City Research Online

City St George's, University of London

Citation: Hatzivasilis, G., Chatziadam, P., Petroulakis, N., Ioannidis, S., Mangini, M., Kloukinas, C., Yautsiukhin, A., Antoniou, M., Katehakis, D. G. & Panayiotou, M. (2019). Cyber insurance of information systems: Security and privacy cyber insurance contracts for ICT and helathcare organizations. 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), doi: 10.1109/CAMAD.2019.8858165 ISSN 2378-4873 doi: 10.1109/CAMAD.2019.8858165

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/23352/

Link to published version: https://doi.org/10.1109/CAMAD.2019.8858165

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

Cyber Insurance of Information Systems

Security and Privacy Cyber Insurance Contracts for ICT and Helathcare Organizations

George Hatzivasilis, Panos Chatziadam, Nikos Petroulakis, Sotiris Ioannidis
Institute of Computer Science FORTH
Heraklion, Crete, Greece
{hatzivas, panosc, npetro, sotiris}@ics.forth.gr

Matteo Mangini
Network Integration and Solutions (NIS) Srl.
Genova, Italy
matteo.mangini@nispro.it

Christos Kloukinas
Department of Computer Science
City, University of London
London, UK
C.Kloukinas@city.ac.uk

Artsiom Yautsiukhin
Institute for Informatics and Telematics (IIT)
Italian National Research Council (CNR)
Naples, Italy
artsiom.yautsiukhin@iit.cnr.it

Michalis Antoniou
HD Insurance (HDI) Ltd.
Athens, Greece
michalis.antoniou@hellasdirect.gr

Dimitrios G. Katehakis
Center for eHealth Applications and Sevices (CeHA)
Heraklion, Greece
katehaki@ics.forth.gr

Marios Panayiotou
Cablenet Communication Systems Ltd.
m.panayiotou@cablenetcy.net

***Abstract*—Nowadays, more-and-more aspects of our daily activities are digitalized. Data and assets in the cyber-space, both for individuals and organizations, must be safeguarded. Thus, the insurance sector must face the challenge of digital transformation in the 5G era with the right set of tools. In this paper, we present CyberSure – an insurance framework for information systems. CyberSure investigates the interplay between certification, risk management, and insurance of cyber processes. It promotes continuous monitoring as the new building block for cyber insurance in order to overcome the current obstacles of identifying in real-time contractual violations by the insured party and receiving early warning notifications prior the violation. Lightweight monitoring modules capture the status of the operating components and send data to the CyberSure backend system which performs the core decision making. Therefore, an insured system is certified dynamically, with the risk and insurance perspectives being evaluated at runtime as the system operation evolves. As new data become available, the risk management and the insurance policies are adjusted and fine-tuned. When an incident occurs, the insurance company possesses adequate information to assess the situation fast, estimate accurately the level of a potential loss, and decrease the required period for compensating the insured customer. The framework is applied in the ICT and healthcare domains, assessing the system of medium-size organizations. GDPR implications are also considered with the overall setting being effective and scalable.**

Keywords—insurance, security, risk analysis, certification, ICT, e-health, CyberSure, Event Calculus

I. Introduction

The increasing importance of the digital insurance market worldwide and the challenges arising in it are indicated by several studies [1], [2]. Recent surveys [2], [3] show significant trends, including: fast expansion, significant investment (e.g., €51M by multi-line insurers, €30M by property and casualty (P&C) insurers and €21M by life insurers), and dramatic increase in cyber insurance costs and premiums.

Cyber insurance and security certification have been effective and widely accepted means of managing uncertainty and risks, and establishing trust in the provision of cyber systems [4], [5]. Certification provides evidence of a satisfactory regular assessment of the provision of a service against protection mechanisms designed to mitigate security risks. Additionally, insurance i) establishes responsibility of covering the costs of re-instating service provision following interruptions or deviations from contractual obligations and/or regulatory standards, and (ii) can provide compensation for losses suffered by service consumers due to improper service operation (e.g., loss of personal or commercially sensitive data). Certification and insurance have been used as two instruments of risk mitigation and trust establishment in a wide spectrum of services and industries, such as the construction businesses, transportation, hospitality, Information and Communications Technology (ICT), healthcare, and services in the banking sector (e.g. [6], [7], [8], [9]).

From an insurance perspective, having cyber security certifications is a way to demonstrate that certain security controls have been implemented according to appropriate standards [4]. Thus, for certified products some insurance companies require reduced premiums [6], [10].

The substantial new revenue opportunities arising from the cyber insurance need to be complemented by large cost savings [11], [12]. Also, insurance will need to introduce more accurate risk assessments, behavior-based insurance contracts and dynamic pricing, and handle diverse consumer technology

This work has received funding from the European Union Horizon's 2020 research and innovation programme under the grant agreement No. 786890 (THREAT-ARREST) and the Marie Skłodowska-Curie grant agreement No. 734815 (CyberSure).

and frequent regulatory changes driven by new compliance challenges. These trends require more dynamic and automated creation, management and adaptation of cyber insurance policies, including dynamic risk assessment and dynamic pricing [12]. In addition, the costs of acquiring customers can be reduced by the use of analytics and increased insurance customization to the characteristics of the subject of insurance.

These requirements cannot, however, be addressed effectively at present [11], [13], [14]. More specifically, certification is currently carried out according to schemes based on labor-intensive inspection and offline testing of cyber systems at distinct time points (e.g. annually). Hence, it is costly and cannot guarantee the preservation of certified properties in between the certification audits. Furthermore, as the estimation of risk and creation of cyber insurance policies also take place at distinct periodic points (rather than continuously), they cannot take into account any changes in systems that may have happened in between. Also, in current practice, the estimation of risk and creation of insurance contracts do not consider detailed operational evidence obtained through continuous monitoring and testing. Thus, risk estimates might not be accurate and insurance policies might not be effective enough for the insurer and the insured.

The overall aim of CyberSure is to fill these gaps by developing an innovative framework supporting the creation and management of cyber insurance policies and offering a sound liability basis for establishing trust in cyber systems and services. This framework will be supported by a platform of integrated tools enabling:

1. the dynamic certification of the security and privacy properties of cyber systems and services that need to be insured,
2. the dynamic estimation of security and privacy risks for such systems and services, and
3. the development, monitoring, and management of the related cyber insurance policies for these systems and services based on (1) and (2).

Two indicative applications scenarios that exhibit different assessment features are considered, with CyberSure evaluating: i) the cloud services[1] in Cyprus that are offered by the Internet provider Cablenet to end-customers, and ii) the healthcare software suite[2] that is provided by an IT vendor (third-party) to a local hospital in Greece.

The rest of the paper is structured as follows: Section 2 outlines the related solutions of cyber insurance and their limitations. Section 3 presents the proposed CyberSure framework and its underlying components. The applied insurance model and the business innovation are detailed in Section 4. The evaluated organizations and their assessment are presented in Sections 5. Finally, Section 6 concludes the results of this work.

[1] CABLENET: cablenetbusiness.com.cy/public-cloud-services-for-business/cloud-server/

[2] CeHA: ics.forth.gr/ceha/FlipbookV1/CeHA.pdf

II. Background & Comparison with Related Work

Insurance tries to protect an organization or individual from economic loss, managing risk and uncertainty [15], [16], [17]. In the case of cyber insurance, we also need to assess the imposition of certain standards (i.e. for security, privacy, safety, dependability, etc.). This study focuses on the security and privacy aspects of an information system. Specifically, it concentrates in the insurance of ICT or healthcare organizations, taking into account the demanded compliance in Europe with the General Data Protection Regulation (GDPR) [18] and data offloading (e.g. [19]), respectively.

Today, there are several cyber insurance frameworks that are offered by international insurance stakeholders [2], [3]. Table I refers the most representative of them and summarizes their main features. CyberSure's insurance strategy extends the capabilities of the HDI cyber insurance modules.

TABLE I. Cyber Insurance Solutions

Product Name / Covers	*HDI (Cyber Sure)*	*AIG Cyber Edge*	*Allianz Cyber Protect*	*Chubb Cyber ERM / DigiTech*	*CAN NetProtect 360*	*Liberty Cyber*
Event management	**X**	X	X	X	X	X
Data protection liability – Third party liability	**X**	X	X	X	X	X
Cyber liability	**X**	X	X	X	X	X
Digital media	**X**	(opt.)	X	X	(opt.)	(opt.)
Network interruption	**X**	X	X	X	(opt.)	X
Cyber Exortion	**(opt.)**	(opt.)	(opt.)	X	(opt.)	(opt.)

The evaluated cyber threats [15], [16] include **i)** general attacks (e.g. malware, Denial of Service (DoS), etc.), **ii)** data breaches by hackers (i.e. security failures, unauthorized access, and employee negligence), **iii)** ransomware, impersonation fraud, phishing, whaling, spam/infected email, and **iv)** problems or exposure by collaborating third-parties. Fig. 1 illustrates the relevant statistics by claim type for HDI. For the examined ICT and electronic health (e-health) sectors, data breaches constitute the most severe threat (especially with the high fines for GDPR violations), while malware infection, ransomware, and exposure by third-parties are also important.

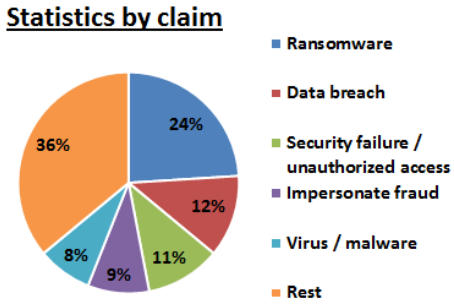

Fig. 1. HDI's statistics by claim

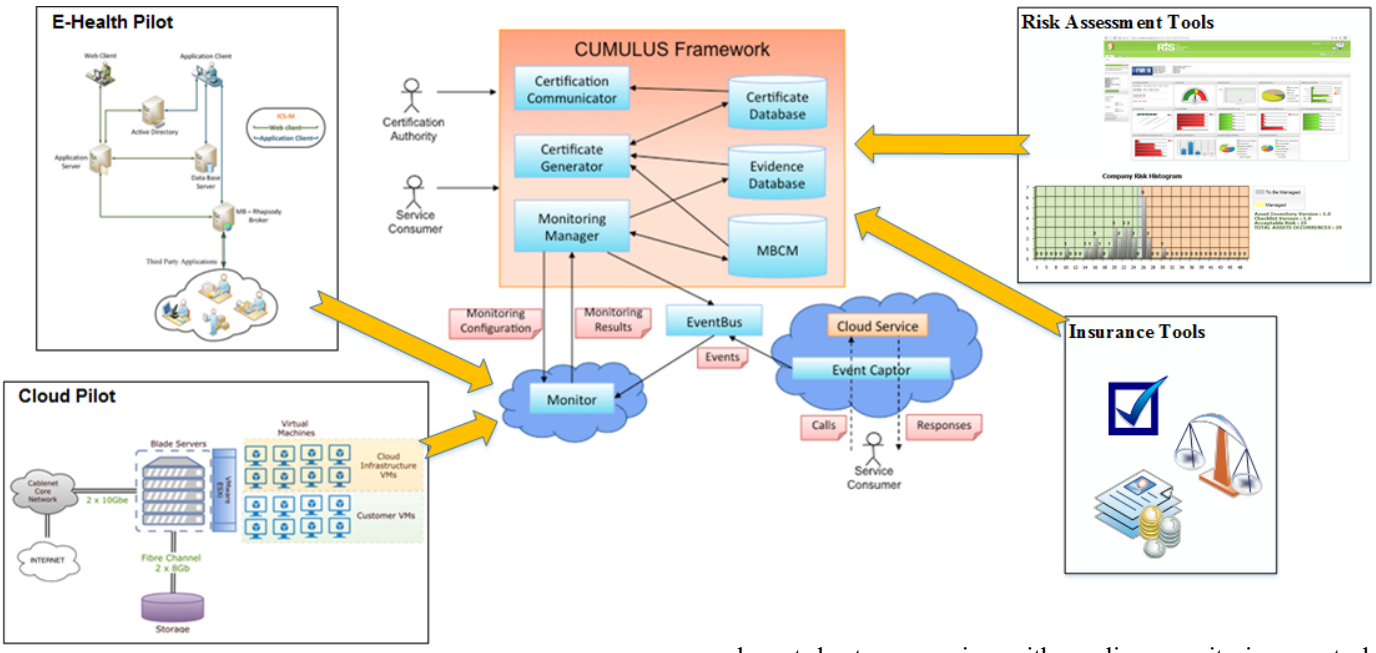

Fig. 2. CyberSure's deployment infrastructure

Insurance is not easy [11], [14]. The next challenges for incumbents include developing underwriting criteria and software solutions to handle coverage for types or classes the industry has no track record for, such as GDPR violations, drones, etc. Emerging areas of new business provide risk and potential return if the price is right. Emerging coverages, however, have potentially very different processing and billing requirements [13].

By relying on automated or semi-automated security certification and risk assessment, CyberSure develops a novel tool supported framework for cyber insurance. In this framework, insurance policies can drive certification procedures and be based on the outcomes of such processes, demanding specific attention to risks to be covered and relaxing the assessment of the risks that are not covered by the policy. The interaction between cyber insurance and security certification will also reduce the *information asymmetry* between insurers and clients. Automating cyber insurance management will also enable the generation of statistical data about risk assessment and rates of accidents, which will improve the maturity of the cyber insurance market.

III. The CyberSure Platform

This section describes the deployment infrastructure of CyberSure. It consists of four core components: i) the risk assessment tools (RIS[3] and NESSOS[4]), ii) the certification tool (CUMULUS [21], [22]), iii) the insurance tool (HDI[5]), and iv) the pilot systems (cloud and e-health platforms). The various components of the CyberSure platform are installed in the relevant host companies with on-line monitoring controls being deployed on the two pilot systems of the ICT provider and the healthcare organization, respectively. The involved systems are integrated, and common interfaces are implemented to enable the exchange of information. Fig. 2 depicts the deployment infrastructure of CyberSure, which is detailed below.

A. Risk Assessment

The two risk assessment tools that perform the baseline and comprehensive risk analysis are installed in the two host companies (the RIS tool in NIS and NESSOS in CNR). The ISO-27001 standard [20] and the GDPR [18] are disassembled into their underlying security and privacy controls, respectively. Then, security experts from these two companies interview the employees of a pilot system sequentially. For both tools, questionnaires and other information are completed on-line by the employees. The tools process the received data and the security experts finalize the risk assessment report.

The *baseline analysis* is performed with the RIS tool and the employees are requested to provide related information regarding the operational systems and the deployed controls. The tool assesses the maturity of these defense mechanisms and procedures, and estimates the probability of exploiting each one of them along with their criticality for the business operations. This initial documentation is provided to the evaluated organization along with a set of suggested system upgrades. The process is repeated for a more thorough analysis that examines the final compliance of each pilot system.

Then, a *comprehensive risk assessment* is performed via the NESSOS tool. The outcomes of the baseline analysis are given as input and the in-depth evaluation concentrates in the most vulnerable points of the system that exhibit high exploitation risk. In contrast to the general analysis of RIS that takes into account the possibility of facing specific security-/privacy-related events, NESSOS considers real incidents that

[3] RIS: https://dgsspa.com/pagine/15/ris
[4] NESSOS: http://www.nessos-project.eu/
[5] HDI tool: https://www.hellasdirect.gr/en/

have been recorded in the examined organization, the local market, or this economic sector in general. Such incidents may include equipment theft, electric power breaks, targeted malicious actions against this organization, and coordinated attacks in similar communities.

B. Certification Process

Thereafter, the on-line certification model and the underlying controls are deployed. These are the CyberSure's components that continuously monitor a pilot system, issue the certificate, and detect potential violations. They deploy CUMULUS certification models (e.g. [21], [22]) for this purpose and, based on automated (or semi-automated) certification carried out using them, they develop ways of dynamically adjusting risk estimates, insurance policies and premiums. In particular, the framework considers the case of dynamic certification, based on *continuous monitoring*, *dynamic testing* and hybrid combinations of them, *adaptation of cyber insurance policies* as the conditions of the cyber system operation evolve and new data become available, as well as *fine-tuning and adjusting the risk* associated to the insurance policies.

C. Insurance Contracts

Finally, the final risk assessment outcomes are parsed by the insurance tool that runs in HDI. Classified historical data regarding the considered risks are aggregated in the model together with other parameters, like discounts or penalizations. The insurance experts estimate the economic parameters of the potential insurance contract. *Risk diversification* is also estimated, meaning that, based on the monitoring portfolio, high-risk aspects are insured for higher price. The result is a set of contract offers that cover specific operational aspects and risks, providing several options from basic to full coverage of the economic loss. Each evaluated organization chooses one of them based on its needs and financial capabilities.

IV. Insurance Model & Business Innovation

A. The Insurance Model

The main target of CyberSure is to build a flexible economic model for publication and pricing decisions and create an automated insurance pricing model. The innovative methods for continuous certification and assurance assist the insurance organization to understand the impact of multiple variables regarding risk and loss, and price its products.

A *Generalized Linear Model (GLM)* is applied in order to estimate the economic value for a specific contract. The pricing formulas are described by equations (1-3):

$$Pricing = \sum_i Cover_i \quad (1)$$

$$Cover_i = Base_cover_i * \prod_j (1+factor_j) \quad (2)$$

$$Base_cover_i = f_i(main\ factors) \quad (3)$$

Where the main factors include core insurance criteria, like: **i)** revenue or asset value, **ii)** limits/deductible (reduce small and frequent claims, e.g. if the employees violate the security ISO and use default or weak passwords), **iii)** critical dependency of business processes on IT/Business interruption, **iv)** past claims (indicative of past security issues or past targeting), **v)** retention time (reward loyal customers), **vi)** type of industry (some sectors are more susceptible to attacks than others), **vii)** type of collected data (sensitive personal data, personal data, or other), and **viii)** for-profit/non-profit (hacktivist) targeting.

The '$Base_cover_i$' in eq. (3) and '$factor_j$' in eq. (2) are derived from the risk assessment process. They determine the prices, taking into consideration the relative risk of this customer for each cover.

The insurance model analyzes the interdependency and impact of multiple factors. It is applied for the prediction of risk and cost from the frequency and severity of claims that are related to specific customers. The impact analysis reveals opportunities to lower premiums for the identified lower-risk customers or to increase them for higher-risk ones.

With CyberSure in place, the overall insurance framework can take advantage of the continuous risk assessment and assurance in order to:

1. Provide the total expected loss for each customer (base pricing)
2. Estimate the risk of each cyber threat for each customer (per cover)
3. Assess how these factors are affected if we exclude small and very large claims (according to deductibles/limits)
4. Monitor if the customers adhere to the security rules
5. Deduce which covers/threats can be supported with higher confidence level
6. And specify which operations we can give (e.g. data protection liability)

B. Business Innovation

The platform provides new business services and opportunities of innovation, both for the organizations and the insurance companies that are involved.

1) Insured Organizations

The insured organizations benefit under this setting, as they are provided with accurate and more complete information regarding the real cyber security status, with suitable and effective suggestions for updating the current systems. The overall risk from disruptive and malicious events is reduced and the business operation is safeguarded against significant economic losses.

Whenever possible, the insured organization is provided warnings towards an upcoming violation of the certificate before the relevant event occurs. The insured organization is

alerted with timely and adequate information in order to take precautionary measures and avoid cyber-threats.

2) Insurance Companies

One main procedure is the collection of statistical data regarding cyber-threats for the specific economic sectors (i.e. healthcare or ICT). It becomes preferable for an insurance company to utilize the collected statistical information from the currently evaluated organizations in order to update its own database and take more robust decisions regarding its insurance models and policies. The insurance company gathers the data about various incidents that have occurred in the specific domains, based on the risk assessment procedures and the interviews of the accountable personnel that took place prior to the certification process. Then, the company updates the information in its own databases that are also considered as a main business asset.

The overall analysis and evaluation procedures of the examined pilot systems provide adequate information and assist the insurance company in order to establish a proper contract with low economic risk. The analysis takes into consideration the fine that is determined by GDPR (€20M or the 4% of the organization's budget). For the insurance company there have to be a decent profit for certifying a business while the economic risk should also be low.

If an incident occurs that is covered by a valid contract, the insurance company must estimate the loss and pay the agreed amount of money to the involved parties in a short period of time. In case of a cyber-security incident, as the CyberSure platform monitors the runtime operation of the pilot system, it verifies in a short period if the agreed policies had been followed or violated by the insured organization and facilitate the compensation procedure accordingly.

V. Application Examples

For the ICT case study, the cloud provider offers data-offloading services to its customers. It needs to insure its own operation and be protected against compensations that must be paid to the cloud users in case where an incident occurs (i.e. security breach) for which the provider is accountable. For the healthcare case, the hospital's management sector needs to issue an insurance contract between the hospital and the IT company CeHA (third-party which provides the software suite for the e-health services) in order to comply with the GDPR [18], regarding the privacy preservation and the prevention of unauthorized disclosure of health-related information. In both studies, we must guarantee that the main confidentiality, integrity, and availability controls, along with the role-based access to the sensitive personal data is enforced in all cases and the access rights are properly handled.

The key security, privacy, and dependability requirements for the two pilots include:

1. the preservation of privacy, confidentiality and integrity of customer data or medical records in-transit and at-storage
2. the preservation of privacy, confidentiality and integrity of financial data and prescription in-transit and at-storage
3. and the preservation of a high degree of the cloud platform and the e-health suite availability.

The integration of CyberSure and each insured system (Cablenet's cloud and CeHA's suite) must itself comply with these technical criteria. The CyberSure platform does not have access to confidential information (i.e. customers' data or electronic health records (EHRs)). Additionally, the monitoring components at the pilot-end do not collect information regarding the users'/patients' personal identifiable information (PII) and are compliant with the GDPR.

A. CyberSure's Monitoring Modules

The monitoring controls on the pilot system should capture the personnel's login behavior and inform the organization if it does not comply with the ISO-27001 security policy, e.g. the password strength is not sufficient, the passwords are not changed regularly, there many failed login connections, etc.

All collected data from the pilot system are anonymized in order to avoid any law violation (GDPR). Also, the service owners must grant their permission for the integration of the monitoring mechanisms with the CyberSure platform. If it is required, the service owners are also informed of the process.

In case where the contract insures the availability of the main servers during the working hours for each organization, the CyberSure platform should inform the beneficiary about the potential violation of the contract before the event really occurs, e.g., the server has not been maintained for some period and the possibility of malfunctioning during the next few days is high.

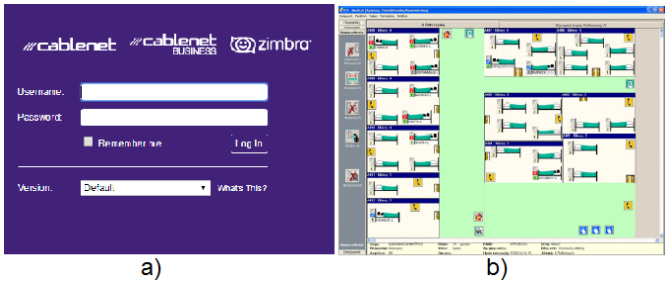

Fig. 3. The insured services for the two pilot systems: a) email service, and b) ward management

B. Server Availability SLA Example

Consider that one of the insured organizations needs to sign a service-level agreement (SLA) regarding the availability of the provided server, such as the servers' up-time, the EHR availability, and the volume of concurrently supported clients. The organization must guarantee a minimum delay in responding to availability issues for the provided client applications (Fig. 3). The off-time cannot exceed the agreed time during the insured period, as described in the corresponding service level agreement.

We issue a contract utilizing the extended version of CUMULUS. The initial evaluation lifecycle is for one year and the contract can be renewed in an annual basis. Every day the framework must monitor the availability of the system every half hour during the working period. The relevant SLA certification model (CM) is defined based on [21], [22].

The organization requests a certificate from CyberSure's certification authority based on this CM (see Fig. 2). The authority submits it to the certificate generator, which configures the monitoring infrastructure for starting the incremental certification process. It then calls the monitoring manager to find the monitoring infrastructure in the organization's end-devices. This monitor is a JAVA program that periodically checks the HTTP request status. The reasoning operation is modelled in Event Calculus [23], [24]. When the server is down, a relevant event is sent to CyberSure and the pilot system operator is warned about the potential contract violation. If the problem is fixed within the foreseen period, the monitoring status is restored. Otherwise, the contract is violated, and the accountable entity takes the responsibility.

VI. Conclusion

The digitalization of insurance procedures and the coverage of cyber assets have now become an emerging necessity. The European GDPR further stresses the need towards cyber insurance, especially for organizations that process high volumes of personal sensitive data. This article proposes a novel cyber insurance framework, called CyberSure. It tackles several limitations of the current solutions by deploying continuous certification and real-time assessment of risk and the contracted insurance policies. As a case study, CyberSure assesses the system of a medium-size cloud provider in Cyprus and a public hospital in Greece. The overall approach is effective and efficient, and reduces the possibility of potential security incidents, benefiting both the insurer and the insured.

Acknowledgment

This work has received funding from the European Union Horizon's 2020 research and innovation programme under the grant agreement No. 786890 (THREAT-ARREST) and the Marie Skłodowska-Curie grant agreement No. 734815 (CyberSure).

References

[1] W. Pritchett, "Insurtech 10: Trends for 2019," The Digital Insurer, KPMG, March, 2019, pp. 1-36.

[2] G. Matouschek, "InsturTechs – Reshaping insurance today," 27th congress of the International Association of Legal Protection Insurance (RIAD), Ireland, Dublin, 5-6 October, 2017, pp. 1-29.

[3] A. Marotta et al., "Cyber-insurance survey," Computer Science Review, Elsevier, vol. 24, May, 2017, pp. 35-61.

[4] P. H. Meland, I. A. Tøndel, and B. Solhaug, "Mitigating risk with cyberinsurance," IEEE Security & Privacy, vol. 13, no. 6, 2015, pp. 38-43.

[5] OECD, "Enhancing the role of insurance in cyber risk management," OECD Publishing, Paris, 2017, pp. 1-142.

[6] P. Millaire et al., "Latest industry trends in cyber security and cyber insurance," CyberCube, May, 2018, pp. 1-10.

[7] G. Hatzivasilis et al., "The CE-IoT framework for green ICT organizations," IEEE DCOSS, Santorini Island, Greece, 29-31 May, 2019, pp. 1-7.

[8] G. Hatzivasilis et al., "Real-time management of railway CPS," IEEE ECYPS, Bar Montenegro, 11-15 June, 2017, pp. 1-4.

[9] G. Hatzivasilis et al., "Review of security and privacy for the Internet of Medical Things (IoMT)," IEEE DCOSS, Santorini Island, Greece, 29-31 May, 2019, pp. 8-15.

[10] D. Woods and A. Simpson, "Policy measures and cyber insurance: a framework," Journal of Cyber Policy, Taylor & Francis, vol. 2, no. 2, 2017, pp. 209-226.

[11] P. H. Meland and F. Seehusen, "When to treat security risks with cyber insurance," International Journal on Cyber Situational Awareness, C-MRiC, vol. 3, no. 1, 2018, pp. 39-60.

[12] S. Romanosky et al., "Content analysis of cyber insurance policies: how do carriers price cyber risk?," Journal of Cybersecurity, Oxford Academic, vol. 5, issue 1, Feb. 2019, pp. 1-38.

[13] T. Bandyopadhyay, V. S. Mookerjee, and R. C. Rao, "Why IT managers don't go for cyber-insurance products," ACM Communications, ACM, vol. 52, no. 11, 2009, pp. 68-73.

[14] M. Eling and J. H. Wirfs, "Cyber risk: too big to insure? Risk transfer options for a mercurial risk class," University of St. Gallen, Institute of Insurance Economics, 2016, pp. 1-163.

[15] A. Arora and R. Telang, "Economics of software vulnerability disclosure," IEEE Security & Privacy, IEEE, vol. 3, issue 1, Jan.-Feb., 2005, pp. 20-25.

[16] J. Armin et al., "2020 cybercrime economic costs: No measure no solution," IEEE ARES, Toulouse, France, 24-27 Aug., 2015, pp. 701-710.

[17] F. Martinelli et al., "Preventing the drop in security investments for non-competitive cyber-insurance market," 12th International Conference on Risks and Security of Internet and Systems (CRISIS), Dinard, France, 19-21 Sept., 2017, pp. 1-16.

[18] Directive 95/46/EC – General DataProtection Regulation (GDPR), European Parliament and European Council, 2016: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679 .

[19] L. Gao et al., "Economics of mobile data offloading," IEEE INFOCOM, Turin, Italy, 14-19 July, 2013, pp. 1-6.

[20] Information security management systems, ISO/IEC 27001, 2013: https://www.iso.org/isoiec-27001-information-security.html .

[21] M. Krotsiani, G. Spanoudakis, and C. Kloukinas, "Monitoring-based certification of cloud service security," OTM Confederated Conferences On the Move to Meaningful Internet Systems, Phodes, Greece, Springer, LNCS, vol. 9415, 2015, pp. 644-659.

[22] M. Krotsiani, C. Kloukinas, and G. Spanoudakis, "Cloud certification process validation using formal methods," International Conference on Service Oriented Computing, Malaga, Spain, 13-16 Nov., 2017, pp. 65-79.

[23] E. T. Muller, "Commonsense reasoning: an Event Calculus based approach," M. Kaufmann, edition 2, 2015.

[24] G. Hatzivasilis et al., "AmbISPDM: Managing Embedded Systems in Ambient Environment and Disaster Mitigation Planning," Applied Intelligence, Springer, vol. 48, issue 6, pp. 1623-1643, 2017.