughout the lifecycle of their various products. These issues need to be understood by the purchasers of software systems, so they can understand the risks that these systems present.

2.3.1 Commercial off the Shelf Software

In recent years, there has been a growing trend for organisations to move away from customised software (e.g. those packages that suit their own, unique needs) and use vendor developed common use software products. Commercial off the Shelf (COTS) software packages are also vulnerable to security flaws and weaknesses. Examples of such packages include Microsoft Office, JD Edwards and WordPerfect.

COTS products also have a practical advantage for large organisations, in that they do not require significant internal maintenance efforts. Rather, the software company can be paid an annual maintenance support fee, normally approximately fifteen or twenty percent of the software purchase price to provide routine updates that correct software bugs, increase functionality, and implement other enhancements such as regulatory requirements.

Lipson, Mead and Moore (2001) studied the security flaws with COTS packages in order to determine the survivability of these systems to withstand attack. One weakness that they identify is that the software engineering information and records are maintained by the software development company. This situation inhibits the customer from being able to conduct a complete risk assessment of their software applications. To mitigate this problem, they suggest that customers work with their COTS vendor(s) and conduct an enterprise-wide software vendor risk assessment. Included in this process are the following sub-sections:

1. Vendor's inherent risk assessment;
2. Visible product attributes;
3. Technical competence;
4. Performance history;
5. Compliance;
6. Trustworthiness;
7. Business management competence; and
8. Controlled (product) evolution;

By conducting this type of risk assessment an organisation can gain a greater understanding of the potential security flaws, exposures and vulnerabilities in the COTS products they use. In turn, it provides a very proactive method of managing computer software security.

2.3.2 Security Engineering

The U.S. National Security Agency (NSA) developed a CMM specifically related to computer security. This methodology builds only the core principles of the CMM for software, and strives to include a number of important security components. Beginning in 1993, NSA brought together representatives of: the government, private industry, academia and research communities to build upon the successes of the original CMM. Today, tools exist to make evaluations of the security engineering content of different products, projects, and organisations. The benefits of this framework include:

1. Improved quality of secure systems, trusted products, and security engineering services;
2. Wider availability of security systems, products and services;
3. Reduced costs of developing and delivering such items;
4. Better investments in security engineering tools, training and management;
5. Increased awareness of the qualifications of security engineering providers; and
6. Improved selection of appropriate security engineering providers.

Adapted from: SSE-CMM Executive Summary, 1999, p. 2

Security engineering is yet another way that security can be built into information systems. Hopefully. resulting in fewer security vulnerabilities. exposures and incidents. At this stage. no publicly available literature appeared to be available in this discrete area.

2.4 Information Sharing and Information Infrastructures

Information sharing and information infrastructures are key conceptual tenants in today's Information Age. Also, included in this section is a discussion of: inter-organisational systems, information communication technology, knowledge management, government information systems, web information systems, global information infrastructure, and the U.S. national information infrastructure. It appears that many of these information systems provide a technical basis for sharing information in a highly effective manner, about what many in the industry have indicated is necessary, and that is cooperation.

2.4.1 Information Sharing

Information sharing is an important issue in computer security and information systems in general. High speed communication in traditional telephone systems, electronic mail and web sites, collectively provide a variety of different media to disseminate information. Other print forms of communication such as magazines, newsletters, and facsimile transmissions are also still available.

Rhodes (1998) discussed an information sharing arrangement that dealt with competing organisations in the petroleum industry. The Year 2000 issue forced these organisations to work together in order to solve common problems. In this highly competitive industry, most companies use similar, integrated control systems that are considered complex. Shell Oil, British Petroleum and others worked together to identify, test and remediate their shared legacy systems.

There are a number of other success stories in this area. Rumizen (1998) applies this scenario to a leading U.K. chemical company, Haver (1998) provides an example from the International Monetary Fund (IMF) and Rouiller (1998) illustrates a case from the Swiss financial services sector. Can this type of successful cooperation be applied to cyber security? This question will be considered at a later stage.

However, sometimes organisations can have competing interests that reduce the overall effectiveness of information sharing. Ferrat (1998) made a study of hospitals in the Dayton, Ohio area and identified a number of related disadvantages. These include:

1. Different interest groups envision the achievements of a project based on their own interest and experience;
2. Those who have been actively involved with a systems development project typically have a higher opinion of the achievements of the project;
3. Different interest groups perceive the problems of a system and recommend changes based on their own perspective;
4. End users of a system are likely to perceive greater problems and recommend more changes than systems developers;
5. Getting users involved in the development process, while important, may be difficult in practice, calling for careful planning of the level and timing of that involvement;
6. High perceived value of information does not always imply high use of a system;
7. A system is useful as long as the stored data, particularly for more valuable items, spans a preferred time horizon;
8. A system designed to support high-cost individuals is likely to be more useful if lower-cost employees perform most of the information retrieval, that is, chauffeured operation is used benefits of an ideal system;
9. Hands-on experience is likely to help users better appreciate the benefits on an ideal system; and
10. Various interest groups perceive high benefits of an ideal system from their own perspective.

(Adapted from Ferrat, 1998)

These findings are interesting since they provide insights into methods of achieving improved functionality and satisfaction. Additionally, Jones Et. Al (2001) and Whiting and Chabrow (2001) discuss some of the reasons why the U.S. Federal Government is eager to forge new relationships with private industry.

2.4.2 Inter-Organisational Systems

Inter-Organisational Systems (IOS) are defined as, "information and communication technology based systems that transcend legal enterprise boundaries" (Kumar and Van Dissel 1996, p. 279). Inherent in this type of technology is its implied level of cooperation and coordination between all participants. By providing a cooperative and strategic method of sharing information it allowed organisations to share costs, improve economies of scale, increasing the product life cycle expectancy and ultimately increase their return on investment. Intra-firm behaviour then subsequently takes on a new inter-firm dimension since information is shared between two or more organisations, for the mutual although necessarily equal benefit of each of the other entities.

Soumi (1988) and Johnston and Vitale (1988) categorise the changes that IOSs bring to an enterprise. These are categorised as organisational changes. economic changes and technological changes. Organisational changes cover such issues as the basic need for an IOS, the 'liberalisation' of the telecommunications industry and structural growth of the organisation. Economic changes deal with increased importance and thereby increased value of data, decreased telecommunication costs, and increased costs of labour. Lastly. technological changes cover improved hardware and software and more standardised protocols and government regulation.

While these systems began in the EDI environment, business process redesign efforts helped organisation capitalise on the strategic benefits of these information systems. Originally, they were heavily used in the manufacturing sector to share information between suppliers, manufacturers and retailers. Early research in this area, focused on the economic and operational benefits to the participating organisations (Johnston and Vitale, 1988). Summarised below are a few notable examples of prior IOS research studies:

Table 2.3 – Prior IOS Research Studies

Researcher(s)	Year of Study	Focus of Study
Lewis and Talalayevsky	2000	Logistics Management
Premkumar	2000	Supply Chain Management
Kumar and Crook	1999	Multiple Case Study
Hendon, Nath and Hendon	1998	EDI to IOS Migration in Marketing Firms

Recently, new research has focused on identifying possible extensions of this type of information system. Kumar and Van Dissel (1996) discuss three types of IOSs. These varieties include pooled information resources, value/supply chain and networked.

Pooled information resources inter-organisational systems whereby information is shared for the aggregate benefit of the participating organisations. This type of IOS has been quite popular in the past twenty years, and some examples are illustrated in the following table. below:

Table 2.4 – Examples of Pooled IOSs

IOS	Purpose

SABRE	Airline Reservation System
GAIN	A Global Alliance for Airline Safety Information
CLUE	Auto Insurance Claim Database
PLUS	Automatic Teller Network

SABRE is a popular airline reservation system used by airlines and travel agents. Even though it was originally developed by American Airlines, today it is a system widely used in the industry around the globe. CLUE provides a central database for automobile insurance claim information through a shared database structure. In this system, participating insurance companies benefit from having a central repository of information. The PLUS pooled inter-organisational system for automatic teller transactions in the United States. This provides participating financial institutions with the opportunity for their customers to withdraw funds at member banks, even those where they do not maintain an account. Transactional information is then shared with all participating organisations to allow for accurate record keeping and control.

Value/supply chain inter-organisational systems exist as a result of the customer supplier relationship and are sometimes referred to as pipeline management systems. By providing information about customer needs (i.e. orders, logistics etc.) the normally uncertainties in the supply chain process can be reduced. In the end, organisations benefit from cost, cycle time, and quality advantages over competitors who do not use similar systems.

Networked IOSs are normally associated with companies involved in joint ventures. In this type of business relationship each partner is hoping for a specific type of advantages perhaps on a global basis. This type of inter-organisational system can be primitive meaning that it uses basic technologies such as e-mail, telephone and fax. They can also be more complex where CAD/CASE interchanges, discussion databases and other collaborative systems are utilised.

Although there are many advantages to inter-organisational systems there are also some significant, potential disadvantages. Kumar and Van Dissel (1996) describe these are follows:

1. Overgrasing can result since some organisations will gain more advantage than others, thus they argue that there will be some winners and losers. The losing organisations suffer from over zealous organisations and/or their own internal failures.
2. Poaching involves one participating company diverting IOS resources from one of the participant organisations for their own use.
3. Fouling or contaminating arises when one organisation corrupts data in the IOS.
4. Stealing can come about when one organisation takes data from another organization for its own advantage.

Since IOSs are often complex and make use of Extranets and other network technologies it is important to control these systems. The following table illustrates in a risk management perspective some controls techniques that can be used to mitigate the IOS risks identified above:

Table 2.5 – Generic IOS Risks and Controls

IOS Risk	Corresponding Controls
Overgrasing	Usage charges and contractual obligations
Poaching	Procedural security, virus scanning and access controls
Fouling/Contaminating	Access controls and transaction monitoring
Stealing	Software security controls and audit and event logs

Adapted from: Kumar and Van Dissel, 1996

Beyond the traditional benefits of IOS services and applications of this technology Holland and Lockett (1997) and Clark and Stoddard (1996) cited a number of factors that contributed to the growth of these systems. These further benefits include: general information sharing, increased availability of information and electronic commerce efficiencies.

Public-private partnerships can also assist in information sharing. Like other countries the United States has sought to gain the support, assistance and buy-in of for-profit companies and other organisations; specifically with regard to a number of information systems initiatives these have typically focused on the development of standards and cooperation with regard to NII initiatives and information systems security. The InfraGard and CERT/CC programs are examples of such public-private partnerships. At this time, it is difficult to gauge the success of these organisations as it does not appear to be discussed in the literature.

2.4.3 Information Communication and Technology

The more prosperous and advanced a society appeared to have a direct relationship with the possessed level of Information Communication and Technology (ICT). While those countries that are not as fortunate struggle to build supporting infrastructure components, there remains what is known as *The Digital Divide*. Steinmueller (2001) argued that this division is narrowing and that some countries may be able to 'leapfrog' other countries with higher wealth and greater infrastructures. Typically, the way economists measured wealth using industrial/manufacturing factors. While this was reliable in a manufacturing based economy, today the technology transfer related to new information technology allows developing counties to 'plug and play'. And it is these adaptive capabilities that create the potential for lesser-developed countries to advance very rapidly. Additional areas of opportunity for emerging economies include: open source software, difficulty in enforcing intellectual property rights and rapid dissemination of information.

The European Union is also using ICT to help develop a Pan-European infrastructure. Rada and Ketchell (2000) explained that there are many challenges to this effort. One of the key obstacles is harmonising telecommunication standards. Another issue is the ability to compete on a global basis for trade. Supporters of the common European currency believe that this is a step forward. Nevertheless, ICTs are important initiatives which can help develop regional, national, and global information infrastructures.

2.4.4 Knowledge Management

Knowledge management is a relatively new approach to a basic concept. Johnson (1998, p. 2) explains that this practice allows executives and other employees to capitalise on their intellectual assets. In this regard, the major points discussed deal with understanding the support roles in an organisation that can contribute to, but also may inhibit the development of a successful knowledge management system. Organisational dynamics, collaboration, corporate learning and knowledge management technology are major factors in this process (Johnson, 1998 p. 2). Although this study was conducted in the healthcare industry, there are a number of important lessons that can be learned. First, explicit knowledge is often found in documents. Second, knowledge management strengthens a service provider's overall organisational abilities. Third, all individuals in an organisation can contribute to knowledge development and sharing. Fourth, in order to have an effective knowledge management system individual experts will need to share their knowledge and put this information into document databases and repositories.

Davenport, Harris and DeLong (2001) and Davenport (1999) explained that collaboration is central to the results of a knowledge management system, and it is indicated that open, non-political, non-competitive environments are often those that can achieve the best results. One of the key underpinnings of this area is to develop a process whereby data is turned into information which in turn is transformed into knowledge that can be used in future decision making. Information systems are particularly useful in developing what Davenport refers to as a knowledge management system. Databases, data warehouses, central repositories and other systems (i.e. decision support systems, expert systems etc.) can provide the technological components to help organisations. Furthermore, these systems can also be used in information systems to store, track, monitor and predict information systems security events.

2.4.5 Government Information Systems

Government Information Systems (GIS) contain a diverse set of data repositories that can be used by other government agencies, commercial businesses and private citizens. The overall purpose is important to consider and some examples are included in the following table:

Table 2.6 – Examples of Popular U.S. Government Information Systems

Agency	Information System(s)	Availability	Purpose
Federal Aviation Administration	1. National Transportation Safety Board (NTSB) Aviation Accident/Incident Database 2. FAA Incident Data System 3. Near Midair Collisions Database 4. Bureau of Transportation Statistics – Airline Traffic Statistics	Public	Share airline safety and performance information

Department of Justice	National Crime Information Centre (NCIC)	Federal, state and local government law enforcement agencies only	Track and maintain records on individuals with criminal records and their backgrounds
Department of Commerce – Census Bureau	Various economic and statistical information systems and surveys	Public	Provide business and consumer demographic data
Occupational Safety and Health Administration	Inspection data repositories	Public	Summarise information about site inspections, workplace injuries and similar issues

Other issues related to national security can evolve when government bodies are too eager to appease pressure groups and use GISs to share information. In one example, the Environmental Protection Agency (EPA) was prepared to share information about chemical warehouses on its web site. The agency has been under intense pressure from environmental activists. However, after the FBI, CIA, Department of Defence and Department of State learned of this situation, they explained to the EPA that such information may increase the risk of terrorist attacks on industrial plants (Harrigan, 1998 and Hess, 1998). While the motivation by EPA administrators was proper the risk to national security outweighed the benefits. In the end, the information was not posted on the EPA web site.

2.4.6 Web Information Systems

Web Information Systems (WISs) take advantage of the inherent capabilities of the World Wide Web (WWW). They also provide an ideal opportunity for governments to share information to a variety of stakeholder groups. Additionally, WISs provide an opportunity for businesses and other large organisations to quickly disseminate large amounts of information in a timely and cost-effective manner to the public at large (Lee and Leifer, 1992). The following table summarises some commonly used general WISs:

Table 2.7 – General Web Information Systems

Name	Description	Sponsor	Web Site Address
EDGAR	Financial information on publicly traded companies	U.S. Securities and Exchange Commission	www.sec.gov/edgar.shtml

Firstgov	Government-wide information repository	U.S. Federal Government	www.firstgov.gov
Debtor Reporting System	Financial information about debt obligations for countries around the world	World Bank	www.worldbank.org/data/DRS/drs.html
United Nations Crime and Justice Information Network	Data repository for crime prevention and criminal justice information for U.N. member states	United Nations	www.uncjin.org

Kambil and Ginsburg (1998) studied the capacity of the Internet to disseminate financial information from publicly traded/listed companies on the Internet using a case study approach to the U.S. Security and Exchange Commission's Electronic Data Gathering, Analysis and Retrial system (EDGAR). Overall, they found the system to be very effective and easy to use, but they also developed a series of eight challenges to developing and maintaining WISs. These include: interfacing, incomplete information, poor identification of data objects, reporting errors, terminology and nomenclature issues, and the use of legal language.

WISs are also very useful in the field of information systems security. Over the past ten years, a number of organisations have developed WISs to share information about security threats, vulnerabilities and exposures. The following table provides a brief overview of such WISs:

Table 2.8 – Information Systems Security Specific Web Information Systems

Sponsoring Organisation	Type of Organisation	Web Site Address
U.S. Computer Emergency Response Team	Government Sponsored	www.cert.org
Computer Incident Advisory Committee	Government	www.ciac.llnl.gov
Global Incident Analysis Centre	Professional Organisation	www.sans.org/giac.htm
Bugtraq Vulnerability Database	Commercial Company	www.securityfocus.com
X-Force	Commercial Company	www.xforce.iss.net

Mitre	Government Sponsored	www.cve.mitre.org
National Infrastructure Protection Centre	Government	www.nipc.gov

The National Infrastructure Protection Centre (NIPC) helped form the focus of this research study. Further background information and analysis is provided later in this chapter.

2.4.7 Global Information Infrastructure

The Global Information Infrastructure (GII) has been a recent effort organised by the G8 countries. These countries include the United States, Canada, United Kingdom, France, Germany, Italy, Japan and Russia. To initiate these efforts, eleven major projects were initiated in 1995, and these are summarised in the following table:

Table 2.9 – Initial G8 Global Information Infrastructure Projects

	Project Description
1.	Global Inventory
2.	Cross-Cultural Education and Training
3.	Electronic Libraries
4.	Global Emergency Management
5.	Government Online
6.	Multimedia Museums and Galleries
7.	Global Healthcare Applications
8.	Global Marketplace for Small and Medium Enterprises
9.	Maritime Information Society
10.	Global Interoperability for Broadband Networks
11.	Environment and Natural Resources Management

Adapted from Trjanne, 1995

Beginning in the early-1990s, these highly industrialised nations, realised that their internal economies were moving from a manufacturing model to a service model and that the Information Superhighway or Internet was one of the critical success factors in advancing their national economies. At the same time, other less developed/industrialised countries were beginning to acknowledge that it was necessary to increase their investment in telecommunication and information infrastructures (Trjanne, 1995).

Graf (1995) commented on U.S. initiatives in this area and discussed the five main principles that are necessary to effectively build information infrastructures. The first principle is a flexible regulatory environment. The next principle is development of the telecommunications market. The third principle deals with open access. And the fourth and fifth principles are private investment and universal service, respectively. Much of these efforts in the United States have been accomplished through though deregulation, increasing competition and auctioning of telecommunications frequencies.

Hudson (1998) explained how three major trends that will support the GII development. Firstly, the rapid introduction of new technologies and services. Secondly, the restructuring of the telecommunications sector will assist in nurturing the GII. Thirdly, the globalisation of economies and communication should also help advance the components of the GII. Additional support for these trends is found in the growth of the Internet and the ability of this technology to support many of the GII initiatives summarised above.

This has been a difficult issue for poor countries for a number of reasons. Their baseline infrastructures were inferior to those of the G-8, especially in areas like Africa, South America and Southeast Asia. Additional obstacles deal with legal, political and cultural issues. While other countries invest more resources to build their own information infrastructures the United States has done the same.

2.4.8 U.S. National Information Infrastructure

President Clinton and Vice-President Gore made the United States National Information Infrastructure (NII) a major national priority in the early-1990s. Building on its leadership in Internet development and a highly functioning telecommunications infrastructure, the USA developed a series of important initiatives for the NII. *The Report of the Information Infrastructure Task Force on Applications and Technologies* broadly defines the NII as "the facilities and services that enable efficient creation and diffusion of useful information" (U.S. Department of Commerce, 1994 p. 1). The NII has many advantages including: enhancing the competitiveness of the manufacturing base, increasing the speed and efficiency of electronic commerce, improving healthcare, promoting the development and accessibility of quality education and lifelong learning for Americans, improving environmental monitoring, sustaining the role of libraries and provide government services in a faster and more efficient manner.

In order to help achieve these ambitious goals the NII has a series of common objectives that stretch across industries and organisations. These include: equal access, standards, privacy and security, training and support, research and development and performance measurement. Cibora and Hanseth (2000) explained that infrastructures are important foundations for supporting business objectives. They identified seven major problems that must be addressed in order to achieve success: strategy alignment, universal use and access to IT resources, standardisation, interoperability of systems, flexibility, resilience and security. In all, the same can be said about NIIs, but on a much larger scale. While much progress has been made, but time help determine if these ambitious efforts succeed. In this regard, there also seems to be significant research opportunities.

2.5 Key Concepts in the Field of Computer Security

Within any discipline there are a variety of concepts, objectives and terms that are used to describe specific issues. In some cases, the nomenclature can be confusing to an inexperienced person. So for clarity purposes, this section is organised into four sections dealing with: fundamentals, objectives, definitions and terms.

2.5.1 Fundamentals

There are three fundamental concepts in computer security that should always be are considered by discussing and understanding the field of computer security. These core concepts are as follows:

1. ***Least privilege*** – a system user should only be granted the minimum amount of rights necessary to complete their task(s);
2. ***Ease of use*** – there is a trade-off of sorts whereby the ease of using a computer system is reduced as the amount of security within that system is increase; and
3. ***Need to know*** – request for system privileges should be restricted to the data and systems that the user has a prudent and justified reason to use.

These three core principles are very important in everyday data processing operations. They should also be considered during IT risk assessment, policy development and future information systems initiatives.

2.5.2 Objectives

The ideal criteria for information technology security revolve around five key objectives. These objectives provide a method for evaluating business processes and supporting information systems. The five primary objectives of information technology security are: confidentiality, availability, integrity, non-repudiation and authentication which are defined in the next sub-section.

2.5.3 Definitions

As in any field there are technical definitions organized usually by standard setting bodies and other recognized authorities. In everyday practice, these definitions can easily take on adulterated meanings by using slang words and biased interpretations. Definitions are as follows:

> ***Confidentiality*** – means that the assets of a computing system are accessible only by authorised parties (Greenstein and Feinman, 2000);
> ***Availability*** – means that assets are accessible to authorised parties when required;
> ***Integrity*** – means that assets can only be modified by authorised parties or only in authorised ways (Pfleeger and Pfleeger, 2002);
> ***Non-Repudiation*** – the property of a scheme in which there is proof of who sent a message that a recipient can show to a third party and the third party can independently verify the source (Ford and Baum, 1997); and
> ***Authentication*** – the process of reliably determining the identity of a communicating party (Kaufman, Perlman and Speciner, 1995).

Confidentiality is probably one of the more difficult IT security objectives to discretely analyse. It is important for each organisation to develop and enforce formal security policies that classify the types of information in their enterprise. As E-Commerce enables more businesses to compete in a global marketplace confidentiality will be more important than ever before. It will also add to the confrontational roles between the competing interests of government, personal and business interests.

An E-Commerce environment utilises a Virtual Private Network a company may choose to outsource some or all of its network management processes. This situation puts an additional burden on the service provider. Nevertheless, a security assessment should be conducted to determine the level of confidentiality needed to adequately protect the company's information. Another important factor to consider is the company's culture and what types of information is allowed to be viewed and shared between various employee groups. While it might be very straight forward to understand why payroll data should not be accessible to all employees; it might be more time consuming and difficult to classify medical information in a large health system. The next key objective of IT security is availability.

As organisations have become increasingly dependent on various types of data to make business decisions; the availability of such data becomes more important of a control issue for overall corporate resiliency. Many Electronic Commerce oriented businesses can easily conduct business 24 hours a day/365 days a year. However, if their inventory or customer information is not available they might experience lost sales, employee downtime and bad publicity. Prudent IT systems such as tape back-ups, disk mirroring and Redundant Array of Inexpensive Disks (RAID) are technologies to help ensure that necessary data is available to those parties that need access to it at the exact time they desire it. This is highlighted by the recent hurricanes in the USA and tsunamis in Asia-Pacific.

Integrity refers to the essential value that data is not altered during input, storage or retrieval. If data is corrupted either intentionally or by error the organisation will be faced with the possibility of making incorrect decisions based on the bad data or incurring additional time to correct and modify the altered data. This in of itself can create havoc for an organisation.

Non-repudiation is the security objective that authenticates a user prior to allowing access to company resources. An individual's identity whether known to the system by a unique user id and password and/or biometric credential is crucial to the overall security of any information technology network. Providing access to individuals who do not have permission obviously creates a very dangerous situation that can result in theft or damage to sensitive information.

Authentication deals with the ability verify a person's identity. It requires that a system be able to validate that a user is who they present themselves to be. Normally, access controls such as user ids, passwords, smart cards and other devices are used to support this process.

With all of these issues and complexities what protective measures can the organisation take to protect itself? This understanding can only arise from a further discussion of the types and levels of computer security.

2.5.4 Terms

Often times various security terms are associated with different meanings (Howard and Longstaff, 1998). Accordingly, it is important to develop a list of common computer security incident terms and definitions.

Access abuse: Inappropriate use of computer or network resources.

Active wiretapping: Unauthorised observation of a data communication transaction.

Computer virus: A self-propagating computer program that may directly or indirectly cause one or more security incidents.

Data system integrity loss: Tampering with an information system.

Denial of service: Unauthorised suspension of network or computer system function(s).

Destruction of data: Erasing data.

Employee access abuse: Inappropriate use of computer system access by an employee.

Financial fraud: The use of deceit or trickery to embezzle money.

Hacking of phone/PBX: Same as Telecomm. Fraud (see below).

Information loss: Removal of information possession by theft, modification or destruction.

Insider abuse of net access: Inappropriate use of network access by someone unauthorised to use the network.

Leak of proprietary information: Same as theft of propriety information.

Manipulation of software apps: Unauthorised modification of software applications.

Manipulation of systems software: Unauthorised modification of system software.

Sabotage of data networks: Destroying data or suspending the function of a network.

System penetration by outsider: Unauthorised access to a computer system obtained by someone not affiliated with the systems owner.

Telecomm. eavesdropping: Unauthorised observation of a telecommunication transaction.

Telecomm. fraud: Theft of telecommunications services.

Theft of computer resources: Using a computer /network for unauthorised activities.

Theft of data, trade secrets: Same as theft of proprietary information.

Theft of proprietary information: Unauthorised taking of sensitive or confidential data.

Trojan horse: A hidden software module that can be activated to perform an unauthorised task; a form of a computer virus.

Unauthorised access by insider: Computer system or data access obtained without proper permission from the system administrator by someone affiliated with the system owner, but not given permission to access the penetrated system or data.

Unauthorised access by outsider: Computer system or data access obtained without permission from the system administrator by someone not affiliated with the system owner.

Unauthorised network entry: Network access obtained without first receiving proper permission(s) from the network administrator.

Virus contamination: Computer system infection by a computer virus.

The following is a set of common IT security technology terms:

Access control: Policies, procedures and mechanisms by which users are authorised and granted privileges to use computer systems and networks.

Anti-virus software: Computer programs that detect the presence of and remove known viruses in a computer system.

Basic user password: Common password access control technology. Users present a users name/id and a password of their choosing to gain access to a computer system.

Biometric authentication: The use of biologically distinct measures to prove user identity, for example, finger print scans, retina scans, etc.

Digital certificate: A form of digital identification in which a certificate authority vouches for the identity of the certificate presenter.

Disaster recovery: Policies, procedures and mechanisms by which the functionality and data of a computer systems and network can be restored after a disaster.

E-mail security: General security policies, procedures and mechanisms to protect e-mail confidentiality, authenticity and integrity.

Encrypted file: Use of cryptographic techniques to scramble a file, thus denying anyone without proper key access to its contents.

Encrypted login: Use of encryption to scramble identification, authentication and authorisation communications.

Encryption: Application of cryptographic techniques to scramble data so that only the proper key holder(s) may unscramble it.

External certificate authority: Use of an outside organisation to vouch for digital certificate presenters.

Firewalls: Specialised routers that filter network traffic between two networks, effectively separating the networks.

Hardware authentication: The use of hardware addresses or some other form of hardware identification to vouch for a user's identity.

Internal certificate authority: Use of digital certificates where the organisation vouching authority is a division within the same organisation.

Intrusion detection systems: Software applications that monitor computer and network activity for computer attacks, enabling them to detect incidents as they occur and sometimes prevent damage.

Multiple logons & passwords: Permitting more than one user on a computer system, using user name and password combinations for access control.

One-time passwords: Passwords that can only be used once.

PC access-control software: Use of software on a personal computer to control the granting of user privileges on that personal computer.

Reusable passwords: Passwords that can be used by their owners multiple times.

Single sign-on: Use of an access control system whereby a user is granted privileges on multiple computer systems by presenting credentials once, such as username and password.

Smart cards: Electronic cards that can be presented or scanned into a system as proof of identification.

Terminal key locks: A physical key that must be inserted into a computer terminal before the terminal will function.

Adapted from Soo Hoo, 2000

2.6 Types and Levels of Computer Security

Computer security is often divided into two distinct categories; physical and logical. As the term implies, physical security addresses a person's ability to physically access computing facilities such as: terminals, printers, telecommunications equipment and data centres. Additionally, computer users can have logical access to information systems. For example, this will cover some specific technologies such as passwords, tokens and digital signatures.

2.6.1 Physical and Logical

Computer security has taken on a whole new meaning in the Information Age. Organisations can no longer attempt to control business assets solely by using physical controls. Popular physical controls include: locked doors, burglar alarms, and security guards. A short list of ten common physical control mechanisms is shown in Table 2.10 below:

Table 2.10 – Ten Popular Physical Control Mechanisms

Number	Physical Control Mechanism
One	Posted Security Personnel
Two	Central Alarm Systems
Three	Closed Circuit Television (CCTV)
Four	Access Cards and Readers
Five	Workstation and Laptop Computer Locking Devices
Six	Locked Entrance and Exit Facilities
Seven	Biometrics
Eight	Smart Cards
Nine	Locked Floppy and Hard Disk Drives
Ten	Peripheral Alarm Systems

Physical controls are important since they help to convey an attitude towards IT security. While they are important, there are other security methods as well.

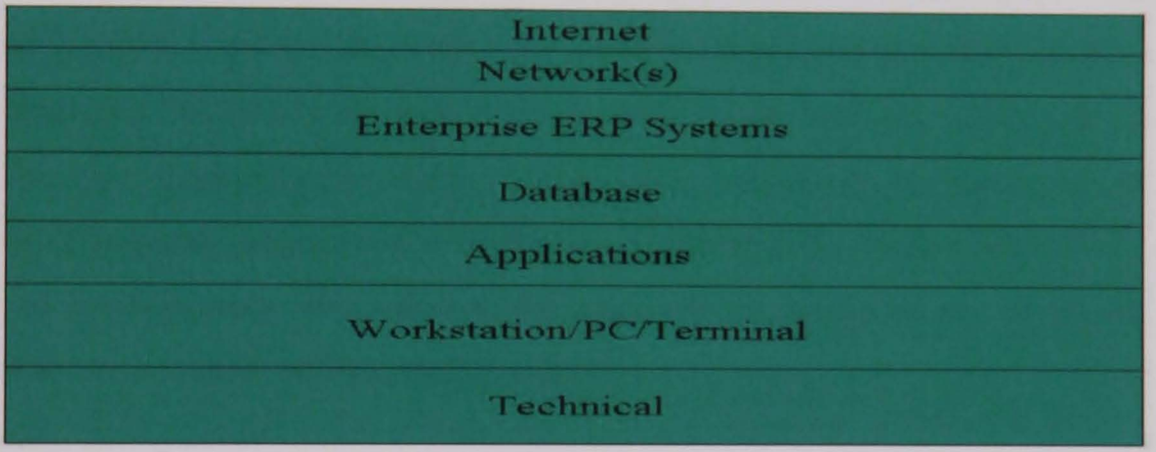
2.6.2 Hardware and Software

Computer security can also be viewed as being hardware or software related. Hardware security is enforced through the use of physical controls, whereas software security is driven by the use of logical controls. Normally, hardware controls are used in data processing centres and individual computing devices. Logical controls are native and specific to individual operation systems, databases and software applications.

2.6.3 Logical Levels of Computer Security

There are various levels of logical computer security. Within an organisation, user rights will need to be assigned for each logical level of security. This is illustrated graphically in the following diagram:

Figure 2.9 – Logical Levels of Computer Security



Furthermore, the functional access that each user has to a particular system can be refined by limiting individual user rights. This can be done at the system, application, menu or transaction level depending on the individual system. Common user abilities include: read only, write, read/write, delete, and move.

2.6.4 Internet Security

Internet security is perhaps one of the most complicated areas of computer security (Gollmann, 1999). One of the main reasons for this is the tremendous growth of the World Wide Web. Embedded software tools like Java applets and CGI scripts create active content which is launched upon logging on to a web site or executing a particular feature within it. The Internet's architecture also makes it difficult to identify the true origin of transmission as well as the actual, specific physical location of the connected device. Furthermore, web browsers allow users to 'surf' the Internet and they can easily activate cookies, small text files that store personal information as well as different types of computer viruses.

This level of computer security is also complicated by the fact that there is currently no global legal framework. Therefore, when security breaches transpire legal proceedings are not always effective (Metchnick, 1997). Web based material can be easily copied, as well. This makes intellectual property protection very difficult. Corporate information assets such as computer software, trademarks and artistic works are particularly vulnerable to theft and abuse (Gollmann, 1999).

2.6.5 Network Security

Network security typically focuses on three core areas: confidentiality, integrity and availability. Since networks are at the core of distributed computing environments, and allow large companies that ability to input, process, store and retrieve information this is a critical area. This type of security also utilises IT protocols and the OSI Reference Model. Due the diversity of network architectures, as discussed primarily in Section Two there is a wide variety of considerations that need to be made by an organization. Typically, risks in network security include sniffing and spoofing.

Sniffing involves an unknown party 'listening' on the network (Maiwald, 2000). This listening can involve undetected e-mail transmissions, free-text user id and password details and other valuable communications. A sniffer is an inexpensive hardware device that can connect to a network at a number of different physical locations. This also makes the detection of such activities difficult for information security officers and network administrators.

Spoofing is an information technology method of masquerading. It allows one user to impersonate another user or pretend to be an external party. This can also greatly complicate the information security enforcement and detection processes.

2.6.7 Enterprise ERP Systems Security

One of the major results of the Year 2000/Millenium Bug crisis was the growth of Enterprise Resource Planning (ERP) systems. Instead of seeking a remedy for the thousands of lines of programming code in their various applications: many organisations found it more efficient and effective to replace their legacy systems with ERP systems. During this time, products such as SAP R/3, PeopleSoft, JD Edwards, BAAN and Oracle Financials became very popular.

One of the concerns with ERP systems is the tight integration of its multiple software modules. From a practical perspective, in order to implement these systems before January 1, 2000 some of these projects were done very quickly. ERP systems are also well-known to be highly complex. Therefore, the security aspect(s) of these systems are inherently complicated.

2.6.8 Database Security

Database security is yet another facet of computer security. The main issues within this area typically involve restricted access control and methods of retrieval (Gollmann, 1999). Individual user rights need to be appropriately restricted based on job duties. Retrieval methods should also be tightly controlled to prevent accidental or intentional data corruption and theft.

Another important issue is the functional abilities of the Database Administrator (DBA). This individual (or group thereof) has responsibilities that cover database access, user set-ups and concurrency controls. Since there may be a tendency to give excessive controls to DBAs and this area is typically investigated in a database audit.

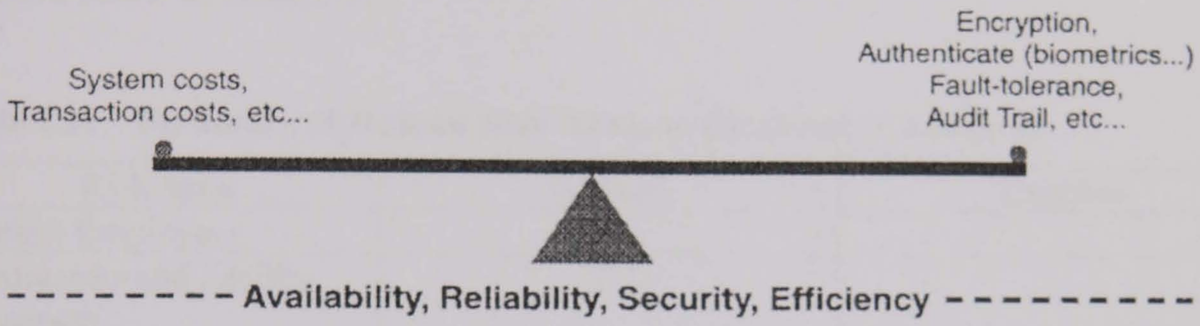
2.6.9 Application Security

Application security focuses on the detailed security parameters within a specific software product. It is dependent on the security capabilities and features build into the software when it was developed. For instance, some applications allow for detailed security settings while others do not. Application security typically covers access controls, transaction processing and file permissions.

2.7 Risks in the Electronic Commerce Environment

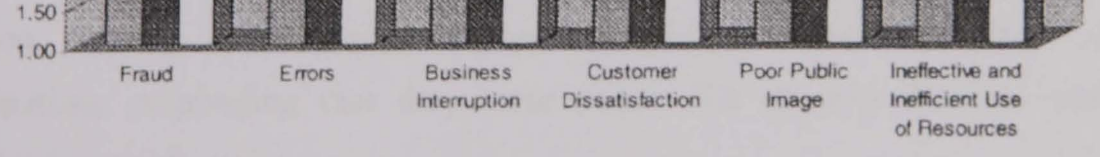
There are various ways of segmenting the types of risks faced by organizations operating in the Electronic Commerce environment. Parker (2001) proposed a relationship between different types of costs and control techniques. This is described further in Figure 2.10 below:

Figure 2.10 – E-Risks According to Parker


System costs,
Transaction costs, etc...
Encryption,
Authenticate (biometrics...)
Fault-tolerance,
Audit Trail, etc...
- - - - - - - - Availability, Reliability, Security, Efficiency - - - - - - - - -

Parker expands this research idea by providing information on a survey conducted by the Institute of Internal Auditors, Inc. regarding IT vulnerabilities. A high-level summary of this information is shown in Figure 2.11:

Figure 2.11 – Early Concerns about E-Commerce Vulnerabilities



IIA/CREC 1998 Internet Effects on Business Controls Survey
Data Source:Center for Research in Electronic Commerce

97%/182 respondents

Various authorities (Parker 2001, Davies, 2000 and Marcella Et. Al., 1998) indicate that there are a wide variety of risks in Electronic Commerce. It appears easy to broadly classify these risks into two general categories: human and technical.

2.7.1 Human Risks

Human risks transpire from devious intentions and unintentional errors. Some sociologists have studied the field of human behavior to formulate ideas as to why people intentionally deceive other people and carrying out malicious activities. A summary of these risks is provided below in Table 2.11:

Table 2.11 – Summary of Human Risk Areas in Electronic Commerce

Risk Area	Internal	External
Current Employees	XX	
Contractors and Facility Managers	XX	
Customers/Clients		XX
Service Providers		XX
Former Employees		XX
Former Consultants		XX
Hackers		XX
Organised Crime Groups		XX
Terrorist Organisations		XX
Competitor Firms		XX
Social Action/Pressure Groups		XX
Roque Nations		XX
Other(s)	XX	XX

Current employees may intentionally attempt to alter systems or steal data in vengeance for some type of work related conflict. This situation may occur due to a missed promotion, low compensation structure, or workplace conflict. In fact, a recent survey on computer crime indicated that most malevolent activities related to IT are actually perpetrated by insiders (Gordon, Et. Al., 2006, Computer Security Institute, 2000) with seventy percent of the organizations responding that they were aware that security breaches occurred in their organisations in the previous year.

Backhouse Et. Al. (2004) provides an excellent analysis of the perceived risks related to cyber crime and security. Their research which was supported by the UK government specifically supports the fact that the Internet is an attractive venue for crime because of its great pool of opportunity for criminals. In addition, stakeholders and social actors have different perceptions of risk such that trust, openness and objectivity are essential elements to risk management in cyber security.

Contractors and consultants may be actively involved in the organisation on a day-to-day basis. Often, companies that are experiencing financial difficulties, defer the recruitment of permanent staff member. In this situation, one practical solution is to utilise personnel from temporary staffing firms. As well, consultants may be working on-site over an extended period of time.

Frequently, consulting and public accounting firms will have staff at the client's premises for months at a time. This is particularly true with large-scale audits and system integration projects. These individuals often have access to sensitive systems and information as part of their responsibilities. Another important internal human risk area is facility managers.

With the rise in outsourcing over the past ten years, some companies have a large number of contractors working on-site for lengthy periods of time. These personnel are actually employees of other companies hired to manage the daily operations of one or more internal departments. In addition to the internal risks, there is a variety of external risks as well.

External risks can evolve from former employees, contractors and consultants, as well as various groups of information warriors (Denning, 1999). Taylor (2000) provides great insight to a popular group of outsiders known as hackers. In fact, he explains that four generations of hackers have been identified. The first generation of hackers, were involved in the earliest stages of computing back in the 1950s and 1960s. The second generation of hackers came about in the rise of the personal computer. The third generation of hackers were computer programmers who spent too much time playing computer games. Finally, the fourth group are those individuals that illicitly attack other people's computers for financial gain or thrill. In his research, Taylor (2000) uses terms like cyberpunks and microserfs to describe hackers and believes that most hackers are nerdy, geeky and obsessive. Nevertheless, they are not the only group to contend with.

Organised crime is another external risk to information technology. Through influence and pressure these groups seek to take advantage of others. They also seek to profit from illegal activities such as: money laundering, drug sales, prostitution and gambling.

Terrorist organisations, rogue nations and political/social action groups also pose threats to the critical infrastructures. According to Denning and Baugh (2000) and Schwartau (1997) the Internet is an attractive mechanism for these groups. Terrorists groups can be either internal nationalists/extremists or foreign terrorists (Williams, 1997 and Carlson, 1995). No matter where they physically reside, the Internet provides an inexpensive tool for destruction. Rogue nations are classical enemies of a nation, for the United States a few examples can be easily identified: Cuba, North Korea, China, Libya and Iraq. While these countries may pose a traditional military threat, they may also pose an information warfare threat as well (Denning, 1999). Lastly, political and social action groups motivated by their own agenda also pose threats.

Specific to the field of cyber security, Vatis (2001) developed a predictive study model for the war on terrorism using a case study approach. His work focuses on four potential geopolitical sources of cyber attacks: terrorist groups, terrorist sympathisers, targeted nation states and thrill seekers. The main case studies in this project were the conflicts between: Pakistan and India, Israel and the Palestinians, Former Republic of Yugoslavia and NATO in Kosovo and the U.S. - China Spy Plane incident. In this study, the following main types of cyber attacks were discussed: web site defacements, domain name service attacks, worms, routing vulnerabilities, infrastructure attacks and compound attacks. The recommendations from this research indicated an increased need for government attention to potential attacks on the U.S. National Information Infrastructure.

When taking all of these internal and external groups into consideration, the complexities of computer security related to individual organisations and the U.S. critical infrastructure should be apparent.

2.7.2 Technical Risks

As was the case with human risks there are number of different risks posed by the technical aspects of information technology. In some cases, technical risks result from initial human risks. Furthermore, while most of these risks are not new, it is merely the different types of technologies and related safeguards that need to be implemented to mitigate the associated risks. From the perspective of the major cyber security information communicated by the NIPC in their CyberNotes newsletters, the following five main technical risks are addressed:

First, Software Bugs are errors in the computer program (i.e. operating systems or application software) which causes the program to not perform as intended. Most software bugs are attributable to the software source code and result in design or compilers processing errors. Normally, computer programmers use a variety of techniques referred to as de-bugging to perform quality assurance and other tests on the software code. Some common types of software bugs are: buffer overflows, race condition errors, memory leaks and stack errors.

Buffer overflows causes memory processing errors. An extra portion of programming code is running such that the program results in the program extending beyond its pre-defined buffers. Race condition errors are the result of the output of the process is unexpectedly and critically dependent on the sequence or timing of other system events. It derives its name from the signals engineering field. Memory leaks refer to unintended memory errors in the computer program. Lastly, stack errors when identified are typically found in operating systems (adapted from Trope, 2005, Karestand, 2003, Thompson, 2002, and Vatis, 2001)

Cifuentes, Waddington and Van Emmerik (2002) studied the errors of software bugs through decompilation and high-level debugging. Their research found that an extensive debugging process will reduce the time required to detect security flaws in computer programs. Another prior study by Chillarege, Kao and Condit (1991) addressed the issues of software defects and the growth of software development processes. This research is linked to the field of software engineering which is analysed in detail by Whittaker (2000) who explains the various complexities of software testing which include: time constraints, tester's skill, interface difficulties and user testing environment problems.

Second, Exploit Scripts are purpose built program scripts that attack specific vulnerabilities in computer software (Adapted from Karestand, 2003). Sometimes these can be generated by computer code generators (Thompson, 2002). Current, common scripting languages include PERL, Visual Basic and Java Script.

Third, Viruses are common form of malware and were studied early on by Cohen (1987 and 1988). Karestand (2003, p. 42) quoting earlier researchers, defines a computer virus. as "a computer program that is able to replicate by attaching itself to other computer programs in some way. The program the virus attaches to is called a host or victim program".

Fourth, Trojans derive their name from the Trojan Horses of ancient times. This type of malware can pretend to be a piece of legitimate (e.g. trusted) software. but yet has a destructive mechanism or function that can be activated. Often this is done by a remote user (Vatis, 2001, Cramer and Pratt, 1989).

Fifth, Probes and Scans refer to external attempts to analyse a program, computer hardware or network.

2.7.3 Data Risks

Company data and resulting information is vital to an organization. Its accidental or deliberate destruction or theft can expose the company in a variety of ways. First, the company managers could not have the data they need to make important business decisions. Second, the data could be shared with a competitor or external party who may be capable of exploiting it in some fashion. This is particularly dangerous in terms of sensitive company information such as: intellectual property assets, customer and employee information, and product formularies.

Another concern related to the loss and theft of data is that if it is truly lost, than it may never be recovered. Depending on the criticality of the information this could have dramatic affects on the organisation. Hackers and other outsiders may also be very difficult to apprehend due to their decentralised locations (Blume, 2000 and Cohen, 1995).

2.7.4 Mechanical Failures

Mechanical failures pose a significant threat to organisations. IT systems are not one hundred percent failproof. Unpredictable environmental changes, volatile electrical currents and internal device failures (i.e. hard drives crashes) are all realistic situations. Preventative maintenance, spare parts and environmental controls help mitigate these technical risks (Warren, Edelson, and Parker 1997 and Karake, 1992)

2.7.5 Malware

Malware is a comprehensive term covering a variety of different malicious forms of computer software. Included in this category are: computer viruses, worms, bacteria and Trojan horses. Computer viruses are the most popular form of malware and popular viruses have received a lot of discussion in the information systems field.

Bergel (2001) discusses the impact of one such powerful Internet worm known as Code Red which was launched in July of 2001. Astonishingly, it spread to 250,000 systems in just nine hours. He further explains that Internet worms account for approximately eighty percent of all malware incidents. Also, new viruses are launched every day and according to figures published by McAfee Corporation, a leading anti-virus software vendor there were over 57,000 known computer viruses at the end of 2003.

With the growth of mobile computing and personal digital assistants, a new generation of handheld viruses has emerged. Foley and Dumigan (2001) discuss the threats that these types of viruses possess. The first known PDA virus, "Liberty", which was discovered in August 2000 it deleted all applications stored on the popular Palm® PDA. Further information indicates that as the use of PDAs expand through new services and new applications specifically designed for these types of devices, there is an increased likelihood for more specific purpose malware. The following table is a compiled list of useful web references for malware tracking and incident information:

Table 2.12 – Common Sources of General Computer Malware Information

	Organisation	Web Site Address
1.	Trend Virus Encyclopedia	www.antivirus.com
2.	WildList Organisation International	www.wildlist.org
3.	Sophos Anti-Virus	www.sophos.co.uk
4.	McAfee Associates	www.mcafee.com
5.	Symantec Corporation	www.symantec.com

Recently, there have been a number of pervasive, powerful and destructive computer viruses. Some of examples of which are the: ILOVEYOU, Melissa, Naked Wife and Anna Kornokova viruses. Many of these viruses spread rapidly through the Internet do to the virus file being attached to e-mail messages. Costs associated with the ILOVEYOU virus were estimated to be seven billion U.S. Dollars (Ohlson, 2000). Other variations of full-fledged viruses include bacteria and worms. These variations can also be very destructive and disruptive.

There are a number of popular commercially available anti-virus software packages. While it is critical to have this software loaded on workstations and servers: it is also important to make sure that this software is updated regularly. By doing so, you help ensure that you are protected against new computer viruses and related variants.

2.7.6 Denial of Service Attacks

Denials of Service (DOS) attacks are particularly important to web-based businesses. In essence a denial of service attack is overflowing of a computer system with more data then the system itself has the capacity to manage. This situation often forces system administrators to shut down their E-commerce systems and web sites until the proper protection can be implemented. During February 2000, a very serious set of DOS attacks assaulted eBay, CNN and Amazon (Harrison, 2000). While it was difficult to quantify the total direct costs of these attacks, the situation was to many in the industry a wake-up call that active information sharing and cooperation is necessary (Pappalardo, 2000).

In terms of critical infrastructure, a large denial of service attack could have truly devastating results. For instance, what would happen if fire, ambulance and police services could not have respond to emergency response systems were disabled by a denial of service attack? Or, if the public telephone system, water supply or banking systems were disabled or destroyed?

2.7.7 Other Risks

There are a wide variety of additional general business risks that are also relevant to E-Business organisations. While common to other traditional organisations it is worthwhile to acknowledge that these risks are also evident. These include: sociological, criminal, political, economic and legal issues.

2.7.8 Sociological and Criminal Issues

In the field of computer security. it is important to consider non-technical issues that also impact this broad field of study. Applied sociologists have studied the impact of computer usage on society. Criminologists have considered the roles of the public and private sectors in crime control and criminal justice. White and Witt (2001) describe how the World Bank seeks to promote economic development and formal national governments formulate laws to foster political and economic stability. In less formal societies, other issues such as customs and family stature effect crime. Additionally, they explained that crime is different from other illegal acts because the injured party is not only the victim, but rather other members of society. In some types of crime such as computer crime this situation will likely be made more complex because the perpetrator identity may not be known. Using the Federal Bureau of Investigation (FBI)'s Uniform Crime Reports the researchers conclude that most criminal activity is conducted by young males. They also point out that it is very difficult to discuss the complete impact of crime since there is a large amount of underreporting, such that the total magnitude of the criminal activities cannot be accurately and completely assessed. Forensic Economists seek to calculate the impact of criminal behaviours (Ireland, 1997). With computer crime on the rise, one study found that it reached one trillion dollars as early as 1999 (Neeley, 2000).

Compounding this trend is the fact that some authorities believe the United States is ill prepared to deal with cyber criminals (Carlson, 1995). Shelly (1998) and Polat (1999) discussed the impacts of transnational crime and corruption in financial services, encryption and child pornography. One of the main points described was that the Information Age has created a global economy without a robust, far reaching criminal framework. As such, basic issues like prosecutory powers and jurisdiction become inhibitors to law enforcement agencies (Polat, 1999 and Shelly, 1998).

2.7.9 Economic and Political Issues

Cultural practices have also been found to have an impact on information systems. Husted (2000) studied the relation of national culture on software piracy using economic development, income inequality and various cultural variables. In the beginning of this study data supplied by the World Bank and Business Software Alliance was used. A thorough discussion of the underlying issues of fear of punishment and national wealth are discussed; and it appears that culture is a contributing factor to software piracy. While protections for intellectual property issues seem to be more of an issue in Western culture and help promote economic growth, the researcher illustrates that Gross National Product (GNP) per capita is significantly correlated to software piracy. Could these issues also relate to information systems security? Some of these economic factors will be considered for further study in this research project.

Hodson, Englander and Englander (1999) studied the ethical, economic and legal aspects of employers monitoring their employee's e-mail. This highly controversial topic is a relatively recent phenomenon and is very important given the growth of e-mail in the workplace. Citing a previous study conducted in 1997 by the American Management Association that found fifteen percent of major companies review employees e-mail and computer files. At the core of their discussion is whether or not it is ethical for employers to engage in this type of activity even though employees may be violating company policies and legal statues. While no definitive answers or solutions are given by the researchers; it is still interesting and may have some application to future research studies.

Other legal issues related to computer security are diverse and often complex. Regulation has been cited as a major obstacle to the development of a number of services on the Internet (Casson, 1997). Privacy, regulation, and the rights of government are still being formulated and debated in many countries across the globe.

2.7.10 National Security and Public Policy Issues

One of the primary roles of government is to develop laws that promote the security and advancement of society. The United States has prided itself on the value of democracy which include freedom of speech, privacy and free elections. Like other national governments the U.S. takes its national security very seriously and implements public policies and laws which support its moral foundations and tactical objectives. One important issue for national security has been terrorism. Its threats have been countered by a longstanding policy of deterrence (Kieffer, 2001 and Schnaubelt, 2000).

With the recent launch of President Bush's War on Terrorism. the United States feels that its systems are vulnerable to attack. Olson (2000) indicates that over seventy-five percent of military communications are conducted using information systems. This illustrates the very high reliance our government has on information systems.

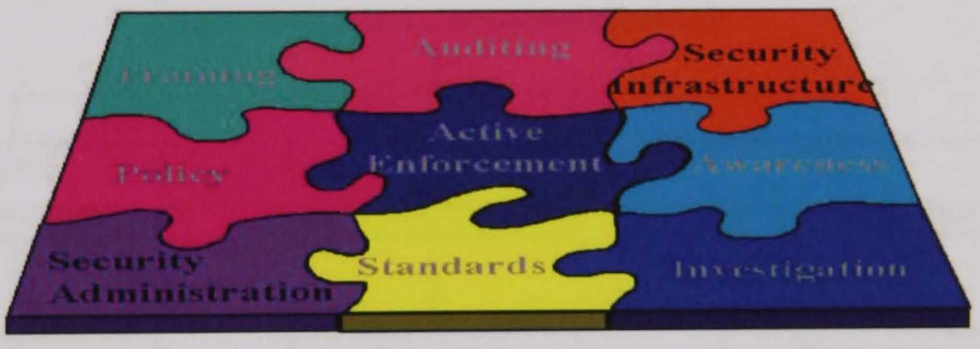
Another important area to address is the relationship companies in the private sector have the government. Blain (2000) citing *Hegel's Theory of the Modern State* and Friedmann's *The State and Rule of Law in a Mixed Economy* explained that according to Hegel that the nation state is one of necessity and exists as the pinnacle of individual freedom. For Friedmann. the government is like the owner of society and therefore must regulate its affairs. These differing views are useful to consider in a democratic nation state like the USA. Contrary views from Marxist and Communist theory are not specifically relevant to this research study.

2.8 Risk Management

The modern business world and society, as a whole, needs to be confident that the various types of risks previously described are effectively managed. Risk management is not a simple discipline, and it involves many considerations which are made more complex in the age of Electronic Commerce.

The inherent nature of global E-Business presents a number of challenges to effective E-Commerce Security. This area of research is not merely a short-listing of computer security issues found in other areas such as networks and the Internet. Rather, it is a consideration of all facets of computer security. This was best depicted by a leader in the E-Commerce Risk Management practice at PricewaterhouseCoopers, LLP, as follows:

Figure 2.12 – The Electronic Commerce Security Jigsaw Puzzle



Source: Joe Morris, 2000

Nevertheless, with all the complexities that exist; organisations need to find tools and techniques to manage these risks effectively.

2.8.1 IT Risk Management

Why do information technologies require effective management and control? First and foremost, this is the basis from which most EC companies operate. Risk management has a variety of definitions, applications and scenarios. However, one highly accepted formal definition of is risk (Hoo Soo, 2000, p. 5 and Kumamoto and Henley, 1996, p. 2) is as follows:

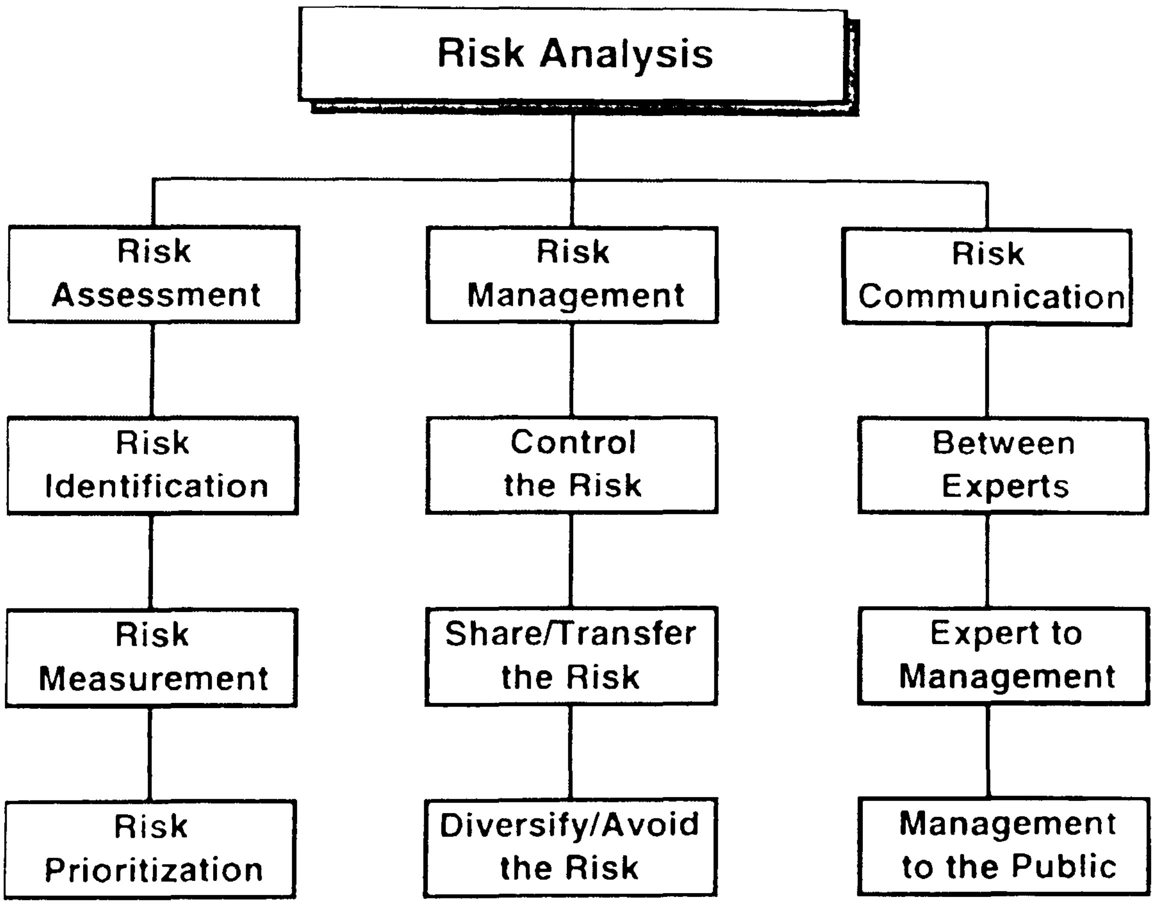
$$Risk=\{L1, O1).....(Li, Oi).....(Ln,On)\}$$

Where:

O = A set of ordered pairs of outcomes, and
L = Their associated likelihoods of occurrence

According to McNamee and Selim (1998) in their study, *Risk Management: Changing the Internal Auditor's Paradigm*, particular emphasis dealt with the fact that effective risk management begins with proper risk analysis. An overview of risk analysis is portrayed in the various risk analysis components shown in Figure 2.13 below.

Figure 2.13 – A Risk Analysis Approach from Internal Auditing



Source: McNamee and Selim, 1998

The three key sub-categories of risk are by themselves multi-facetted. Furthermore, risk assessment is the initial process within risk management and can be undertaken from different perspectives. Table 2.13 below provides a basic comparison of the three methods described:

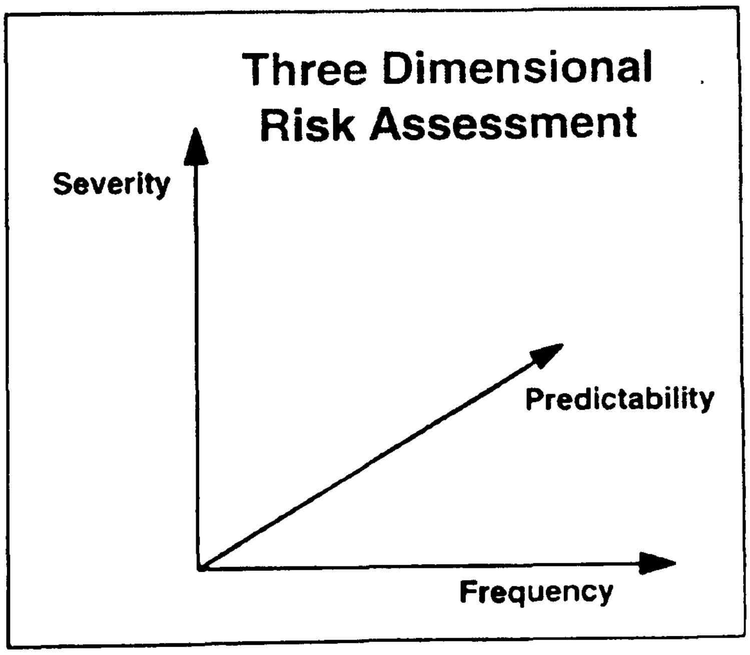
Table 2.13 – Three Approaches to Risk Assessment

Approach Orientation	Major Considerations
1. Asset	Asset size, location, type and portability
2. External Environment	Economic, political, financial, technology, regulatory, and customers etc.
3. Threat Scenario	Natural disasters, man-made disasters and fraud

Source: (Adapted from McNamee and Selim, 1998)

These researchers also support the notion that internal auditors in particular and other personnel in general can measure risk in different ways. Typically, risk was measured in highly discrete terms and had solely negative conations. But in reality, risk also presents attractive opportunities to an organisation, such as additional profits, the development of new technologies and increased market share. They argue that risk can be measured in terms of severity, predictability, and frequency as depicted in the following figure:

Figure 2.14 – Three Dimensional Risk Assessment

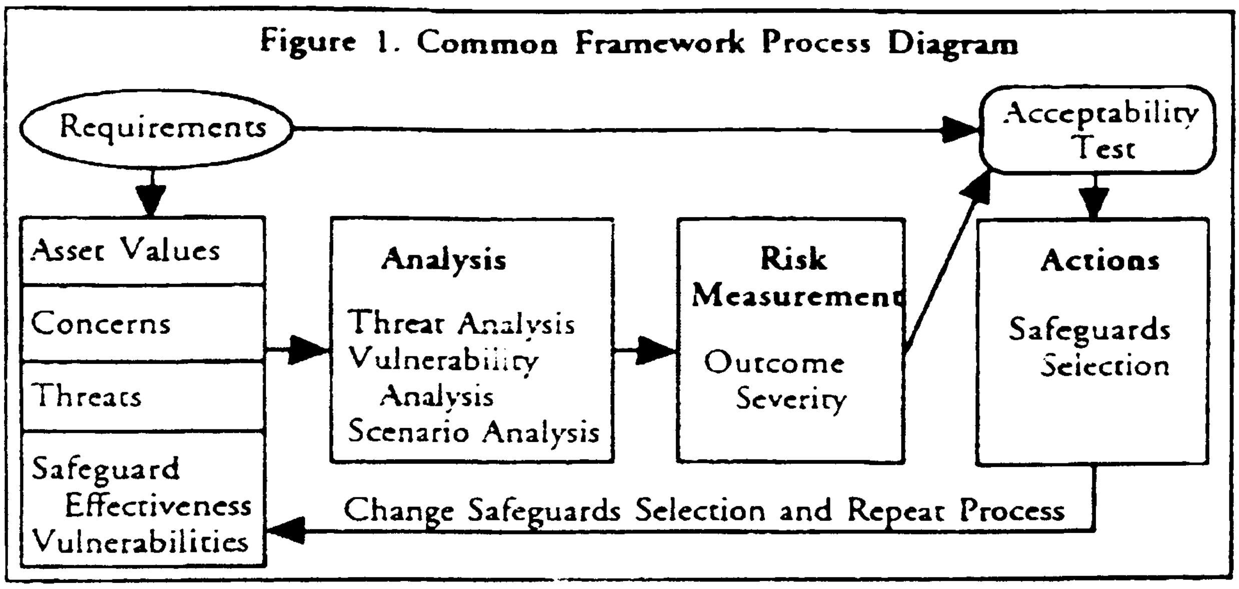


Source: McNamee and Selim, 1998

Risk management involves an on-going process to address the various types of risks in an enterprise. It is not merely insurance coverage or financial hedging, but rather it should be a continuous effort within the company. Furthermore, risk communication addresses the feedback and dissemination about risks that should occur in an organization. Effective risk communication is a core component of a risk management program.

Hoffman and Hung (1989) developed a specific risk management model for computer security. This is illustrated in the following figure:

Figure 2.15 – Common Framework Process Diagram in Computer Security



The framework had seven basic elements:

Requirements: R $\equiv$ $[R_1, R_2, \ldots, R_j]$
e.g., expected Loss < $100K, expected Loss < $1M

Assets: A $\equiv$ $[A_1, A_2, \ldots, A_k]$
e.g., hardware, software, data

Security Concerns: C $\equiv$ $[C_1, C_2, \ldots, C_n]$
e.g., confidentiality, integrity, authenticity

Threats: T $\equiv$ $[T_1, T_2, \ldots, T_m]$
e.g., human, natural

Safeguards: S $\equiv$ $[S_1, S_2, \ldots, S_p]$
e.g., physical, system, communication, admin.

Vulnerabilities V $\equiv$ $[V_1, V_2, \ldots, V_q]$
e.g., physical, software, hardware, administrative

Outcomes: O $\equiv$ $[O_1, O_2, \ldots, O_r]$
e.g., combinations of A, C, T, S, V

The framework also included three associated quantities:

Asset Values: $A_{val} \equiv [A_{1val}, A_{2val}, \ldots, A_{kval}]$

Safeguard Effectiveness: $S_{eff} \equiv [S_{1eff}, S_{2eff}, \ldots, S_{peff}]$

Outcome Severity $O_{sev} \equiv [O_{1sev}, O_{2sev}, \ldots, O_{rsev}]$
e.g., ALE of the outcome, qualitative judgment

Adpated from Soo Hoo, 2000

While the above noted model is useful; it is also important to note that some underlying elements and quantities may be difficult to estimate. From practical experience this is particularly true of vulnerabilities and safeguard effectiveness.

Research by Soo Hoo (2000) used data from the *1999 Annual FBI/CSI Computer Security Survey* to examine computer related risks. First, a history of computer security risk modelling was presented. Building upon Annual Loss Expectancy (ALE) models a new decision analysis-based-ALE is discussed. This is done in order to develop an approach to IT risk management recognising the traditional approaches to risk management.

2.8.2 Risk Avoidance

Is it possible for an organisation to avoid risks? In the field of finance, students are educated about a core concept known as the risk-rate relationship. Put simply, this principle dictates that the greater the risk the greater the possible reward. I believe that the same condition is true within Electronic Commerce.

If an organisation absolutely avoids risk by being extremely conservative (e.g. risk adverse) in their business practices than they will likely achieve minimal incremental rewards. Conversely, the inability of an organisation to move quickly and take action can have lasting detrimental affects. Therefore, there are risks in both diametric extremes.

2.8.3 Risk Transfer

Given the fact that not all risks can be absorbed or managed internally by an organisation, one other approach is risk transfer. In risk transfer, a risk in its totality or partiality is transferred to another entity. For example, an E-Commerce organisation may use a third party Application Service Provider (ASP) to process daily business transactions and accounting services. Since the EC entity determined that they themselves were not going to process this data, the risk of ensuring the accuracy and timeliness of this process rests with the ASP.

It is important to emphasise that although risk has been transferred to another organisation the E-Commerce company still faces some risks. For instance, what will happen when a natural disaster occurs or when an ASP goes bankrupt?

2.8.4 Risk Sharing

Some times risks can be shared. For example, in a joint venture risks can be shared based on a pre-determined formula between the shareholders. Also, some risks can be shared by outsourcing business functions to another organisation. Losses from operations can be shared by the company and the third party service provider organisation. Internal controls of all variations can assist the owners and managers of an entity in achieving their goals and objectives. In the auditing profession, there are various types of control frameworks and internal controls. Specifically relevant to the field of information technology are management controls and technical controls.

2.8.5 Management Controls

Management controls are those traditional internal controls instituted by the management of a company. Typical objectives of an internal control structure include: accurate financial reporting, efficient use of resources and safeguarding of assets (Weber, 1999).

Government and industry standards are not immediately apparent in all areas of information technology. Rather they evolve over time and seek to promote better operating practices. Ideally, this leads more reliable and secure service that is valued by the business community and individual consumers. These allow an individual at one client say in Baltimore, Maryland to successfully send data across the Internet to another client in London, England with only a small chance of the transmission failing or getting corrupted en route.

Industry standards relevant to computer security have been developed by a variety of international organisations. These groups include; the International Standards Organisation, World Wide Web Consortium (WWWC), United Nations, Organisation for Economic Cooperation and Development (OECD) and the World Bank. While these diverse organisations have different specific goals many of the lower-level objectives are similar.

Some national governments have also been progressive in developing computer security standards and regulations. The United States, United Kingdom, France, and Japan have been very active in this regard. A good example of a non-U.S. national standard is BS7799 – Part One: Code of Practice for Information Security Management and Part Two: Specification for Information Security Management.

Formal organisational policies and procedures are commonplace in most medium and large entities. Small organisations normally operate informally, so written and detailed policies and procedures are not as practical. These control tools help provide direction and clarity to different practices in the company. From an IT perspective, common policies include password change parameters, e-mail privacy and Internet usage

2.8.6 Technical Controls

In the past, attacks on company facilities were generally carried out in physical terms such as theft, spying and destruction of property. With the advent of information technology new attack methods have emerged. These include computer hacking, computer viruses and e-mail spamming. The computer and telecommunication industries continue to respond to these threats by developing improved preventative and detective mechanisms that include: firewalls, anti-virus software, encryption, and biometrics.

Certificate Authorities (CAs) are typically external organisations that provide a method of authenticating a user. It is also possible to maintain an internal CA if desired and warranted by business needs. A certificate is a unique identifier for an individual user. By using such a mechanism encryption keys can be managed to maintain a list of approved users and a hot list of unauthorised users who should not have access to specified resources. The primary functions of the CA are to manage these keys and prevent unauthorised access. By placing this responsibility in the hands of a trusted third party businesses can devote more of their resources to core business functions. Leading commercial certificate authorities include: VeriSign, IBM, GTE and the United States Postal Service (USPS). When using the Internet to conduct Electronic Commerce an important method of protecting company information during transmission through this public network is encryption. The International Telecommunications Union (ITU) published standard X.509 which covers certificates, the authentication framework and related management procedures.

Since Roman times encryption has allowed one party to scramble data into an unrecognisable format to prevent it from being understood by an outside party. After the information is encrypted it must be decrypted to convert the jumbled data back into meaningful information.

While this process was originally done using a simplistic substitution method today complex mathematical algorithms are used.

The more complicated the algorithm the more secure the data is. This also impacts the time it should take someone to crack code. In the United States, the federal government controls the regulations embodied in the Data Encryption Standard (DES). This legislation provides for a maximum of 56-bit encryption, which many industry observers believe is not sufficient for modern day communication. In fact, many U.S. based companies have argued that they would like to re-locate outside of the U.S. in order to take advantage of more liberal encryption standards (e.g. longer and more complex algorithms), which are allowed in Europe and other areas of the world. The main argument put forth by the U.S. government is that more complicated encryption would delay the decryption of data that might be needed by law enforcement agencies such as local police departments, the Federal Bureau of Investigation (FBI) and Secret Service.

The popular U.S. encryption standard, DES3/AES had previously encountered a tremendous amount of controversy. Law enforcement officials felt that the use of this technology who prevent or at least limit their investigative abilities. Because of extensive private industry pressure it was ultimately permitted for commercial use in the United States. Commonly referred to as 'triple DES' since it provides for a maximum of 168-bit encryption (three times the standard DES key length), it fundamentally allows for more secured transmissions due to the longer key length. Some of the popular commercially available encryption products include: RSA, IDEA, PGP and Kerberos.

Biometrics can be either physiological or behavioural and have various degrees of success. Examples of physiological biometrics include: iris, face, palm print and fingerprints. Additionally, voiceprints, handwritten signatures and keystroke/signature dynamics are behavioural biometrics. These techniques allow for truly unique characteristics to be used in authenticating users, and are generally considered more reliable when used in conjunction with unique user ids and passwords.

The supporting scientific rationale is that these characteristics cannot be shared or changed, like user IDs and passwords. In my previous work experience, the researcher has found these advanced techniques to be only used in very sensitive governmental and commercial applications. However, this was primarily due to relatively high costs of such technologies. Today, biometric systems have become more affordable: therefore we should expect to see further utilisation of this technology in the future.

While these different security objectives are all very important they must be considered in the larger realm of the businesses goals. A detailed initial assessment together with a Cost-Benefit Analysis (CBA) will be very useful to the growing organisation as well as the mature organization seeking to capitalise on new technologies such as Virtual Private Networks and business frameworks like Electronic Commerce.

In a business context, trust is not very different than in a personal relationship. Trust involves a premise of being able to rely on the duties and responsibilities of another party. Company A may seek to establish a trusted relationship with a certificate authority in order to allow the certificate authority to provide authentication mechanisms on their behalf.

This criterion is important when selecting a third party vendor. In response to these concerns different organisations have attempted to establish factors and definitions; which then can be used to judge vendors. The U.S. Department of Defence developed the Trusted Computer System Evaluation Criteria (TCSEC). This publication is more commonly referred to as 'The Orange Book' due the color of its cover.

Table 2.14 – TCSEC/Orange Book Security Rating Criteria

Criteria Grade	General Definition
A	Verified Protection
B	Mandatory Protection
C	Discretionary Protection
D	Minimal Protection

Source: (Gollmann, 1999)

The European Union developed similar guidance referred to as the European Community's Information Technology Security Evaluation and Certification (ITSEC) scheme. These tools continue to require on-going modification as technology changes. Additionally, a new set of international security standards known as the Common Criteria have received much support from the computer security community. At present, there are over twelve nations participating the second release of guidelines and standards that recommend rating criteria and guidelines to government and private industry. The U.S. and U.K. are two countries that have taken a leading role in advancing these efforts.

Over the next ten years, the E-Commerce market will continue to experience rapid growth (Rayport and Jaworski, 2001). New vendors will enter the marketplace, in terms of products and services for the four existing types of electronic commerce. The value of Common Criteria will be even more intrinsic as the business community adopts and relies upon more information technology in a global marketplace.

2.8.7 Information Technology Governance

Corporate governance has seen renewed interest in recent years, given various major scandals in the US and elsewhere. The IT Governance Association has developed a variety of guidance tools for information security practitioners, auditors and members of the Board of Directors (IT Governance Institute, 2006).

This guidance has presented various suggestions for best practices to the larger business community in an effort to enhance information security within the private sector. In this regard, there are five desires outcomes for information security governance:

1. Strategic alignment of information security with business strategy to support organisational objectives;
2. Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level;
3. Resource management by utilising information security knowledge and infrastructure efficiently and effectively;
4. Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved; and
5. Value delivery by optimising information security investments in support of organisational objectives. (IT Governance Institute, 2006).

So with these various objectives improved governance can be implemented in the area of IS security.

2.9 U.S. Federal Government Initiatives

Like most G-8 nations, the government of the United States has been active in the area of computer security. Furthermore, over the past five years, there has been significant research, publicity and public pressure to induce the U.S. government to get more involved. The growth of the Internet and Electronic Commerce together have placed additional pressure on the government to take a more active role in cyber security. Further contributing to this situation is the publicity gained by computer hackers and the spread of powerful computer viruses.

2.9.1 Historical Overview

In many ways, the U.S. government has been a leader in the field of computer security. Some of the most notable accomplishments in this area are:

1. Development of computer security standards through National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI) and the Department of Defence (DOD);
2. Formulation of a standardised computer audit manual, Financial Information Systems Computer Audit Manual (FISCAM), which is published by the Government Accountability Office (GAO);
3. Initiation of a comprehensive review of the national critical information infrastructure; and
4. Creation of a framework for cyber crime investigation and communication, through the Federal Bureau of Investigation's National Infrastructure Protection Centre (NIPC).
5. Establishment of the Department of Homeland Security shortly after the September 11th terrorist attacks with a dedicated division for cyber security.

Historically, the majority of these actions have been focused on technology management and business operations issues at Federal Government agencies. However, now based on the general nature of Electronic Commerce; the U.S. government to try and achieve new methods of cooperation and the sharing of information between industry, government and academia sources.

2.9.2 President Clinton's Initiatives

In 1996, President William J. Clinton organised a diverse group of experts in the field of computer security to make recommendations for improvements to computer security programs and systems. Known as the President's Commission on Critical Information

Infrastructure (PCCIP), personnel from academia, industry and government participated in this landmark effort. Table 2.15 below provides a descriptive list of these individuals.

Table 2.15 – PCCIP Commissioner Membership

Individual	Organisational Affiliation
Robert T. Marsh, Chairman	Not Known
John R. Powers, Exec. Director	Federal Emergency Management Agency
Merritt E. Adams	AT&T
Richard P. Case	IBM
Mary J. Culhan	Georgetown University
Peter H. Daly	Department of the Treasury
John C. Davis	National Security Agency
Thomas J. Falvey	Department of Transportation
Brenton C. Greene	Department of Defence
William J. Harris	Association of American Railroads
David A. Jones	Department of Energy
David V. Keyes	Federal Bureau of Investigation
Stevan D. Mitchell	Department of Justice
Joseph J. Moorcones	National Security Agency
Irwin M. Pikus	Department of Commerce
William Paul Rogers, Jr.	National Association of Regulatory Utility Commissioners
Susan V. Simens	Federal Bureau of Investigation
Frederick M. Struble	Federal Reserve Board
Nancy J. Wong	Pacific Gas and Electric Company

Source: Alexander and Swetnam, 1999

This commission was also supported by various staff members, consultants and reviewers. At the completion of their work, a diverse set of recommendations was forwarded to the President. These opportunities for improvement are summarised in the following Table 2.16:

Table 2.16 – Number of PCCIP Recommendations by Functional Area

	Functional Area-Brief Description	No. of Recommendations
1.	New federal policy entity	12
2.	Federal coordinating entity	14
3.	Need for a permanent IPTF	15
4.	Emergency response plans	15
5.	Minimal essential infrastructure	5
6.	Centralised data collection	9
7.	Federal government model	3
8.	Existing government jurisdiction	8

9.	Administrative and regulatory requirements	10
10.	Public-private research	29
11.	Certifications and standards etc.	20
12.	Existing liability climates	4
13.	Private sector regulations	22
14.	Public-private investment initiatives	6
15.	New risk management models	1
16.	Public awareness and education	19
17.	Professional training	11
18.	International cooperation	8
19.	Export and trade policy	5
20.	Enhancements to deterrence	2
21.	Period of transition to war	3
22.	Time of declared war	0
23.	Existing legislation and regulations	9
24.	Short-term assurance measures	8

Source: Adapted from Alexander and Swetnam, 1999c

Perhaps one of, if not the most important item that this commission did was to help define what areas were to be considered as critical infrastructure. A set of eight sub-areas were determined to be critical to sustaining normal government operations. In other words, those that are needed to maintain civil obedience, order and critical services (Alexander and Swetnam, 1999). A more precise definition of infrastructure is "the basic, facilities, services, and installations needed for the functioning of a community or society, such as transportation, and communication systems, water and power lines and public institutions" (Lukasik, Greenberg and Goodman, 1998). The following is a general overview of each of these areas as announced in *Critical Infrastructure Protection, Presidential Decision Directive 63*, which was the Executive Order issued in May 1998. This began the process of formally incorporating the PCCIP's recommendations into areas of governmental responsibility:

1. *Oil and Gas* – encompassing various elements of the energy sector including: electricity, oil, natural gas and all related sub-networks and delivery systems.
2. *Financial Services* – areas necessary to support the national economy such as bank transfers, stock and bond markets as well as supporting transaction processing database systems.
3. *Water Supply* – including drinking water, fire-fighting, public safety, heating/cooling and business uses as well.
4. *Emergency Services* – covering such areas as police, fire, ambulance and emergency management services in the event of disasters, ordinary and catastrophic.
5. *Government Services* – including federal, state and local agencies dealing with the general public welfare.

6. *Electrical Power Services* – addressing all major areas of electric power generation, storage and transportation necessary to the provision of vital services.
7. *Transportation Services* – covering all areas of people and consumer goods movement, thereby protecting our national role and impact in the global economy.
8. *Telecommunication Services* – maintaining the public telephone network, Internet viability and computer systems used on a daily basis.

Source: (Adapted from Alexander and Swentam, 1999 and Rathmell, 2000)

Organisationally, this executive order created six different areas of responsibility. First, is the National Infrastructure Assurance Council. This organisation is comprised of government and private sector personnel that focuses on policy recommendations to the President. Second, is the Infrastructure Assurance Support Office provides functional support for this effort. Third, for each of the eight critical infrastructures outlined above a lead government agency was assigned to ensure that information gets shared effectively between various stakeholder groups. Fourth, a Sector Infrastructure Assurance Coordinator acts as a repository and clearinghouse for all related information provided by various parties during their information sharing activities. Fifth, an Information Sharing and Analysis Centre organised by government and private sector groups to synthesise the information gathered and prepare conclusions that can be used in future initiatives. Sixth, a warning centre was established to provide advance notice and information about physical and cyber attacks on the critical infrastructures. This effort gave birth to the FBI's National Information Protection Centre.

There are five primary functional areas related to partnership and dynamic interaction between the private sector and the U.S. Federal government (PDD 63 as explained by Alexander and Swentam, 1999). Firstly, policy formulation is needed to address areas of national security risk and make sure that required assurance objectives, services and strategies are implemented. Secondly, risks should be prevented and mitigated, based on threat assessments and risk management practices. Thirdly, information needs to be gathered and shared. This type of information normally deals with law enforcement agencies and intelligence services, but can extend to the public as well. Fourthly, counteraction or incident management needs to occur in order to deter attacks on the critical infrastructures and apprehend the attacker(s) when attacks are successful. Finally, the government needs to have functions that can respond and restore systems after they have been attacked.

The work of the PCCIP was truly groundbreaking. Their activities represented major positive actions at the national level. Furthermore, the U.S. model is now being investigated for application in other countries around the world (Fischer-Hubner, 2000 and Thomas, 2000). However, these governmental efforts are not without controversy. For example, civil liberty and privacy groups feel that the government is taking too great a role in managing the U.S. computer security environment (Electronic Privacy Protection Centre, 1998). Nevertheless, the plans recommended by the PCCIP have largely moved forward.

2.9.3 Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) is normally involved in the discovery and investigation of criminal activity across state boundaries. This entity has law enforcement capabilities across all 50 U.S. states and in certain circumstances performs activities with state and municipal police authorities. Since 2001, the FBI has maintained 56 Field Offices, all of which have some computer crime resources (General Accounting Office, 2001).

One of the specific recommendations issued by the Presidential Commission on Critical Infrastructure Protection (PPCIP) in 1998 called for the establishment of a coordinated government-wide approach to computer security incidents related to the critical information infrastructure. With the adoption of this recommendation the National Infrastructure Protection Centre (NIPC) was founded. Due to its intrinsic importance to national security a detailed description of their specific responsibilities is discussed in Section 2.9.10 below.

2.9.4 National Institute of Standards and Technology

The role of the National Institute of Standards and Technology (NIST) is to develop and promulgate detailed standards for use in specific industries. Technical bulletins are issued in order to promote security, operating practices and other issues related to IT and business 'best practices'. One of the most commonly used sources of computer vulnerability information on a global basis is NIST's Common Vulnerability and Exposures (CVE) dictionary.

This organisation supports the research and analysis of computer vulnerabilities and recently helped support the mission of the Department of Homeland Security (DHS) information sharing efforts by extending this dictionary into a database. In 2006, the National

Vulnerability Database (NVD) has full search capabilities and a vulnerability scoring tool which helps users assess the potential impact on their IT systems.

This organisation is similar to the Department of Trade and Industry (DTI) in the United Kingdom. Since NIST standards represent official guidance, mandatory compliance is required of most government departments and agencies. The notable exceptions are the intelligence agencies which are free to develop more stringent standards.

2.9.5 Department of Defence

The major area of responsibility of the Department of Defence (DOD) is to protect and defend the nation state from a military stance. Within the U.S. DOD, there are various branches: Army, Navy, Air Force, Marines, and Coast Guard. With respect to computer security, DOD is particularly at risk to computer security threats because of past, present and future military activities. Recent examples of such risks include:

1. President Bush's War on Terrorism;
2. Operation Desert Storm Conflict in the late 1980s;
3. International peacekeeping activities in Bonsia-Hertzogovenia and Kosovo;
4. Routine surveillance missions in the South China Sea where a U.S. fighter jet was captured by Chinese authorities; and
5. Military activities in world 'hot spots' such as the Middle East and Asia-Pacific.

During these types of events other countries or third party interest groups desire to gain military advantage by gathering intelligence and disabling computer systems. For instance, in the Desert Storm Conflict an Iraqi computer hacker gained access to sensitive DOD computer systems. Furthermore, one of the most highly effective yet controversial sub-units of the DOD is the National Security Agency (NSA).

Rumours have been circulating in international political and technology circles that NSA has a top-secret unit known as ECSHLEON, which reportedly conducts: sniffing and monitoring of other U.S. government computer systems, ears dropping on government officials and private citizens; and penetrating the computer systems of allies and adversaries through the use of defensive information warfare exploits. In early-2001, some European government officials held public hearings about this program. In public testimony, representatives of the U.K., Danish and French governments acknowledged the existence of this program. This is much to the dismay of civil libertarians and others who believe the ECSHLEON violates such basic democratic dictates as freedom of speech and privacy of information. When computer security incidents transpire legal cases are normally brought forward for prosecution.

2.9.6 Department of Justice

The Department of Justice (DOJ) is responsible for the prosecution of legal matters involving the public interest. With regard to computer security, the DOJ works on a variety of computer frauds, Internet scams, identity thefts, extortion and computer hacking incidents. Most staff members at the DOJ are attorneys and legal researchers. For example, when the famous computer hacker, Kevin Mitnick launched the Morris Worm, it was attorneys from the DOJ who litigated this case against him in court.

2.9.7 Other U.S. Federal and State Government Agencies

There are a variety of other federal and state government agencies that may also have a role to play in computer security. These federal organisations include the: Federal Emergency Management Agency, U.S. Marshal's Office, Federal Trade Commission, Department of Commerce, Federal Aviation Agency, Department of Transportation, Government Accountability Office and Department of Health and Human Services. On a state level, there are normally corresponding bodies and some additional agencies.

2.9.8 Computer Emergency Response Team/Coordination Centre

After the outbreak of the Morris Worm, the U.S. Government established the Computer Emergency Response Team (CERT) in November 1988. In my opinion, the U.S. government received 'a wake-up call' about Internet and computer security from this event. Later, in 1997, this organisation was officially renamed *The CERT/Coordination Centre* to more accurately state its mission and supporting objectives. CERT/CC is primarily funded by the U.S. Federal government. Annual budget allocations are made from the Department of Defence budget which then allocates funding to the National Science Foundation (NSF) who, in turn, provides funding to Carnegie Mellon University's Software Engineering Institute (SEI). In turn, it is the SEI that has responsibility for managing the daily affairs of CERT/CC.

Additional funding is provided by other U.S. Federal government agencies, as well, as some private sector contributions. Further details of the yearly contributions and funding sources can be found in the CERT/CC annual reports and can be accessed by the public from the organisation's homepage.

The primary objective of CERT/CC is to respond to and investigate Internet based security incidents. Over the years, CERT/CC has been very successful in its efforts. In fact, today the model of practice is now used a prototype for other organisations around the world. CERT/CC issues various types of communications about computer security. The main communications are:

1. Advisories - provides a description of a serious security problem and its impact, along with instructions on how to obtain a patch or details of a workaround;
2. Alerts - various types of e-mail announcements; and
3. Incidents and Vulnerability Notes - contains information that does not meet the organisation's own criteria for alerts, but that might be useful to the Internet community at large.

Source: (Adapted from the CERT/CC Web Site, June 2004)

In recent years, the number of security incidents reported to CERT/CC has changed dramatically. For instance, in 1990 there were 252 such incidents, compared to 9,859 in 1997, and 21,756 in 2000 and with steady increases through 2006 (see www.cert.org for up-to-date details).

Earlier research by Rich (2001) and Howard (1997) involved an exploratory study of the CERT/CC's efforts with formidable discoveries and interesting results. Various facets of this research are worth examining in further detail. Rich (2001) primarily used secondary data available from the *1999 Annual FBI/CSI Computer Security Survey* to identify relationships between Internet security incidents and general demographic changes. Howard (1997) analysed, classified and summarised Internet security incidents from 1988 to 1995 using actual CERT/CC data. Some of the items discovered include:

1. Various types of Internet security attacks occurred;
2. There are various methods to classifying the security incidents investigated by CERT/CC:
3. There are various known and unknown causes for Internet security incidents;
4. Various threats and vulnerabilities are at the root cause of Internet security incidents;

5. More information could be shared by the organisation to facilitate further research in this area; and
6. Encryption programs were effective in protecting sensitive information.

While these research efforts are very impressive in its own right; it is important to also realise that:

1. This research was done as an initial studies;
2. The commercial uses of the Internet were not as evident then they are today;
3. The global growth of the Internet continues to accelerate; and
4. There are a number of interesting suggestions for further research that can be explored in the future.

These limitations and suggested areas for further research are considered for further exploration in Section Nine of this chapter, as well as, in Chapter Three of this project. While this organisation was a successful initial establishment of a national government effort, it also became a role model for other countries to help counteract their Internet security threats. Currently, there are similar organisations in the United Kingdom, Australia, Singapore, Canada and other countries. Another U.S. government initiative related to computer security is the Federal Computer Incident Response Centre.

2.9.9 Federal Computer Incident Response Centre

No matter how effective protective security measures are there will be intrusions that breach government computer systems. The Federal Computer Incident Response Centre (FCIRC) is responsible for responding to such incidents. Additionally, FCIRC publishes information about computer security incidents and breaches on its web site at www.fcirc.gov.

The FCIRC makes various types of information available solely to federal government agencies. The general types of information including: incident reports, software bug descriptions and CERT/CC related information on possible high-level Internet security issues. For practical purposes, while this information is useful it is only circulated to verifiable contact personnel at federal government agencies, thus providing a limited information sharing capability.

2.9.10 National Infrastructure Protection Centre

The NIPC functions as the central command centre for computer security issues related to the various critical information infrastructures. The public has been waiting to see what type of results the NIPC can deliver. Responsibilities of the NIPC are best outlined in the organisation's mission statement. The main areas of responsibility, as publicised by the organisation include:

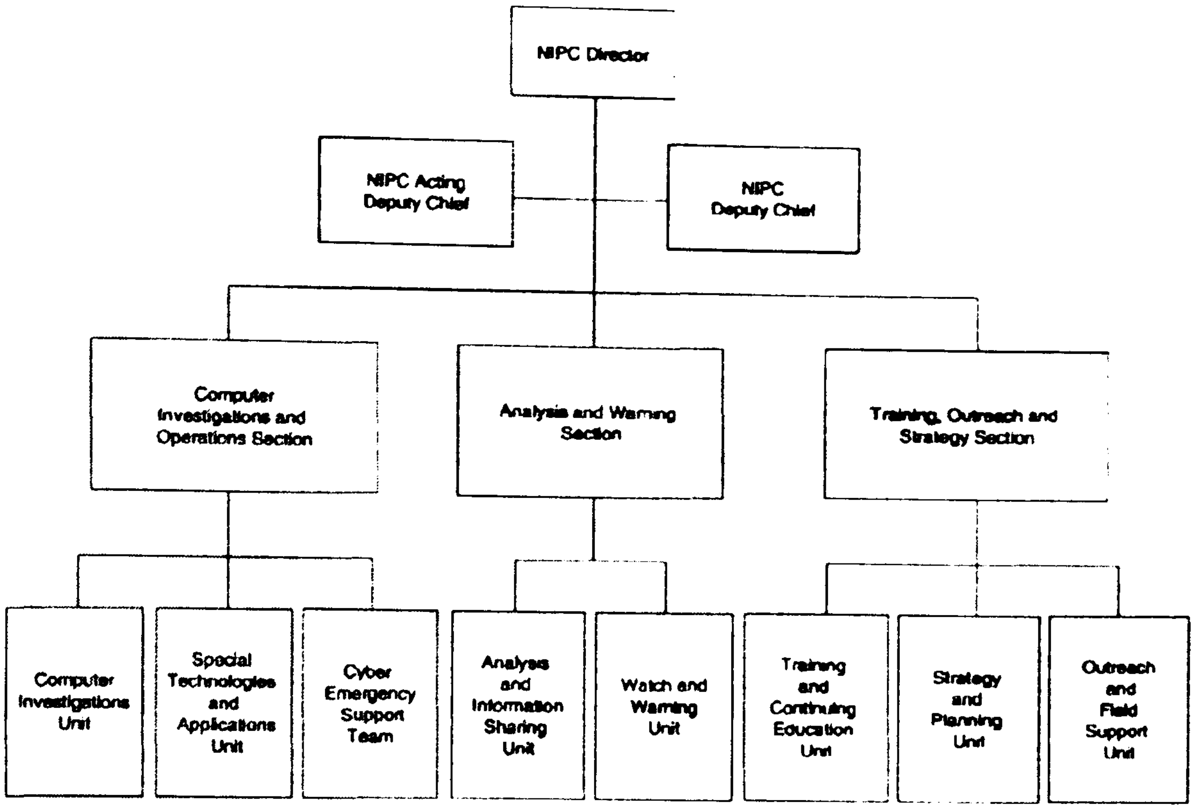
1. Deter, detect, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber that threaten or target our critical infrastructures;
2. Manage computer intrusion investigations; support law enforcement, counter-terrorism and foreign counterintelligence missions, related to cyber crimes and intrusion; support national security authorities when unlawful acts go beyond crime and are foreign-sponsored acts on United States interests; and
3. Coordinate training for cyber investigators and infrastructure protectors in the government and private sectors.

Source: Adapted from NIPC Web Site, May 2002

General scrutiny has also been disseminated from the General Accounting Office which functions as the audit body for the federal government sector which according their published audit reports (GAO 2000 and 2001) which indicated that there are significant shortcomings in terms of organisational resources, coordination of work and technical capabilities that limit the organisation's overall effectiveness.

Provided below in Figure 2.16 is an organisational chart for this entity. It helps to illustrate the key functional areas of responsibility.

Figure 2.16 – NIPC Organisational Chart as at April 2001


NIPC Director
NIPC Acting Deputy Chief
NIPC Deputy Chief
Computer Investigations and Operations Section
Analysis and Warning Section
Training, Outreach and Strategy Section
Computer Investigations Unit
Special Technologies and Applications Unit
Cyber Emergency Support Team
Analysis and Information Sharing Unit
Watch and Warning Unit
Training and Continuing Education Unit
Strategy and Planning Unit
Outreach and Field Support Unit

Source: General Accounting Office, 2001

The main programs include coordination with the FBI, InfraGard a private industry-public sector partnership organisation, information sharing and analysis centres, and technical communications. Table 2.17 below summarises the advisory communications. These are particularly important to this research study, since they will be used in the investigation of the research questions and hypotheses.

Table 2.17 – NIPC Advisory Summary by Type: 2000-2003

Type of Advisory	2000	2001	2002	2003
Assessments	10	4	2	2
Advisories	13	21	9	11
Alerts	10	4	3	0
Total	33	29	14	13

Source: Compiled from the NIPC Web Site in June 2004

The NIPC's has a critical role to play in terms of protecting national security, promoting a beneficial relationship between the public and private sectors. The information is then shared in a newsletter format that is at the core of the data collection and analysis portion of this research project.

2.9.11 Department of Homeland Security

In March 2003, President Bush formed the Department of Homeland Security out of a consolidation of 22 agencies, with over 170,000 employees and hundreds of computer systems (Peters, 2003). Many government observers believe it represents one of the most significant overhauls in federal government over the past 50 years. The current structure of DHS is designed to speed the flow of information and improve internal and external communications. These groups include twenty-two agencies, most notably the: Federal Bureau of Investigation, Secret Service, Federal Computer Incident Response Centre, the National Infrastructure Protection Centre, and Critical Infrastructure Assurance Office. The reorganisation has aligned these former agencies into four major sub-units: the Border and Transportation Directorate, the Emergency Preparedness and Response Directorate, the Science and Technology Directorate, and the Information Analysis and Infrastructure Protection Directorate. While each division has multiple components to it, the groupings have been designed to promote efficiency and effectiveness of operations.

DHS's overall mission is very diverse. In fact, it deals with human and technological systems affecting critical infrastructure. Some examples include: science, high technology, information systems, laboratories and research facilities, weapons of mass destruction, and physical security issues such as border security, transportation, and maritime sectors. While the trends in this industry have been indicative of greater reliance on technical systems, the human factors remain very important. While combining of the previously described units into various directorates in DHS, it is hoped that information sharing will be improved, intelligence and counter-intelligence operations will be streamlined and the overall effectiveness of security operations will increase. Additionally, many observers believe that this will also bring the government to new levels of accountability in these same areas.

Many broad and major challenges exist. For example, public confidence needs to be improved so that U.S. citizens can remain vigilant against security threats. Another major issue is with the government's IT investments and operating budget process. While this continues to increase steadily each year, even though the availability of qualified personnel is in short supply. Both of these items will have implications on DHS's overall success. The second secretary for DHS, Michael Chertoff has continued to make small agency reorganisations.

In addition, *The National Strategy to Secure Cyberspace* was released by DHS in 2003 (U.S. Department of Homeland Security, 2003). This policy document outlined three major strategic objectives as follows: prevent cyber attacks against America's critical infrastructures, reduce national vulnerability to cyber attacks and minimise damage and recovery time from cyber attacks that do occur. Each of these strategic objectives was then supported by specific programmatic initiatives and priorities. However, industry analysts and academic researchers have been somewhat sceptical of these efforts primarily because they are quite similar to the PCCIP original recommendations.

2.10 Summary, Conclusion and Research Questions

The Internet and Electronic Commerce are basic concepts by themselves. However, the rapid growth of these domains and the ever-changing area of technology create a highly dynamic environment. The field of computer security in today's Information Age is a wonderful area for exploratory research. As a whole, this area is fascinating, challenging and needing of additional research.

2.10.1 Summary

We are witnessing an exciting economic revolution of sorts. Electronic Commerce and the Internet are changing the way we conduct business and participate in daily activities. No longer are we an agrarian or industrial economy, and the Information Age has transitioned many local businesses to global businesses operating beyond stringent geographical boundaries.

Those companies that embrace EC as an effective mode of business will likely increase their overall competitive advantage and shareholder value. However, these opportunities are not without significant computer security risks.

Additionally, the emphasis of critical information infrastructures highlights the fact that commercial business and government organisations will face both an increased intra and inter reliance. This situation is highlighted by the following key factors:

1. It is a dynamic time in modern society filled with changing dimensions related to Electronic Commerce;
2. The nature of evolving technologies force new products quickly into a competitive market, which in turn produces vulnerable products;
3. The increase in the reported number of Internet security incidents to CERT/CC; and
4. Innovative U.S. Government efforts in examining the critical information infrastructure and establishing the National Information Protection Centre.

These particular points correlate to the research questions that have been formulated for this study.

2.10.2 Conclusion

The current state of Electronic Commerce and the Internet has revolutionised the way society functions. Our use of and reliance on technology has changed the way businesses operate. It has also modified the way in which individuals carry-out their personal affairs. Today, national governments also are changing the way they protect our society as a whole.

Through the exploration of these changes in the form of research questions, I hope to gather new beneficial and useful information.

2.10.3 Research Questions

The following table summarises the major research studies discussed in this chapter. Careful consideration of the focus and approach of each project was made by the researcher prior to constructing the research questions included herein.

Table 2.18 – Sampling of Related Research Projects in Information Systems Security

Researcher(s)	Year of Study	Focus	Approach
Vatis	2001	Predictive models of cyber attacks	Case study approach with known adversaries in regional conflicts
Rich	2001	Internet security incidents	Analysis of secondary data supplied by CERT and others
Comer Et. Al.	2000	Buffer overflows as a primary security vulnerability	Experimental analysis of related protection techniques
Wagner	2000	Software assurance	Experimental analysis and model development
Puketza	2000	Filtering and testing	Experimental analysis and model development
Soo Hoo	2000	IT risk management	Analysis of secondary data and model development
Howard	1997	Internet security incidents	Analysis of secondary data supplied by CERT
Landwher Et. Al.	1994	Computer security flaws	Survey analysis
Bakersville	1993	Security factors related to I.S. design	Survey analysis and comparative model analysis

After a thorough review of the literature and a close examination of the above noted research studies including the research methods, results and suggestions for future research. The researcher developed a series of research questions and related hypotheses.

These research questions have been further decomposed into specific hypotheses and are described in more detail in Chapter Three.

Research Question Number One:

How do the various types of NIPC advisory communications correlate to the nature and type of broad Internet security incidents as reported in the CyberNotes newsletter communications during the period of January 2000 through December 2003?

Hypothesis No. 1:

There is a defined correlation between the new 'critical' software bugs detailed in the NIPC's CyberNotes newsletters and the general number of new software bugs identified by the U.S. Computer Emergency Response Team/Coordination Centre (CERT/CC) and the U.S. National Institute of Standards and Technology (NIST).

Hypothesis No. 2:

There is a defined correlation between the number of critical computer viruses detailed in the NIPC's CyberNotes newsletters and the general number of computer viruses found 'in the wild'.

Research Question Number Two:

Did the number of critical infrastructure related security incidents as reported by the NIPC change from January 2000 to December 2003 based on U.S. Internet utilisation?

Hypothesis No. 3:

There is a positive correlation between the total number of U.S. Internet users and the critical cyber security infrastructure information reported by the NIPC.

Hypothesis No. 4:

There is a positive correlation between the number of U.S. based Internet host computers and the cyber security critical infrastructure information reported by the NIPC.

Hypothesis No. 5:

There is a positive correlation between the number of global World Wide Web (WWW) pages and the cyber security critical infrastructure information reported by the NIPC.

Research Question Number Three and Related Hypotheses

Research Question Number Three:

Do the computer security advisory communications of the NIPC during the period of January 2000 to December 2003 relate to the U.S. Electronic Commerce transactions?

Hypothesis No. 6:

There is a positive correlation between the total value of U.S. Electronic Commerce transactions and the cyber security critical infrastructure security information reported by the NIPC.

Research Question Number Four and Related Hypotheses

Research Question Four:

How do the various types of NIPC advisory communications correlate to various broad macroeconomic factors during the period of January 2000 through December 2003?

Hypothesis No. 7:

The NIPC's cyber security information communications is positively associated with various macro-economic factors such as: major interest rates, stock market indices, Consumer Price Index (CPI), Gross Domestic Product (GDP), inflation, and unemployment.

Research Question Number Five and Related Hypotheses

Research Question Five:

Do the computer security advisory communications of the NIPC during the period of January 2000 to December 2003 increase during U.S. military conflicts and political events.

Hypothesis No. 8:

There is an increase in the number of critical computer security advisory communications of the NIPC during time periods of military events: specifically 1) the attack on the USS Cole Battleship, 2) the War in Afghanistan, 3) September 11th Terrorist Attacks, 4) U.S. Invasion of Iraq, and 5) U.S. Military Intervention in Liberia.

Hypothesis No. 9:

The number of computer security advisory communications of the NIPC is positively associated with an increase during periods of domestic political change and crisis such as the: U.S. Presidential Election, Western States energy crisis, severe winter weather storms, and Northeast Blackout.

The analysis of these research questions and related hypotheses is discussed in greater depth as part of the next component of this research study, Chapter Three – Research Methodology.

Chapter Three – Research Methodology

3.1 An Introduction

The purpose of this chapter is to thoroughly explain the methodology, need, specific research methods and hypotheses of the research study. Each of these individual areas is addressed in separate sections herein. All academic research involves epistemology or the development of knowledge. In this research study, the researcher focuses on the possible relationships of computer security information gathered, analysed and shared by the National Infrastructure Protection Centre (NIPC) in the context of critical infrastructure protection in the United States.

Three primary research philosophies: positivist, interpretivist and critical were identified in the information systems literature (Galliers, 1992 and Orlikowski, 1991). Included in this section is a discussion of each major philosophy; together with examples of previous research studies conducted using approaches associated with these underlying philosophies.

The first major research philosophy is known as positivist, and is directly associated with empirical or basic research approaches as illustrated in Table 3.1 below:

Table 3.1 – Common Empirical/Positivist Research Approaches

1.	Laboratory Experiments
2.	Field Experiments
3.	Surveys
4.	Case Studies
5.	Theorem Proofs
6.	Forecasting
7.	Simulation

(Adopted from: Galliers, 1992, p. 149 and Orlikowski, 1991, p. 124)

Not every project undertakes more than one of these approaches. There are various advantages and disadvantages of each individual approaches; some of which are highlighted and briefly described in the following table together with the most appropriate area of research for the individual study objective.

Table 3.2 – Advantages and Disadvantages to Empirical/Positivist Research Approaches

Approach	Features and Strengths	Weaknesses	Appropriate Area for the Study Objective
Laboratory Experiments	A small number of variables in thoroughly examined in a laboratory setting.	The limited extent by which relationships exist in the real world compared to the isolated setting of the laboratory where the variables were tested.	Useful in testing casual relation, but not well suited for generalisation and difficult when dealing with a research model that contains a large number of variables.
Field Experiments	Extends laboratory type experiments into real life which creates a greater relationship to reality.	Identifying willing organisations to participate in this type of research.	Good for testing casual relationships, but more difficult when studying information systems security due to the nature of the subject matter and governmental policies and restrictions.
Case Studies	Hopes to describe relationships which exist in reality, but within a single or limited number of organisations. Useful in understanding reality in great detail and allows for an analysis of multiple variables.	Restriction on a few or even one organisation which in turn limits the generalisability of results.	Less appropriate for testing casual relations. Difficult to generalise results concerning the research model's validity to other cases.
Surveys	Gives snapshots of practices at a set point in time regarding relationships that exist in the past, present and future. Allow a greater number of variables to be studied than in experimental approaches. Provide real work situations and are more appropriate to generalisations.	Difficult to gain insight into the causes of phenomena being studied. Possible bias may exist in the respondent population, with the researcher and/or at the moment in time the research is undertaken.	More feasible and appropriate in allowing the use of statistical analyses such as regression. Provides a systematic method of validating the research model and obtaining results that may be generalised. Suitable to a study across a wide range of organisations and environments.

Adapted from: El-Kordy, 2001 and Galliers, 1992

While both surveys and experiments are useful research tools, they are not appropriate for all research studies. Specifically, for this project which deals with an innovative government program related to computer security, these tools do not appear to be useful. This is true even if the common obstacles noted above could have been overcome. For instance, there are a plethora of legal restrictions governing what type of information government employees can disclose to non-privileged parties (i.e. academic researchers and private industry representatives). Secondarily, the sensitivity of the subject matter is very great and the likelihood of bias was felt to be very high. For these reasons, experiments and surveys were not deemed appropriate for this project.

Experiments can be either human or technological. In fact, Silverman (1993) argued that quantified data is the only type of valid proof of social facts. Gathering of experimental data is not relevant to the research study hypotheses described in Section 3.3. Therefore, experiments and field studies were not considered for exploration in this research study. This is in consistent with a grounded theory approach described in more detail in Section 3.1.5, since there will not be a lag time in obtaining and analysing the data. Essential to the accomplishment of this goal is designing a sufficient scope for this research study. The NIPC was established in 1998 and was strictly focused on computer security issues related to critical national infrastructures as defined by the Presidential Commission on Critical Infrastructure Protection (PPCIP). This is in sharp contrast, to the Computer Emergency Response Team/Coordination Centre (CERT/CC); which is well established and has been actively involved in IT security for more than twelve years, as studied earlier by Howard (1997).

The *interpretive approaches* normally involve an assumption that access to reality is only possible through different types of social constructions including: language, consciousness and shared meanings (Myers, 2001). The typical modes of analysis in this approach include: hermeneutics, semiotics, narrative and metaphor. Within the second mode of analysis, semiotics, three distinct forms were organised. The first of which is content analysis. According to Krippendorff (1984, p. 21), this is "a research technique for making replicable and valid references from data to their contexts". Weber (1990) and Myers (2001) further explain that this technique allows the researcher to search for structures, patterns and similar features in the text and make inferences about these regularities. Conversation analysis is quite similar to content analysis except for the fact that the researcher puts him/herself in the situation being researched in order to describe information about the practices. Discourse analysis uses elements of each of the other two semiotic approaches in a language game method of analysis.

Finally, another research philosophy known as the *critical approach* can be used in information systems research. This approach involves an assumption on behalf of the researcher that "social reality is historically constituted and that it is produced and reproduced by people" (Myers, 2001 p. 5). According to Myers (2001) and Trauth (2001) this approach is not as common as other approaches in modern information systems research.

The researcher adopted an interpretivist approach as the philosophical underpinning of this study. The next step in a research project is to select a specific research method or combination of research methods that will be used in the study.

3.1.1 Overview of Research Methods in Information Systems

Today, there are a diverse and growing number of research methods being used in the field of information systems research. Originally, most research was of a quantitative nature. In fact, many authorities commonly refer to quantitative research as traditional research. However, qualitative research has gain increased popularity and presents many unique advantages to the researcher (Trauth, 2001, Bradley, 1993 and Bogdan and Ksander, 1980).

3.1.2 Quantitative Research Methods

Typically, quantitative research methods involve extensive statistical analysis. Many contemporary IS researchers argue that this is a traditional approach to academic research (Myers, 2001; Trauth, 2001; and Lacity and Janson, 1994). These tools are very effective in answering 'how much' change a particular variable has exhibited from one year to another. Research can utilise quantitative methods in different ways. For instance, in the social sciences, surveys and experiments are still extremely popular.

While these types of studies are favoured by many 'traditional' researchers: pure quantitative studies are not free from criticism (Trauth, 2001). This is because these studies are useful in answering various 'how many' type questions, but they do not probe further with questions that deal with the explanatory 'why' types of questions.

The case study, survey, field study and experiment approaches were briefly considered for this project. But, after further examination and discussion with the research supervisor all of these approaches were deemed not to be appropriate. The primary reasons were government restrictions on highly sensitive information, the unwillingness of some people to assist with these tasks and the general practicalities involved. Furthermore, while some social scientists believe that survey instruments produce the best data collection method in the social sciences, some others disagree. According to Fowler (1995), poorly designed surveys can create inaccurate data which in turn results in inferior recommendations. Additionally, surveys are normally pilot tested in order to ensure good form and attainment of objectives. Doodley (1984) argued that surveys can also be subject to sample bias, data collection error, and various types of sampling errors. In addition, past computer security surveys have been conducted by highly practitioner oriented groups such as: the Information Systems Audit and Control Association, Computer Security Institute, SANS Institute, and Big Four Accounting Firms.

The merits of quantitative research are numerous and these methods are used extensively in many research projects. However, if a researcher also desires to answer the 'why' aspect of research questions, then qualitative research can be highly effective.

3.1.3 Qualitative Research Methods

Qualitative research methods have their roots in the fields of Anthropology and Sociology and were made famous in the early part of the twentieth century in the United States. *The Chicago School*, as it has been referred to; was actually an academic department at the University of Chicago in Illinois.

In recent years, a number of important information systems researchers have argued that qualitative research is an under-utilised research method, and should be used more aggressively in future research studies (Trauth, 2001a and Meyers, 1997).

There are four main types of qualitative research methods used in information systems (Orlinkowski, 1993). In order to compare and contrast each of these methods the following summary table was developed:

Table 3.3 – Qualitative Approaches Commonly Used in Information Systems Research

Qualitative Approach	Variation Number One	Variation Number Two	Variation Number Three
Heurmeneutics	Pure Textual Data	Critical Heurmeneutics	
Semiotics	Content Analysis	Conversation Analysis	Discourse Analysis
Narrative and Metaphor	Oral Narrative	Symbolism	

Adapted from: Myers, 2001

Lacity and Janson (1984) discussed two main reasons why some IS researchers do not like qualitative methods. In their research, they explain that this is due to two main reasons. The first reason is that they are not familiar with the research methods used in qualitative research. In this regard, I.S. researchers are seemingly unwilling or at least inhibited to learning new research methods (e.g. those which they have little or no previous experience with). Secondly, they indicated that many believe that qualitative approaches are equated to nonpositivist, antipositivist interpretive research. A significant assertion made in this research is that all researchers could consider using qualitative methods regardless of their underlying research philosophy (Bakersville, 2001 and Trauth, 2001).

Content analysis is a popular qualitative research method used in a variety of the social sciences. Many authorities including Krippendorff (1984) trace the origins of this approach back to World War II. At that time, the allied forces tried to analyse Nazi propaganda communications to predict military movements and actions.

Other examples of studies done using content analysis are particularly popular in: marketing, advertising, communications and public policy. For example, Naccarato and Neurendorf (1998) conducted an advertising study using content analysis to assess a series of business-to-business promotional campaigns in a trade publication for the utilities sector. In their study, they investigated both form and content variables using a detailed codebook and included regression analysis. At the conclusion of their research, they determined that the main predictor of the effectiveness of the study was the size of the advertisement and other predictors were colour, attractiveness, and argument. One of the advantages of content analysis is that data can be gathered from a variety of sources, including: newspaper articles, magazine advertisements, interview transcripts and official publications.

3.1.5 Event Study Methodology

Event study research has been used in a variety of social sciences such as: capital markets, corporate finance, accounting, marketing, advertising and others (i.e. strategy, organizational behavior) for a considerable period of time. It is a well accepted and frequently used technique in these fields.

In order to design a proper event study project a number of key research tasks must be carried out by the researcher (MacKinley, 1997, Ball and Kothari, 1991) First, the researcher must define the event of interest (e.g. event window) and identify the period over which the impact of this event should be measured. Second, the researcher customarily defines the event window larger than the actual event (i.e. such as a one day announcement or incident) to permit a liberal interpretation of the related impact. Third, the researcher should define the other periods of time as the non-event window such that comparisons can be made with statistical measures between this period of time and the event window itself. Finally, basic statistical measures can be used to analyse the potential differences in this windows or period of time.

At the core of this methodology, is the efficient market hypothesis (Agrawal and Kamakura, 1995). In more detail, this technique postulates that share prices are indicators of a firm's value and that an event (i.e. earnings announcement, management change, strategic decision) would have an impact on the company's share price. In other words, what response does the share price of a particular company have related to such a public announcement?

To help build the basis for part of this project, the researcher evaluated a number of prior event study research studies. First, Agrawal and Kamakura (1995) used this methodology in the field of advertising to analyse the impact of celebrity endorsements in major print media advertising campaigns for various consumer products. They found that there was a positive impact of these endorsements on consumer buying habits of selected consumer products. Second, in the fields of economics and finance MacKinlay (1997) used an event study methodology to study financial markets and assess the impact of a specific event on the value of a firm. He used publicly available data to measure earnings announcements by U.S. publicly traded firms to investigate share price variation. He found that generally shareholders respond to earnings announcements by these companies. There are some further studies that are worthy of highlighting their use of an event study methodology.

In the field of Information Technology, Im, Dow and Grover (2001) used this methodology to study IT investment and firm market value. A variety of variable such as: firm size, capital invested, industry/sector, financial ratios and other factors were reviewed. Their research results indicate that there is a positive variation with regard to an increase in price and volume of shares related to such public announcements by companies. They also found that the effects of industry/sector and firm size grew stronger over time.

In the security field, Murphy, Gordon and Mullen (2004) studied personal value systems after the September 11th Terrorist Attacks. They used a survey tool with statistical sampling to understand the attitudes, impressions and behaviours of 500 aviation industry employees. In this project, means and rankings were calculated for a variety of study variables to measure three hypotheses which delineated questions according to "before September 11th" and "after September 11th". The results of this research project demonstrated a cultural upheaval in America as well as statistically strong variances in areas related to family, security and salvation values. These results also appear to be consistent with an earlier study by Rokeach who conducted a similar study in the Vietnam War Era.

3.1.5 Mixed Methods

The mixed methods approach takes advantage of both quantitative and qualitative research methods. In fact, while quantitative research is normally done at the first stage, but this does not have to be the case. In other words, if the researcher can present a justified reason for executing qualitative research methods first and then use quantitative methods secondarily this is also acceptable (Creswell, 1994; Greene and Caracelli, 1997; and Tashakorri and

Teddlie, 1998). Furthermore, Creswell (1994) explained that there are no fewer than seven different approaches (e.g. combinations) to mixed methods research.

There are many examples of where mixed methods have been applied in information systems research even though the percentage of all IS research studies that used a combination of these methods was only three percent in 1991 (Sawyer, 2001). One such endeavour by Sprull and Kiesler's in 1991 studied the role of observational data (e.g. the qualitative approach) in providing insight into experimental results (e.g. the quantitative approach).

When using mixed methods additional consideration related to triangulation, integration and interdependence must be made by the researcher. Triangulation often deals with combining data sets from different sources (Sawyer, 2001). This allows the researcher to revisit the same 'research event' in multiple ways. Integration looks to combine two different methods into one study. Inter-dependence deals with the discrete reliability of each data set. To help facilitate this, the researcher can identify linkage(s) with the theory being formulated and attempt to overlap concepts.

Mixed methods are growing in popularity and can utilise a diverse set of research methods. It was used in this study for the reasons described above and in Section 3.4.

3.1.6 Grounded Theory

Grounded theory is normally an interpretivist approach to research that allows the researcher a number of attractive advantages. It was an approach originally developed jointly by Barney Glaser and Anselm Strauss in 1967. The original ideas for grounded theory originated in the theories of human behaviour and spread rapidly as an acceptable method of qualitative research. What was once a clear theoretical approach to research has become a bit vague because the original theorists developed separate and somewhat conflicting individual theories in later years.

Therefore, it is necessary to provide a discrete interpretation of the 'classical' variation of this approach to that which was used in this research project. Creswell (1998) puts forth an excellent working definition of what grounded theory is. This is provided in the following twelve items:

1. The aim of grounded theory is to generate or discover a theory;
2. The research must set aside theoretical ideas to allow a 'substantive' theory to emerge;
3. Theory focuses on how individuals interact in relation to the phenomenon under study;
4. Theory asserts a plausible relation between concepts and sets of concepts;
5. Theory is derived from data acquired through fieldwork interviews, observations and documents;
6. Data analysis is systematic and begins as soon as data is available;
7. Data analysis proceeds through identifying categories and connecting them;
8. Further data collection (or sampling) is based on emerging concepts;
9. These concepts are developed through constant comparison with additional data;
10. Data collection can stop when new conceptualisations emerge;
11. Data analysis proceeds from 'open' coding (identifying categories, properties, and dimensions) through 'axial' coding (examining conditions, strategies and consequences) to 'selective' coding around an emerging storyline; and
12. The resulting theory can be reported in a narrative framework or as a set of propositions.

In order to promote creative thinking in how grounded theory can be executed Strauss and Corbin (1998) suggested the following nine explicit behaviours:

1. Be open to multiple possibilities;
2. Generating lists of options;
3. Exploring various possibilities before choosing on;
4. Making use of multiple avenues of expression;
5. Using non-linear ways of to go back and gain a fresh perspective;
6. Diverging from one's usual way of thinking and working;
7. Trusting the process and not holding back;
8. Not taking short cuts; and
9. Having fun doing it.

The researcher attempted to utilise many of these practical suggestions throughout the project. These practical recommendations help address project quality and enhanced results.

Grounded theory has been an effective approach in Information Systems (I.S.) research over the past decade. Urquhart (2001) provided a number of examples of such prior studies; which are summarised in the following table:

Table 3.4 – Prior I.S. Research Studies with a Grounded Theory Approach

Researcher/Year of Study	Study Category	Brief Description
Heaton, 1998	Text Analysis	Social construct of computer supported cooperative work in two different cultures
Phillips, 1998	Document Analysis	Security, anonymity, and privacy in a consumer payment system
Davidson, 1997	Narrative Analysis	Project history review using research interviews
Ang and Endeshaw, 1997	Document Analysis	Legal analysis of disputes with IT management

Summarised and Adapted from: Trauth, 2001

Certain parts of this definition require further explanation; such that a proper framework can be established. This will be done throughout later sections of this chapter.

3.1.7 Summation

This section of the chapter discussed the major considerations involved when formulating a research methodology. Additionally, a general presentation of all major methods of research in information systems including the major advantages and disadvantages of each was presented. Finally, a thorough justification for an interpretivist research philosophy with a mixed methods sequential design including a grounded theory approach to this study was included. This provides a foundation for the actual content analysis (e.g. qualitative methods), as well as the parametric and non-parametric statistical analyses (e.g. quantitative methods) that will be employed over two stages during this project.

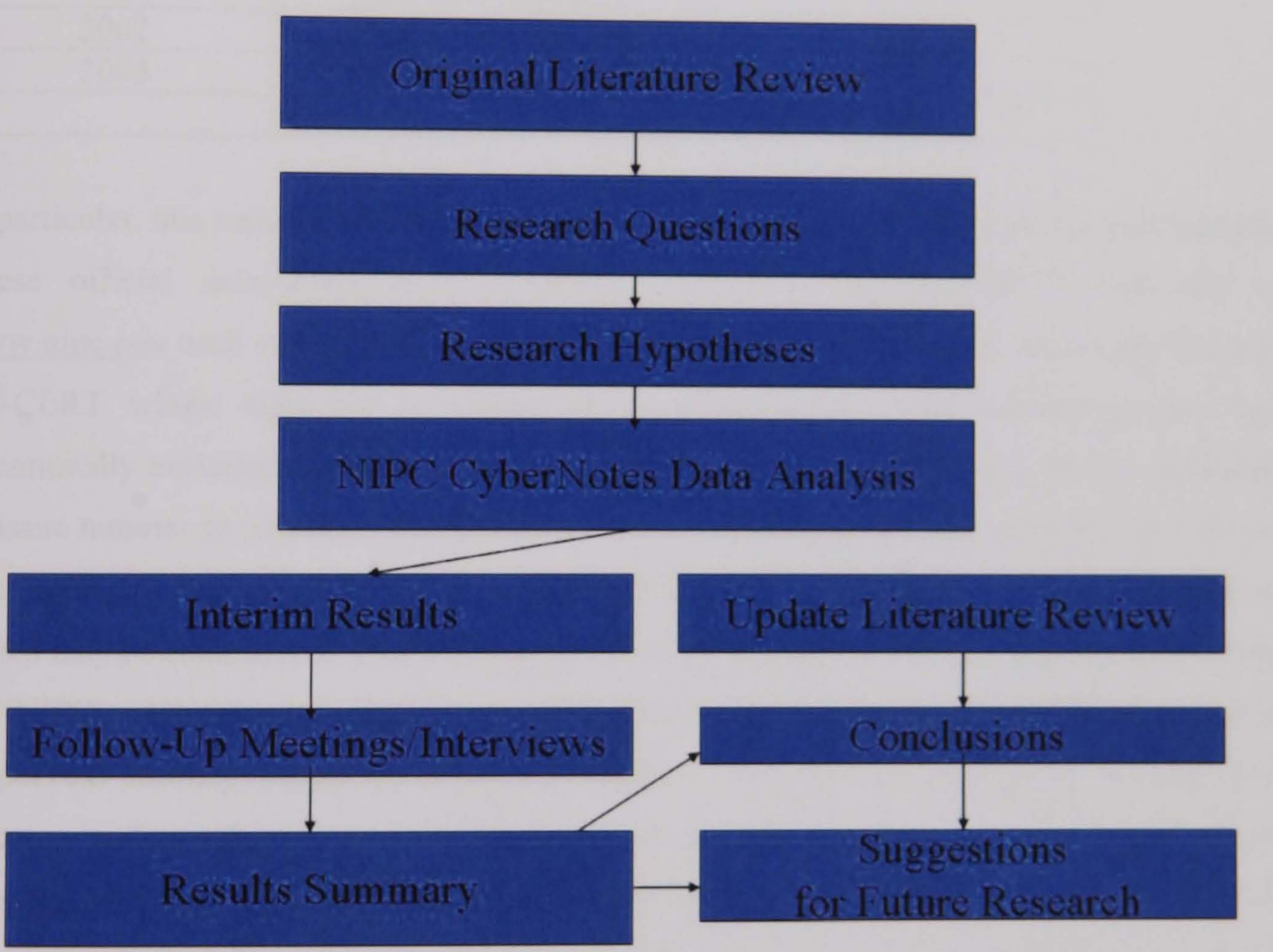
In the proper form, this research study includes a research model, a series of specific research questions and related hypotheses. Each individual research hypothesis was formulated in such a manner that it can be independently tested. Furthermore, the totality of this study provides evidence of the advancement of scholarly knowledge. as considered necessary and appropriate for the granting of a Doctor of Philosophy degree by Cass Business School of City University. The researcher developed a comprehensive research model for this project. This overall approach is discussed in greater detail in Section 3.5.

3.2 Scope of the Research Project

This research project will address the efforts of the National Infrastructure Protection Centre (NIPC) as it relates to providing cyber security information necessary to safeguard the U.S. Critical Infrastructure (CI). In the researcher's opinion, this organisation represents one of the most important initiatives of the United States Government related to cyber security.

In order to accomplish this formidable goal, a research model has been developed. This is shown in the following diagram:

Figure 3.1 – Overall Research Model



This framework was useful in guiding the researcher throughout the course of the project.

3.2.1 Data Collection

This data collection and analysis components are key aspects of this research project. Quantitative data analysis of the bi-weekly CyberNotes published by the NIPC is the main related activity. This is analysed for four years of NIPC operations from January 2000 though December 2003. See Supplement One for a sample copy of this newsletter.

During the research study, the researcher will examine the entirety of official publications for the time period identified. This total census approach will provide for extensive testing and overall consistency throughout the project. The sequencing of the CyberNotes newsletters is summarised in the following table:

Table 3.5 – Summary of NIPC CyberNotes Newsletters: 2000-2003

Calendar Year	Issue Numbers	Number of Newsletters
2000	2000-01 to 2000-25	25
2001	2001-01 to 2001-25	25
2002	2002-01 to 2002-25	25
2003	2003-01 to 2003-25	25
	Total	100

In particular, this research will make extensive use of the bi-weekly CyberNotes publications. These official newsletters were originally available from the NIPC's web site at www.nipc.gov until early-2004. At that time, their major responsibilities were transferred to US-CERT whose web site is located at www.us-cert.gov. This research project has intentionally excluded the yearly summary report for each year of the study; this is published as issue number twenty-six. The CyberNotes newsletters provide very detailed information about security vulnerabilities related to critical infrastructure protection. A small number of which may be addressed in other, more general advisory communications were also issued by the NIPC. All necessary documents were freely available in Adobe Acrobat© .pdf and HyperText Markup Language .html file formats. In order to develop an efficient and effective coding scheme the researcher through professional contacts obtained the MS-Word version of all files from the Federal Bureau of Investigation (FBI). This eliminated the need for a complicated file conversion process; thereby improving the overall efficiency of the research study.

In addition, in order to test some of the hypotheses other data needed to be gathered. All of this data will be obtained from appropriate U.S. Government agencies (e.g. Department of Labour, Department of Commerce and Department of Treasury), reputable consulting firms, such as Gartner Group, Yankee Consulting Group and the CERT/CC organisation. Any estimated values, assumptions, or limitations are properly noted in the appropriate chapter section.

3.2.2 Coding Procedures

The data from each of these publications was 'coded' solely by the researcher. In the summer of 2003, a preliminary codebook of study variables was prepared and discussed with the project supervisor. Since the researcher himself was intimately involved in this part of the project, perceived and actual bias was consistently considered. However, no related issues were observed and therefore not documented in Chapters Four and Five. Accordingly, issues related to inter-coder reliability did not need to be considered further.

Normally, this very important condition arises in large studies that employ many coders that are not very familiar with the data and are poorly compensated. To address these issues it is important to provide accurate instructions to all parties involved, test sub-sets of the data for consistency and avoid judgmental errors (Potter and Levine-Donnerstein, 1999; Krippendorff, 1986 and 1984). Another issue highlighted by Bradley (1993) is coder fatigue, while this is normally an important consideration it is expected to have little impact due to frequent re-checks of the coding and maintenance of a paper based audit trail by the sole coder.

In a content analysis study, coding is usually broken done into three elements (Criswell, 1998 and Krippendorff, 1984). First, open coding begins the process by identifying broad categories, properties and dimensions. Second, axial coding focuses on examining specific conditions, strategies and consequences. Finally, selective coding helps the researcher build a storyline. Ultimately, it is this stage that can form the foundation for theory development. This is very advantageous since the researcher can use different 'building blocks' (e.g. those developments from open and axial coding) to help him or herself hypothesise about an emerging theory or theories.

3.2.3 Data Analysis

Data from data repositories has been used in academic research for quite some time. This type of empirical research is an extension of primary data that is used for another purpose (e.g. not its original intent). This is commonly referred to as secondary data analysis. In other words, secondary data allows a researcher to work quickly within an emerging area, and not encounter significant time delays in creating or obtaining data themselves (Reidel, 2000 and Schwab, 1999).

Schwab (1999) explained in great depth the various benefits of secondary data analysis. His main points emphasise data availability and cost. Both of these qualities are particularly applicable to this research project. In particular, it will ensure easy access to the data, thereby allowing the researcher to proceed quickly.

Also important for the data analysis phase is the level of statistical power to be utilised. Baroudi and Orlikowski (1989) discussed how researchers in Management Information Systems (MIS) typically use a low level of statistical power. This can be problematic since according to their study, this situation can result in a forty percent chance of not detecting the phenomenon under study. To overcome this scenario, a number of their recommendations were followed in this research study. These include: increasing the sample size, improving the nature and type of statistical tests, and carefully selection of all study variables. Each of these issues is discussed in more detail in Section 3.2.5 below.

3.2.4 Quantitative Statistical Tools and Analysis

During the quantitative analysis stage, SPSS™ and SAS™, both highly regarded computer applications were utilised to manage the data. These computer software programs also assisted the researcher in executing parametric and non-parametric tests. A variety of statistical tests, correlations, and relationships were made, using a significance level of five percent.

Parametric tests are commonly known as traditional statistical tests. They are used to calculate ratios, levels of measurement, measure variances and distribution normality, and make inferential statistical tests (Brace, Kemp and Snegler, 2000). The original list of expected parametric tests to be executed included:

1. Trend Analysis;
2. Frequency Analysis;
3. Measures of Central Tendency;

4. Pearson's Product Moment Coefficient: and
5. Time Series Analysis:

According to Gibbons (1993, p.1), "Non-parametric statistics is a collective term given to the methods of hypothesis testing and estimation that are valid under less restrictive assumptions than classical techniques". The original list of expected non-parametric tests to be completed included:

1. Measures of Association;
2. Mann-Whitney-Wilcoxon;
3. Wilcoxon Rank Sum Test:
4. Spearman's Rank Correlation Coefficient: and
5. Shapiro-Wilk Goodness of Fit Test

Normally, academic research projects have to place reliance on statistical sampling methods. Statistical sampling allows researchers to test less than the entire population of items with mathematical accuracy. Conclusions are normally generalisable to other elements of the study. In these studies, a thorough discussion of the many different probability procedures and sampling methods is useful. However, due to the researcher's ability to test one hundred percent of the entire population only a brief summary of statistical sampling is included in the following table below.

Table 3.6 – Common Probability Statistical Sampling Techniques Used in Research

Type of Sample	Description and Sampling Procedure
Simple Random	Every individual in the population has an equal and independent chance of being selected for the study. The sample is obtained through selection by chance, and a table of random numbers, or computer generated random numbers.
Systematic Random	Based on the number needed in the sample, every Nth item in the population is selected for the sample. This can be used only if a randomly ordered list of the population is available.
Stratified Random	This is used when the proportion of subgroups or strata are known in the population: selection is random, but from each of these strata.
Proportional	The proportion of each subgroup within the sample is the same proportion of each subgroup within the population.
Non-Proportional	Regardless of the proportions in the population, the sample includes an equal number of individuals from each of the subgroups. The results are generalisable to the subpopulations rather than to the population as a whole.

	This sampling strategy is useful for populations in which some minority groups do not have a large enough proportion that can be represented if simple random sampling is used.
Cluster	Already formed groups within the population are selected as sampling units. Because the group is the unit of selection, a relatively large number of groups must be selected.
Multi-Stage Cluster	This combines the cluster sampling with others usually either simple random or stratified random techniques.

Adapted from Tashakkorri and Teddlie, 1998 p.75

Eventhough this study accommodated the entire census of CyberNotes newsletters from 2000 through 2003; some specific issues related to reliability and validity are applicable.

3.2.5 Qualitative Tools and Analysis

Qualitative tools such as AtlasTI™ can be used to execute content analysis based projects. Common qualitative tests that are likely to be made include: key word counts, word frequency lists, key word in context lists, concordances, single classifications, multiple classifications and others.

With the advent of personal computers in the later part of the twentieth century, researchers began to use computer software programs to conduct content analysis. Prior to that time, it was an intensive manual process. Coxon (1999) and Weber (1984) delineated three major advantages: improved reliability, speed and efficiency.

Furthermore, Weber (1990) and Krippendorff (1986 and 1984) discussed four primary issues related to the process of content analysis. The first such issue is measurement. Since the assignment of measured values will represent different aspects of the text (i.e. words, phrases, categories and themes) being analysed it is important to have a definitive coding scheme organised. In this regard, it is important to count all occurrences equally while giving consideration to the connotation of words. For instance, Weber (1990) classified 'bonus' and 'allowance' in the same category 'wealth' since both terms are connected with wealth. Secondly, the indication or inference made by the investigator of some unmeasured characteristic or quality of the text or the assigned numbers. Thirdly, representation covers the actual techniques used for describing the text's syntax or semantics. Finally, interpretation also needs to be considered. This issue normally is involved with the translating different elements into a common meaning.

Due to the timeframe for completing this project the original idea of supplemental qualitative research was aborted. However, this area is discussed in the Suggestions for Future Research section in Chapter Six.

3.2.6 Reliability and Validity Considerations

Reliability and validity are two critical considerations for a Ph.D. research project. The essence of reliability deals with the representations of variable measurements in real phenomena, discoveries of idiosyncrasies and potential biases in research procedures. In fact, Krippendorff (1984 p. 129) stated, "Reliable data, by definition, are data that remain constant throughout variations in the measurement process". Reliability does not guarantee the results of the research, but rather sets limits to the potential validity thereof.

Authorities in this area, primarily Potter and Levine-Donnerstein (1999), Weber (1990) and Krip6endorff (1984 and 1984), and Weber (1990) agree that reliability actually involves three distinct components. These are stability, reproducibility and accuracy. Firstly, stability involves the level of change in data over time. If multiple coders are involved in a research project an important consideration would deal with how these various coders interpret the instructions and data set(s). Other terms synonymous with stability are 'intra-coder reliability' and 'consistency'. Secondly, reproducibility deals with "the degree by which a process can be recreated under varying circumstances" (Krippendoroff, 1984, p. 131). This issue addresses the ability to re-establish the research results under different circumstances, such as using different coders, locating the coders in different locations or providing them with different instructions/guidelines. Reproducibility is also commonly referred to as 'inter-coder reliability', 'inter-subjective agreement' and 'consensus' amongst research professionals. Thirdly, accuracy is the strongest of all types of reliability. It covers issues related to conformity with standards and is useful when dealing with correct performance and measurement.

In terms of this research study, the concerns related to reliability are mitigated due to fact that only one coder, the researcher himself (previously discussed in more detail in Sections 3.2.2 and 3.2.3) and likely biases regarding the data and any limitations thereof (discussed in more detail in Chapter One). Another series of important factors focuses on validity.

Validity considerations cover issues related to correlating the research findings to real phenomena. Similar terms are 'empirical truth', 'predictive accuracy' and 'consistency with established knowledge'. Krippendorff (1984) discusses how these issues are important to all research studies. In this regard, these research-oriented recommendations can be particularly significant when evaluated and considered by a government agency or industry group. Therefore, if validity is addressed seriously since it assures a sound foundation for the recommendations developed in a research project.

Of the two main obstacles to validity, one is conceptual and the other is methodological in nature. The conceptual issue is internal reliability and this is synonymous with reliability (discussed in Section 3.2.6 above). The second issue is external validity which deals with the methodological component of validity. It covers the major issues of: semantical validity, sampling validity, correlation validity, and predictive validity.

In content analysis, semantic validity assesses the sensitivity of symbolic meanings. Potter and Levine-Donnerstein (1999) and Krippendorff (1984) agree that these issues are largely insignificant when a data gathering process is highly structured. This is true in this research project since 100% of the data is obtained from a single source in a highly structured process.

Sampling validity includes issues identical to the statistical sampling components included in Section 3.2.5 in this chapter. These are not applicable to this research study. Correlation validity deals with the how the research findings correlate with other findings by the researcher and/or other researchers. Predictive validity demands that the inferences borne out during the research study concur with the facts of the study, as directly observed by the researcher. In other words, the findings of the research must be based upon the work and related factual observations made during the study.

As with any research study, there are threats to the reliability and validity of this study. Potter and Levine-Donnerstein (1999) discuss three main threats. The first threat they identify is fatigue. When a researcher is fatigued quite simply he/she is more inclined to make more clerical errors than if they are well rested and alert. To counteract this issue, the researcher attempted to work on the research during regular work hours on days when he had no teaching commitments and took short, frequent breaks. The second threat that they discussed is the misapplication of coding rules. As mentioned previously, this issue was minimised because the researcher did most of the coding himself and used a pilot study approach to insulate against extensive re-work. Poor training is the last significant issue. To mitigate this situation, the researcher began conducting and interpreting preliminary analyses of the documents containing the secondary data for a number of months. This together with his years of practical experience in the field and recent training courses in SPSS™ minimised these specific risks.

All of the considerations about reliability and validity were adequately addressed in terms of the research design and corresponding methods. The information included in the limitations and benefits of the study, as included in Chapter One; provides additional related information.

3.2.7 Pilot Study

In order to test the coding process and variable descriptors the researcher will conduct a brief pilot study. During the summer of 2004, SPSS™ was used on a finite, three-month sample set of data. By testing one-sixteenth of the data, data handling procedures and revisions to the draft codebook was identified. Once this part of the research was done the discoveries and anticipated changes were documented and discussed with the Ph.D. supervisor before proceeding with the complete data set.

3.2.8 Follow-Up Procedures

There are two main reasons for follow-up work procedures. While it is important to consider the types and overall necessity of additional procedures that will complete the research project, these were not finally determined until after the data analysis stage.

The first purpose of follow-up work is to gain clarification on the interim results of the research study (Bradley, 1993). Some data analysis might produce clear results, whereas other analyses may produce ambiguous results that would benefit from further investigation. This particular type of additional work can be highly valuable when using a secondary data analysis approach (Scwab, 1999). Therefore, it was always anticipated that some limited follow-up work would be necessary.

Another function of follow-up work is that it can in of itself enrich the research study. Specifically, it can add value to the research by fully developing the recommendations. Furthermore, it can also help materialise the suggestions for future research presented by the researcher at the conclusion of the study. For all of these reasons, follow-up procedures were incorporated into the research model included in Section 3.2.

There are two types of follow-up procedures that will likely be utilised. The first group to follow-up with involves recognised IT security experts. Their practical and research experiences in the profession can assist the researcher by sharing other insights, new ideas and methodologies helping to make sure that the appropriate coverage to the study is concluded. The second group to assist with follow-up involves the Federal Bureau of Investigation's InfraGard program. Members of this group include federal cyber security investigators and industry computer security professionals that use and benefit from computer security communications, (e.g. including preventative warnings and corrective incident reports). This follow-up group is subject to program restrictions and related laws and regulations.

The researcher considered how follow-up work may be orchestrated. Three potential methods of handling follow-up were originally envisioned. These involve in-person interviews, telephone interviews and the dissemination of an on-line World Wide Web (WWW) based survey. The necessity of follow-up procedures was analysed at all critical stages of this project and required review by the researcher's Ph.D. supervisor.

3.3 Study Hypotheses

According to Locke, Spirduso and Silverman (2000) research questions guide the development of the research hypotheses. Various formats of research hypotheses such as null hypotheses and directional hypotheses can be utilised. In this study, directional hypotheses are used since they are in agreement with the exploratory nature of this grounded theory based project.

3.3.1 Introduction

The purpose of this section of the research study is to introduce the research hypotheses that will be tested. In addition, the hypotheses themselves must specifically be related to the research questions initially identified in Chapter Two: The Literature Review. Each research question is associated with multiple hypotheses in order to explore different dimensions of the formulated research question using different criteria.

3.3.2 Research Question Number One and Related Hypotheses

Research Question Number One:

How do the various types of NIPC advisory communications correlate to the nature and type of broad Internet security incidents as reported in the CyberNotes newsletter communications during the period of January 2000 through December 2003?

Hypothesis No. 1:

There is a defined correlation between the new 'critical' software bugs detailed in the NIPC's CyberNotes newsletters and the general number of new software bugs identified by the U.S. Computer Emergency Response Team/Coordination Centre (CERT/CC) and the U.S. National Institute of Standards and Technology (NIST).

Hypothesis No. 2:

There is a defined correlation between the number of critical computer viruses detailed in the NIPC's CyberNotes newsletters and the general number of computer viruses found 'in the wild'.

3.3.3 Research Question Number Two and Related Hypotheses

Research Question Number Two:

Did the number of critical infrastructure related security incidents as reported by the NIPC change from January 2000 to December 2003 based on U.S. Internet utilisation?

Hypothesis No. 3:

There is a positive correlation between the total number of U.S. Internet users and the critical cyber security infrastructure information reported by the NIPC.

Hypothesis No. 4:

There is a positive correlation between the number of U.S. based Internet host computers and the cyber security critical infrastructure information reported by the NIPC.

Hypothesis No. 5:

There is a positive correlation between the number of global World Wide Web (WWW) pages and the cyber security critical infrastructure information reported by the NIPC.

3.3.4 Research Question Number Three and Related Hypotheses

Research Question Number Three:

Do the computer security advisory communications of the NIPC during the period of January 2000 to December 2003 relate to the U.S. Electronic Commerce transactions?

Hypothesis No. 6:

There is a positive correlation between the total value of U.S. Electronic Commerce transactions and the cyber security critical infrastructure security information reported by the NIPC.

3.3.5 Research Question Number Four and Related Hypotheses

Research Question Four:

How do the various types of NIPC advisory communications correlate to various broad macroeconomic factors during the period of January 2000 through December 2003?

Hypothesis No. 7:

The NIPC's cyber security information communications is positively associated with various macro-economic factors such as: major interest rates, stock market indices, Consumer Price Index (CPI), Gross Domestic Product (GDP), inflation, and unemployment.

3.3.6 Research Question Number Five and Related Hypotheses

Research Question Five:

Do the computer security advisory communications of the NIPC during the period of January 2000 to December 2003 increase during U.S. military conflicts and political events.

Hypothesis No. 8:

There is an increase in the number of critical computer security advisory communications of the NIPC during time periods of military events; specifically 1) the attack on the USS Cole Battleship, 2) the War in Afghanistan, 3) September 11th Terrorist Attacks, 4) U.S. Invasion of Iraq, and 5) U.S. Military Intervention in Liberia.

Hypothesis No. 9:

The number of computer security advisory communications of the NIPC is positively associated with an increase during periods of domestic political change and crisis such as the: U.S. Presidential Election, Western States energy crisis, severe winter weather storms, and Northeast Blackout.

3.3.7 Hypotheses Summary

The research hypotheses represent a well-organised series of ideas. Each of which is specific, measurable criteria based on the research questions presented in this chapter. Additionally, all of the results of the hypotheses testing including the statistic techniques are described fully in Chapters Four and Five of this study.

3.4 Final Thoughts on Chapter Three

This chapter discussed the major issues and areas within the research methodology of the current study. First, a general introduction to the research philosophies in information systems was given. This section provided a basis for the next section, which addressed qualitative methods commonly used in this research domain. An overall research model which covered all of the main stages of the research project was also presented.

A number of different research approaches and designs were discussed. Next, justifications were provided for adopting a grounded theory approach was presented. Information about quantitative, qualitative and event study research methodologies was included along with details of sample prior related research studies. This chapter also discussed the data collection and analysis methods to be executed in the study. Furthermore, the critical issues of reliability, validity and inter-coder reliability were presented. This assisted the researcher is also developing a preliminary codebook that will be used in the study. Also, included in this section was an overview of the pilot testing approach adopted by the researcher. Furthermore, examples from a number of different areas in the social sciences were illustrated. This helped to highlight the common advantages and disadvantages of this particular technique.

For the quantitative methods used in the study were also discussed. This included an overview of parametric and non-parametric statistics to provide evidence of the traditional tests that were made from data coded into categories in the first stage of the research project. The original second stage of this project was removed and included in the Suggestions for Future Research section in Chapter Six.

In conclusion, this chapter provided diverse examples from previous social science and business research studies from highly regarded academic journal articles and other publications. These efforts were very beneficial to the research project and surely impacted the overall quality of the project.