Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 7, Issue 2, 2019

State of the cyber insurance products within Slovenian insurance companies

Tina Kavčič, Faculty of Information Studies, Slovenia, tina.kavcic@gmail.com

Boštjan Delak, Faculty of Information Studies, Slovenia, bostjan.delak@fis.unm.si

Abstract

With the growing prevalence of cyber threats and cyber attacks enterprises have to manage their cyber risks. There are several risk strategies for cyber risk mitigation. One of them is to transfer the cyber risk to insurance companies through the so called "cyber insurance". Cyber insurance is an insurance package used to protect companies and individuals from Internet risks, Internet of things risks, and risks associated with information technology infrastructure and activities. It is estimated that approximately 85% to 90% of the cyber insurance market is located in the United States while the European market is estimated to account for approximately 5% to 9%. With the exception of the Baltic countries, smaller countries have problems raising cyber risk awareness within their countries. This paper describes the results of our survey on availability of cyber insurance products in Slovenia. Results show that currently only a few insurance companies even offer cyber insurance products. On the other hand, the survey shows that regulators did not issue any guidelines to insurance companies to develop such insurance products. The aim of our paper was to raise awareness about the potential of cyber insurance products among scholars, insurance stakeholders, regulators, and also among potential clients.

Keywords: Cyber threats, cyber risk, transfer the risk, cyber insurance, insurance products.

Introduction

According to Ponemon Institute (2018), the average global probability of a material breach in the following 24 months was 27.9%. Information Systems Audit and Control Association (ISACA)'s (2018) cybersecurity report, based on a survey among 2,366 participants found that 80% of the respondents predict that their enterprise will likely or very likely experience a cyber attack in 2018. Due of constant business changes, developing new methods and work procedures, with information system support, which is more global from day to day, with inclusion in the global cyberspace, leading companies to new information systems risks/cyber risks (Kennedy, 2017).

European countries vary in their cyber risk resilience and in their approach to or readiness for cyber insurance products. With the exception of the Baltic countries, smaller countries have problems raising cyber risk awareness within their countries and preparing various procedures for transferring related cyber risk or mitigate it. Global Cybersecurity Index 2018 ranked the UK as the leading country on cybersecurity, followed by the United States and France, while Slovenia ranked 48 (ITU, 2018).

Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation (ISO, 2009). Risk mitigation strategies include: avoidance, acceptance, sharing/transfer, and mitigation (ISACA, 2013). According to ISACA, risk sharing/transfer means reducing risk frequency or impact by transferring or otherwise sharing a portion of the risk. Common techniques for risk sharing/transfer include insurance and outsourcing. Zhao, Xue, and Whinston (2009) defined cyber insurance as a range of first-party and third-party coverage that enables companies to transfer their security risks of the commercial insurance market. European Union Agency For Network and Information Security (ENISA) (2012) further described cyber insurance as insurance market covering first and third party risk relating to cybersecurity. Consequently, cyber insurance has 'captured the imagination' of many involved in cybersecurity at the policy and research level, as a mean to transfer these financial risks to third parties (Böhme & Schwartz, 2010).

This paper describes the current state on availability of cyber insurance products among insurance companies and brokers in Slovenia. This paper is organized as follows: first we present the aim of our research, our hypothesis and our research questions, followed by a literature review and the presentation of research methodology. Finally, we discuss the results and concluding remarks.

Aim of this Research

The aim of this paper was to analyze and describe, the availability of cyber insurance products in Slovenia and what insurance products Slovenian insurance companies offer to Slovenian companies to mitigate cyber threats. The goal of our research was to determine how many insurance companies already offer cyber insurance products to their customers - companies. We also wanted to check if the Slovenian Insurance Association and/or Slovenian Insurance Supervision Agency issued guidelines for cyber insurance products to insurance companies.

Our hypothesis is:

Insurance companies in Slovenia are not yet ready to offer cyber insurance products to companies.

Related research questions (RQ) are:

RQ1: *Are Slovenian insurance companies offering only insurance products of information sources against successful cyber threats?*

RQ2: *Are cyber insurance products in Slovenia offered to companies only through agents (insurance brokers) of foreign insurance companies?*

RQ3: *Did the Slovenian Insurance Association and/or Slovenian Insurance Supervision Agency issue insurance guidelines on cyber threats to insure company?*

Literature Review

The insurance industry has been quantitatively assessing risks for hundreds of years in order to minimize risks and maximize profits. The World Economic Forum noted in its 2014 Global Risk

Report that there would be considerable opportunity for the nascent cyber risk insurance market to evolve and mature (WEF, 2014). Cyber insurance is an insurance product that is used to provide levels of protection to companies and individuals from cyber risks associated with information technology infrastructure and activities. According to Bandyopadhyay (2012), cyber insurance refers to the specific insurance contracts that provide coverage against loss from theft of data and information system assets. Shackelford (2012) identified cyber risk insurance as a tool to manage liability exposure and mitigate the hazard of cyber attacks. He indicated that investment in cyber risk insurance should be a recommendation to businesses to enhance cybersecurity, but proactive cyber strategies should always be the starting point. In 2016, ENISA estimated in that global cyber insurance market will reach $7.5 billion in annual sales by 2020 and over $20 billion by 2025. Ishaq (2016) stressed that enterprises are beginning to consider cyber insurance as a component of their risk transfer strategy. Ogbanufe, Kim, and Takabi (2016) explored how top managers assess usage of cyber insurance to protect the company's information assets. Young (2016) in his thesis presented a framework which incorporates the operating principles of the insurance industry in order to provide quantitative estimates of cyber risk. Talesh (2017a) wrote that insurance companies play a critical role in assisting companies to comply with privacy laws and deal with cyber theft. In the cyber context, the insurance industry tries to engage in loss prevention and does so in a manner that is focused on managing and averting the risks associated with data breaches. Talesh (2017b) argued that insurance companies do not offer simply pooling and transferring risk, but are heightening the security systems of companies and preventing any data loss.

The United States (US) Department of Homeland Security (DHS)'s report concluded with observing that cyber insurance is vital: "A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection" (DHS, 2017, para. 1). Simply knowing what issues to consider when purchasing a cyber insurance policy is one of the most difficult challenges for consumers.

Mukhopadhyay, Biswas, and Pal (2018) presented a novel framework that computes the insurance premium to be paid by the firm depending on the intensity as well as the likelihood of a phishing attack. According to DiGrazia (2018), cyber insurance policies are a relatively new insurance product, especially as a stand-alone insurance policy, and that they generally cover first-party losses because of a cyber-event. He also wrote that insurance companies must remain aware of the overall potential exposure that companies have to a cyber attack.

While the market for cyber insurance is generally perceived as being in its infancy, specific cyber insurance products have been available for nearly 20 years in some countries, particularly in the United States (OECD, 2017). The size of the stand-alone cyber insurance market in 2016 is estimated to be in the range of $2.5 billion to $3.5 billion in gross written premiums and is estimated to be 85% to 90% of all worldwide gross written premiums, while the European market is estimated to account for approximately 5% to 9% ($150 million to $400 million in gross written premiums). An estimated EUR 90 million of gross written premiums originated in Germany and EUR 30 million in France (OECD, 2017). The implementation of the General Data

Protection Regulation (GDPR) in the European Union could lead to significant growth in the cyber insurance product adoption with some reports suggesting that the EU market could eventually equal the size of the US market (Marsh, 2016).

Franke (2017) reviewed 15 Swedish insurance companies, which sell cyber insurance products and found, that cyber insurance is not merely an instrument of risk transfer, but also contains aspects of avoidance and mitigation. The products are quite similar in covering both first party costs, e.g. from business interruption, and third party liabilities e.g. from data breaches. However, there are important differences in the coverage of non-malicious events, which could lead to complications. Insurance companies impose information and information system security requirements on their customers, and insurance pricing and underwriting nudge customers in to increase security, although practices vary between insurance companies (Franke, 2017).

In 2016, the Republic of Slovenia has published Cybersecurity Strategy. It includes the objective of "cybersecurity in an economy" with two measures: promotion of development and introduction of new technologies in the field of cybersecurity and regular awareness raising programs on cybersecurity for business entities (Digital Slovenia, 2016). Global Cybersecurity Index (GCI) for 2018 shown that Slovenia has scored 0.701 and has ranked 48 from 175 countries at global list and ranked 30 from 46 countries at regional Europe's list (ITU, 2018). Table 1 shows the top 10 countries in the global list.

Table 1. GCI's Global Ranking – Top 10 Countries

Rank	Country	Score
1	United Kingdom	0.931
2	United States of America	0.926
3	France	0.918
4	Lithuania	0.908
5	Estonia	0.905
6	Singapore	0.898
7	Spain	0.896
8	Malaysia	0.903
9	Canada	0.892
9	Norway	0.892

Slovenian Computer Emergency Response Team (SI-CERT) established in 1995, issues an annual report on network security. In 2017, SI-CERT dealt with 2,300 security incidents which is seven times higher as in 2008, when SI-CERT prepared the first report (SI-CERT, 2018). Because of all stated above, we had decided to review if mitigation of cyber risk by insurance companies had been introduced in Slovenia. We conducted an analysis of the state of cyber insurance and cyber insurance products in the county.

Methodology

This research was conducted by a survey methodology based on the questionnaire with open and closed questions (the complete questionnaire is presented in Appendix 1). The questionnaire was sent to the selected insurance companies in Slovenia. Slovenia is a small insurance market. At the time of our survey, only 13 insurance companies operated in the Slovenian market. Of these, we have only included seven universal insurance companies in our survey, as the other insurance companies are specializing only in personal, health or car insurance. We have also included two insurance brokers, as they were offering special information system insurance through specialized European insurance companies.

The population of the survey was seven insurance companies and two insurance brokers. Both insurance regulators have been contacted by an e-mail. The survey was open from November 21st 2018 to January 20th 2019. We have collected six responses from insurance companies and two responses from insurance brokers.

Results

Currently, only one insurance company offers cyber insurance products to companies. Insurance policies for large companies are individually tailored to their needs and custom made. In October 2018, the same insurance company additionally launched a more standardize product targeted at SME 'Insurance of cybersecurity for small and medium enterprises'. One insurance company offers cyber insurance only for individuals, this insurance is imbedded in insurance coverage under non-life insurance products. Two insurance companies were developing cyber insurance products at the time of our survey. Two other insurance companies did not offer special cyber insurance products, and one company did not respond to our questionnaire. We have also received responses from both insurance brokers we have contacted. They offered special cyber insurance products from abroad (mostly from the UK). Brokers sell cyber insurance products through seminars, conferences, newspaper articles and interviews. Brokers also offer personal contact with the customers and provide them with specific brochures where information security and cyber insurances are presented in a simplified format. Table 2 shows the survey results.

Table 2. Survey Results

Status	**A number of insurance companies**			
	Offer	**Under development**	**Do not offer / will not offer**	**No answers**
Cyber insurance product for corporate	1	2	2	1
Cyber insurance products for individuals	1	N/A	N/A	N/A

N/A – not applicable

The results collected from received questionnaires are:

The insurance company A – Cyber insurance for corporate clients

The only insurance company in Slovenia that offers cyber insurance to companies provides both: the cover of first-party claims (own damage) as well as the coverage of third-party claims (liability insurance). The insurance company offers two insurance coverages with several functionalities:

- Basic coverage: the response a cybersecurity incident; the cost of restoring data and software; liability for breaches of confidentiality and privacy; liability for network security.
- Additional coverage, such as: operational delays (loss of profit during the period of business interruption); cyber extortion (including ransom cost); and cybercrime (coverage of unlawfully collected funds).

The response to the cybersecurity incident covers the costs of an expert to carry out an investigation and prepare a report. Coverage includes damages for personal data protection breaches. The recovery of the cost of restoring the system involves restoring data and software after a cybersecurity incident. Responsibility for breaches of confidentiality and privacy is to cover costs incurred by third-party or employee compensation claims for breach of data protection in respect of confidential or personal data or for breach of applicable personal data protection legislation. In addition, all legal costs are covered by liability for confidentiality and privacy violations. This insurance company also covers costs for network security responsibility, which covers the costs associated with the cybersecurity incident, theft of data, or an unreachable/denial of service attack on third-party computer systems. The responsibility for network security, however, includes all legal costs. The cyber insurance covers all costs associated with the ransom paid by the insured and all the expenses for the resolution of cyber attacks.

Before the insurance company prepares the offer, the corporate company must complete a questionnaire, which includes seven sub-areas: general information about the company and its activities; quality and quantity of data, activity and services; outsourcing of services; information system security; history of damages actions, damage balancing services and information on insurance cover.

The insurance company B – Cyber insurance for individuals

Another insurance company offers insurance products for privately owned personal computers and covers costs of damages incurred in the case of a ransom ware attack. The insurance product covers the cost of restoring the computer's performance due to infection and the cost of ransom paid. The computers that serve for business purposes or are the property of third parties are not covered.

Others insurers

The brokers answered that they cover damages caused to third parties and their own damage.

We inquired how insurance companies assess the client's cyber threats. The insurance brokers assess cyber threat readiness of their potential clients by using different approaches, including: client statement, questionnaires, and expert assessments on the client's state of cybersecurity. On the basis of the results, the insurance companies may also ask additional questions to which the policyholder must respond if he receive a binding offer. In the case of major clients or more complex risks, an insurance company may also additionally request "Risk Survey" done by the insurance company's cybersecurity expert.

None of the respondents provided answers to the question of what type of methodologies (NIST, ISACA, ENISA, own) they are using. The findings of the survey were that around 270 companies had shown interest within the last six months for cyber insurance products, which is approximately 2.7% of all companies in the country.

Discussion

All Slovenian insurance companies do not yet offer cyber insurance or risk insurance against cyber attacks, while those Slovenian insurance companies who do cover the damages caused to third parties as well as their own. On the other hand, we have to mention that no serious cyber attacks had yet occurred in Slovenia neither by hostile nation-states nor by organized crime. The Slovenian Ministry of Public Administration stated only two major cyber incidents in its report (2018). The first occurred between February 4th and February 17th, 2012, when the hacktivists group Anonymous initiated several distributed denial-of-service (DDoS) attacks on government websites, tried to hack into the public administration systems and some websites debugging, and the second major incident occurred between May 12th and May 15th 2017 – by WannaCry ransomware attack. Officially, only eight companies were affected by this ransomware attack, it did, however, include a large factory.

ENISA (2016) research had shown that insurers identified the following core challenges: lack of cybersecurity incident data, gathering information on cybersecurity management, customers less likely to share any documentation and uncertainty around their accumulating risk. We got similar findings from those Slovenian insurance companies which do not offer cyber insurance products yet. The UK Department for Digital, Culture, Media, and Sport (DCMS) (2018) wrote that small minority of businesses (about 9%) have a specific cybersecurity insurance policy. In Slovenia, due to low awareness of cyber risk and cybersecurity only 2.7% of the companies had shown interest in cyber insurance products.

Our research has shown resemblance with Talesh (2017b) findings, as also Slovenian insurance companies are not only tools for pooling and transferring risk, but also offer counseling, training etc. The obtained results show that only a few insurance companies offer cyber insurance, but we could answer negatively to first research questions (RQ1) as both insurance products offer more than only information source against cyber threats. The similar negative answer is to the second research question (RQ2), as parallel to two insurance brokers, who offer insurance products from foreign insurance companies, also one Slovenian insurance company offer cyber insurance products to corporate clients. As have checked with regulators and we can also negatively answer to the last research question (RQ3), while Slovenian Insurance Associations and Slovenian Insurance Supervision Agency have not issued any guidelines against cyber threats to

insurance companies yet. We can confirm our hypothesis, that insurance companies in Slovenia are not yet ready to offer cyber insurance products to companies.

Conclusion

The aim of our research was to analyze and describe, the availability of cyber insurance products in Slovenia and what insurance products Slovenian insurance companies offer to Slovenian companies to mitigate cyber threats. The functioning and even the very existence of a modern society are inextricably linked to the continuous and reliable operation of information systems and networks. The ever-faster development of information and communication technologies, on the one hand, brings the benefits of a modern society, on the other hand, it influences the emergence of ever new and technologically more complete cyber threats. One way to manage the risk is transferring it to insurance companies as it is also suggested by the World Economic Forum (WEF, 2014). At the time of our research, only one insurance company out of seven offered cyber insurance products for companies and one insurance company offered cyber insurance product for individuals. Two insurance companies were developing cyber insurance products.

The purpose of our study was also raising awareness about the potential of cyber insurance products among scholars, insurance stakeholders, regulators and also among potential clients. On the other hand, we would like this paper to alert management of the regulators to prepare guidelines how insurance companies should handle cyber threats and also alert management of insurance companies to develop and prepare new insurance products to cover cyber threats.

The presented research has had some limitations. Firstly, the number of filled-in questionnaires we received was below our expectation. We have planned to receive complete answers from all Slovenian insurance companies, we could include in our research. But on the other hand, Slovenia as a small country with a small number of cyber threats until now, and only total of seven out of 13 insurance companies is a significant limitation of this study. Secondly, we have concentrated only to one European country - Slovenia, due to the lack of resources preventing us, to enlarge survey to all Central and Eastern Europe insurance companies. Third, our questionnaire has not been focusing on a specific size companies, as we have asked insurance companies regarding their support to any company independent to size, type and ownership structure.

This research was the first analyze of state of cyber insurance in the country. The results could be a good basis for further analyses and researches in this field. Responses to some of the questions might require additional specific questions to be added and develop an expanded and detailed questionnaire for further researches. Similar or even enlarged research can be repeated within two or three years to follow-up on the development of cyber insurance products in Slovenia. Another possibility is to enlarge the survey to wider areas, maybe to all Central European countries or even to whole European Union, which would require solicitation for collaboration with other researchers and analyze their status. The fourth possibility, of further research is to analyze cyber insurance products for specific customers (large enterprises, small and medium enterprises, public companies, individuals).

Our finding could increase the awareness of scholars, insurance top management, stakeholders and also their clients for the situation regarding cyber risk transfer to the insurance companies. Risk transfer is one possible approach to manage risks, while others are more complex and require much more resources. Cyberspace is becoming more and more complex and we have to monitor it regularly to better understand current risks and study new ones.

Acknowledgement

We would like to thank to Faculty of Information Studies, Novo mesto, Slovenia, for the support provided to us with this study. We would also like to thank to KM2019 and OJAKM reviewers, who gave us comments and suggestions for improving this paper.

References

Bandyopadhyay, T. (2012). Companal adoption of cyber insurance instruments in IT security risk management– a modeling approach. *Proceedings of the SAIS 2012*, Article 5. Retrieved from http://aisel.aisnet.org/sais2012/5.

Böhme, R., & Schwartz, G. (2010). *modeling cyber-insurance: Towards a unifying framework, working paper*. Harvard: Workshop on the Economics of Information Security (WEIS) Harvard, USA.

DCMS. (2018). *Cybersecurity breaches survey 2018: Statistical release*. UK, Department for Digital, Culture. Media and Sport, UK. Retrieved from https://www.gov.uk/government/statistics/cybersecurity-breaches-survey-2018.

DHS. (2017). *Cyber insurance*. Department of Homeland Security, Washington, USA. Retrieved from https://www.dhs.gov/cybersecurity-insurance

Digital Slovenia. (2016). *Cybersecurity startegy – establishing a system to ensure high level of cybersecurity*. Digital Slovenia, Ljubljana, Slovenia.

DiGrazia, K. (2018). Cyber insurance, data security, and blockchain in the wake of the Equifax breach. *Journal of Business & Technology Law*, *13*(2), Article 5. Retrieved from http://digitalcommons.law.umaryland.edu/jbtl/vol13/iss2/5

ENISA. (2012). *Incentives and barriers of the cyber insurance market in Europe.* European Union Agency For Network and Information Security, Heraklion, Greece.

ENISA. (2016). *Cyber insurance: Recent advances, good practices and challenges*. European Union Agency For Network and Information Security, Heraklion, Greece.

Franke, U. (2017). The cyber insurance market in Sweden. *Journal Computers and Security*, *68*(C), 130-144.

ISACA. (2013). *COBIT5 for Risk*. ISACA, Schaumburg, Illinois, USA.

ISACA. (2018). *State of cybersecurity 2018 - part 1: Workforce development*. ISACA. Schaumburg, Illinois, USA.

Ishaq, S. K. (2016). Cyberinsurance: Value generator or cost burden? *ISACA Journal*, *5*.

ISO. (2009). *ISO/IEC 31010:2009 risk management – risk assessment techniques*. International Organization for Standardization, Geneva, Switzerland.

ITU. (2019). *Global cybersecurity index (GCI) 2018 (draft)*. ITU Publication. International Telecommunication Union. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.

Kennedy, C. (2017). New treats to vehicle safety: How cybersecurity policy will shape the future of autonomous vehicles. *Michigan Telecommunications and Technology Law Review, 23*(2). Retrieved from https://repository.law.umich.edu/mttlr/vol23/iss2/4/

Marsh. (2016). *Continental european cyber risk survey: 2016 report.* Marsh LLC, Maroussi, Greece..

Ministry of Public Administration. (2018). *Assessment of cybernetic risks* (in Slovene language) version 1.0. Republic of Slovenia, Ministry of public administration, Ljubljana, Slovenia.

Mukhopadhyay, A., Biswas, B., & Pal, S. (2018). C-R-P-M-I: A framework to model cyber risk from phishing and mitigation through insurance. *Proceedings of the 24th Americas Conference on Information Systems,* New Orleans, USA. Retrieved from https://aisel.aisnet.org/amcis2018/Security/Presentations/27.

OECD. (2017). *Enhancing the role of insurance in cyber risk management*. OECD Publishing, Paris, France. http://dx.doi.org/10.1787/9789264282148-en.

Ogbanufe, O., Kim, D. J., & Takabi, H. (2016). Top manager's perspectives on cyberinsurance risk management for reducing cybersecurity risks. *Proceedings of the 22nd Americas Conference on Information Systems*, San Diego, USA. Retrieved from https://aisel.aisnet.org/amcis2016/ISSec/Presentations/10/.

Ponemon Institute. (2018). *2018 cost of data breach study: Global overview*. Ponemon Institute, North Traverse City, Michigan, USA.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 349–356.

SI-CERT. (2018). *Annual report on network security 2016-2017*. SI-CERT, ARNES, Ljubljana, Slovenia (in Slovene language).

Talesh, A. S. (2017a). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry. 43*(2). Retrieved from https://www.researchgate.net/publication/318164430_Data_Breach_Privacy_and_Cyber_Insurance_How_Insurance_Companies_Act_as_Compliance_Managers_for_Businesses_Data_Breach_Privacy_and_Cyber_Insurance.

Talesh, A. S. (2017b). Insurance companies as corporate regulations: The good, the bad, and the ugly. *DePaul Law Review*, *66*(2), Article 7. Retrieved from https://via.library.depaul.edu/law-review/vol66/iss2/7.

WEF. (2014). *Global risk 2014 (9th ed.) insight report*. World Economic Forum, Geneva, Switzerland.

Young, D. R. (2016). A framework for incorporating insurance into critical infrastructure cyber risk strategies. Air Force Institute of Technology, *Theses and Dissertations. 329*, Retrieved from https://scholar.afit.edu/cgi/viewcontent.cgi?article=1328&context=etd.

Zhao, X., Xue, L., & Whinston, A.B. (2009). Managing interdependent information security risks: A study of cyberinsurance, managed security service and risk pooling. *Proceedings of the 2009 International Conference on Information Ssystems, paper 49*.

Authors Biographies

Tina Kavčič is MSc candidate at the Faculty of Information Studies–Novo mesto Slovenia. Since September 2011, she has been employed at the Agency for Agricultural Markets and Rural Development of the Republic of Slovenia, in the IT department where she is involved in the management of information projects and the processing of spatial data. Informatics is an area that has always been interested in and inspiring.

Boštjan Delak, Ph.D. is auditor at the Republic Slovenia Court of Audit, Ljubljana, Slovenia. He is a certified information system auditor and certified information security manager, he is also assistant professor at the Faculty of Information Studies –Novo mesto, Slovenia. He is lecturing: IS auditing and Fundamentals of Information Security. His research interests are: IS due diligence, IS analysis and Knowledge management.

Appendix

Questionnaire

1. In what way does your insurance company offer insurance against cyber threats to medium-sized or large companies?
2. What kind of insurance / collaterals covers your insurance company for cyber risks?
3. How do you to check the insured's willingness to cyber threats?
    a) If you have replied to the preliminary questions in an affirmative manner, would you please indicate how you check the insured's willingness, and do you perhaps use any of the following procedures or methodologies?
        i. By statement,
        ii. By questionnaire,
        iii. By expert opinion on cybersecurity.
    b) If you use the methodology, please specify which:
        i. From NIST,
        ii. From ISACA,
        iii. From ENISA,
        iv. Your own,
        v. Other: _____ (please, specify).
4. What kind of insurance do you offer from cyber threats:
    a) Insurance of resources,
    b) Insurance of data (data protection),
    c) Insurance of services,
    d) Insurance of people.
5. Has your insurance company already met an injured party who was subjected to material and information damage from a cyber source and in what way did the insurance company recover the damage?
6. How does your insurance company cooperate with forensics and cybersecurity experts?
7. How many small / large companies have in the past been interested in insurance against information loss or from cyber threats?
    a) Less than 10,
    b) From 10-50,
    c) From 51-99,

d) 100 or more.

8. Does the International Insurance Association provide guidelines for the preparation of offers for cyber insurance?
9. Does the Slovenian Insurance Association give guidance on the offers for cyber insurance?
10. If your insurance company is part of a major holding, how you're holding give you guidelines in the direction of cyber insurance?
11. Why do you think that companies do not insure their information resources at your insurance company?
12. Do you see within The Slovenian Act on information security Article 5 your active role as the contractor of essential services?