International Conference at the Brno University of Technology,
Faculty of Business and Management, September 16-17, 2021 Brno, Czech Republic
Perspectives of Business and Entrepreneurship Development: Digital Transformation for Business Model Innovation

A systematic literature review of cyber security insurance

Nikola Sunavcova[a,*]

[a] Brno University of Technology, Faculty of Business and Management, Kolejni 2906/4, 612 00 Brno, Czech Republic

Abstract

Purpose of the article This paper is a systematic review of the literature. It describes and compares insurance options in the field of cyber security, especially from the perspective of small and medium-sized businesses. It also points to possible shortcomings and weaknesses in this area.

Methodology/methods To fulfill the main goal of this article, I used the method of secondary research. I used a system approach, which was based on the structured collection of the necessary data, in order to obtain as much relevant information in the field in order to achieve an overview of the state of scientific knowledge of insurance issues in the field of cyber security.

Scientific aim The main goal of my article is to identify insurance options (in the field of cyber security) for small and medium-sized companies based on a search of scientific literature. Compare possible types of insurance and reveal trends in this area. A partial goal of my contribution is to identify the shortcomings and threats that cyber security insurance brings.

Findings In the article, I analyzed the insurance options. I also looked at the shortcomings in this area. From the information obtained, I concluded that insurance in the field of cyber security is still quite high, on the other hand, it is becoming more and more popular with companies. This finding is mainly based on the fact that the business environment has recently undergone changes, which include, in particular, digitization, work with large amounts of data and the constant development of efficiency and speed.

Conclusions The whole article is a systematic review of the literature, which provides the reader with an overview of cyber risk insurance. The article contains a more comprehensive view of the solution to cyber security through insurance. This article also points out the shortcomings of cyber insurance and contains current trends in this area.

Keywords: cyber security, insurance, IT security, cyber security insurance, business environment

JEL Classification: M15, M21

[*] Corresponding author.
E-mail address: xpsunav00@vutbr.cz

Introduction

The time in which we live is closely connected with the concept of digitization of information, when the company massively deploys devices that are permanently connected to the Internet and where various cloud information systems and web services are implemented. Trends today are leading to a sharp increase in online software-driven devices in industry, transportation and other diverse industries around the world. Due to this transformation, the requirements for cyber security are becoming more and more deep into the day-to-day management of companies, as the digitization of information creates space for new threats and risks from which companies must protect themselves.

In recent years, cyber risk has been a growing and growing global threat. While it is true that digitalisation is revolutionizing business models and changing everyday life, it brings with it room for cyber-attacks that are a growing threat to businesses (Lloyd's 2017). This statement is substantiated, for example, in the report of the World Economic Forum on Global Risks of 2018. This report ranks cyber attacks and massive fraud with data among the top five risks of 2018 (WEF 2018). Therefore, organizations try their best to eliminate cyber risks, even though they can never achieve 100% security. Furthermore, the finding that investing in cybersecurity is often ultimately more costly than the benefits of incremental security for a company should be taken into account (Gordon and Loeb, 2002). Therefore, those responsible for preventing cyber threats within their company must also consider the costs and benefits of investing in cyber security.

In addition to investing in activities that prevent or reduce cyber security breaches (e.g. firewalls, intrusion detection systems, data encryption, employee training, etc.), companies can also invest their funds in cyber security insurance. Cyber security is a means of transferring some cyber security risks to another organization (Herath and Herath, 2011). Even more so, cyber security insurance allows an organization to transfer part of the risk associated with the actual cyber security breach at a certain cost. However, as insurance companies seek to make a profit, they set cybersecurity premiums in line with the risks they take when writing insurance contracts (Lawrence D. Bodin et al., 2018).

The primary ability to insure against cyber security risks is to transfer cyber security risk in order to mitigate the impact on organizations. However, cyber insurance is generally expected to have other positive effects (Lawrence D. Bodin et al., 2018). Probably the most important advantage of cyber insurance is to provoke companies to invest more in their own protection in order to reduce premiums (Toregas C et al. 2014). Majuca, R. P. (2006), in turn, states that cyber insurance can improve social well-being by improving the overall cyber level, and Anderson, R. et al. (2006) expressed the idea that cyber insurance can serve as an indicator of the quality of protection.

1 Motivation and aim of the paper

As part of a collaboration on a project, I dealt with the issue of cyber security insurance. From a review of the scientific literature on the subject, I have noticed that very few scientific articles focus purely on insurance. Many articles contain sections related to the issue of cyber security insurance, but there is little literature that focuses purely on a summarized view of this area. This motivated me to provide my view on the issue related to a comprehensive review of the literature. With this article, I would like to point out the current state of insurance in the cyber security area, outline current trends and future directions in the area and point out the shortcomings and weaknesses of insurance.

2 State of the cyber insurance market

In this part I will focus on the development of cyber insurance. I will describe some historical knowledge in the field of cyber security insurance and then describe the current procedures and the current state in this area.

2.1 Risk management and statistics of cyber attacks

Cyber insurance is generally a way of managing risks. Therefore, if we want to understand insurance, we should first describe and define risk management (Vaughan, 2007).

Alberts et al. (2001) characterized risk as the possibility of suffering harm or loss. For the first time, a definition appeared in their article, emphasizing that risk is not certainty, but the possibility that risk will arise in the future. The occurrence of a risk is then called an incident. Strupczewski (2018) confirmed this definition by arguing that cyber risk is essentially a loss, disclosure or breach of the relevant data. This may be the result of harmful or unintentional conduct, as well as negligence, and may be performed by internal personnel such as employees or contractors, or by external actors, such as a hacker or former employee.

The possibility of risk occurrence depends on two aspects. The first is threat and the second is vulnerability. The threat describes the cause of the risk, such as a kidnapping, a natural disaster, or a leak of confidential information. Vulnerability is an existing weakness that can be exploited to create an incident. Thus, we can argue that risk is a combination of threat, vulnerability, and impact that indicates the loss to the firm that the incident has caused (Marotta et al., 2017).

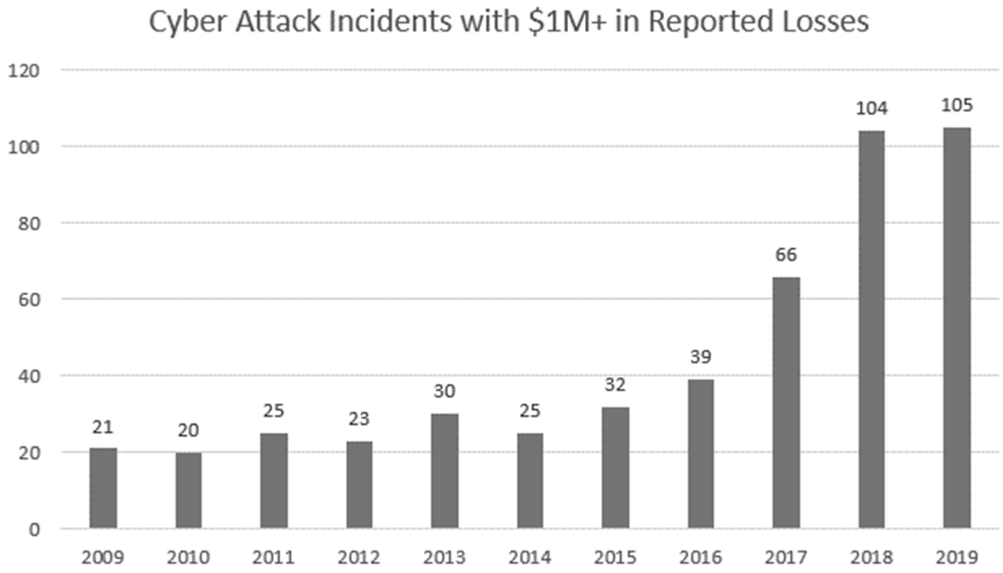
Every company should include in its strategy the possibility of the occurrence of risks that may disrupt the proper functioning of the company. This process is called risk management and is characterized as a process by which we are able to identify risk and implement plans to address it (Alberts et al., 2001).

This process consists of a sequence of activities, which are: risk identification, risk assessment and risk treatment. Risk identification characterizes threats, vulnerabilities and the impact of risk. The risk is assessed using a risk analysis that takes into account two parameters: the probability of the incident occur-ring and its degree of impact. Risk treatment is then the selection and subsequent implementation of measures by which the company can prevent risk. There are four basic alternatives:

- Risk reduction, by introducing measures that help reduce risk.
- The transfer of risk is the transfer of part of the potential losses to another organization.
- Risk avoidance is the decision to avoid a risk event.
- By accepting the risk, the firm accepts the possible consequences of the incident, mostly be-cause the risk cannot be prevented or the cost of taking measures against the risk is higher than the consequences that the incident would cause (Alberts et al., 2001).

Cyber insurance is therefore one of the ways (risk transfer) of risk management by which a company can prevent risk. The development of cyber attacks is therefore very closely linked to insurance itself. Businesses should first take out insurance against the threats that are most likely to occur or can cause them the most losses. Therefore, when it comes to cyber security insurance, it is appropriate to deal with the statistics of cyber attacks themselves.

Many statistics show the development of cyber attacks (incidents) in recent years, some are even regular in terms of counting from year to year. As an example, I will mention one such statistic of cyber attacks, which we can monitor from year to year. This is the number of cyber attacks that reported losses in excess of $ 1 million (Crane, 2020).



Source: (Crane, 2020)

Figure 1 Statistic of cyber attack incident

It is clear from the graph that the number of cyber attacks is growing from year to year and this trend is not changing in any extreme way. Until 2016, this increase was not entirely clear, but between 2016 and 2017 we can already see an obvious increase, which was repeated between 2017 and 2018.

The year-on-year increase in attacks is also confirmed by Kurmaiev (2020), who in his publication pre-sents a table showing the number of cyber attacks on American companies.

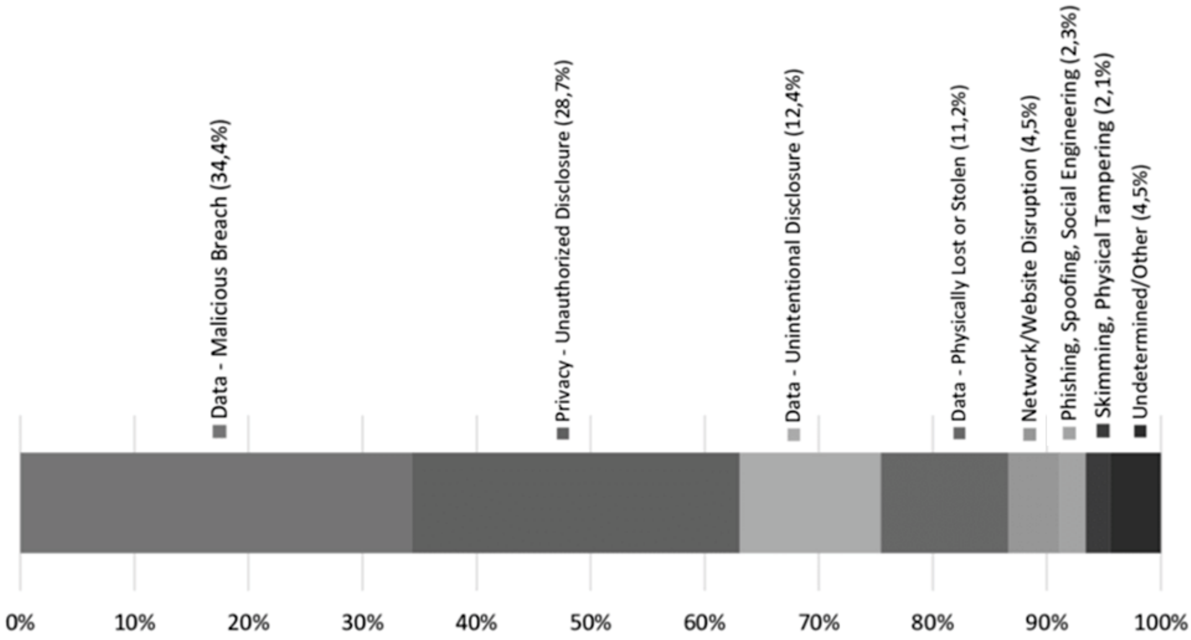
Table 1 Correlation of Cyber-Attacks

Year	Losses [USD]	Number of cyber attacks	Price of one cyber attack [USD]
2015	1 070 700 000	288 012	3 717,55
2016	1 450 700 000	298 728	4 856,26
2017	1 418 700 000	301 580	4 704,22
2018	2 706 400 000	351 973	7 689,23

Source: Federal Bureau of Investigation, 2019

The table shows that in the United States, losses related to cyber attacks increased more than 2.5-fold during 2015-2018, although the number of cyber attacks alone increased by only 22% (Kurmaiev, 2020).

Of course, the rise of cyber-attacks means that companies have to look for new ways to protect themselves from attacks in order to prevent financial or other losses. However, if the protection of compa-nies against cyber attacks is to be effective and efficient, it is necessary to look at what types of attacks are most common. Strupczewski (2018) presented following statistics in his work. He stated that the vast majority of cyber events / attacks (86.6%) were related to data processing (a more detailed breakdown is shown in the figure below). Network and website interruptions account for 4.5% of total cyber events, while phishing and other related cyber attacks account for only 2.3% of cyber attacks.



Source: own work based Strupczewski (2018)

Figure 2 Cyber event count by type

Strupczewski (2018) further states that if we compare statistics that include the average cost of a parti-cular type of cyber event and statistics on the number of attacks in different areas, the results will differ. The most costly type of cyber event seems to be an IT processing error ($ 78.2 thousand). The following incidents also represent significant average losses: phishing ($ 23.1 thousand), network / web interruption ($ 18.7 thousand), IT configuration errors ($ 16.9 thousand). The average cost of a malware breach is ap-proximately $ 10,000.

The conclusion of the statistics is that the largest losses in cybersecurity have been caused by network or computer interruptions and privacy-related incidents will not be reflected in the company's financial losses to the extent that might be expected (Strupczewski, 2018).

2.2 Cyber insurance

Already in the late 1970s, specialized reports on cybercrime appeared (Majuca, 2006). In 1990, security software companies began working with insurance companies to offer insurance packages that consisted of software and insurance (Lelarge, 2006). The first stand-alone insurance contracts appeared in 1998. The contracts were against hacker attacks, introduced by the International Computer Security Association (Kabay, 1998).

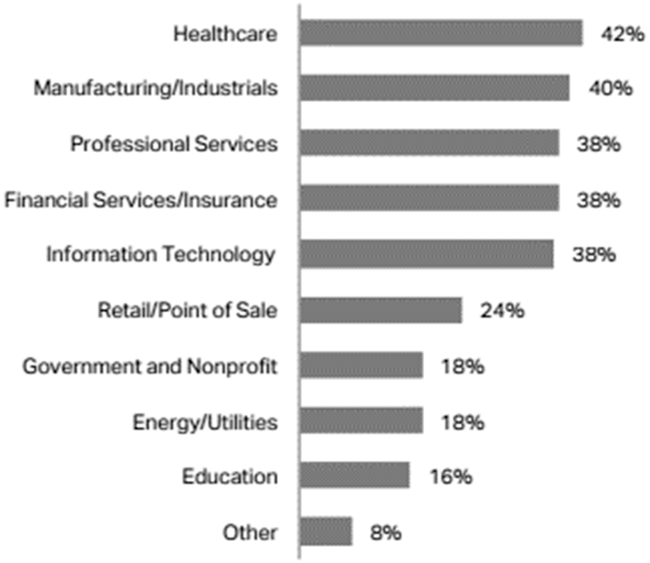
Since then, the cyber security insurance market has expanded considerably. One of the main aspects that is helping to expand this area is large-scale cyber attacks, which have caused great losses in the past. Some estimates suggest, for example, that the attack from February 2000 cost affected companies up to $ 1.2 billion (Gohring, 2002). Of course, companies are responding to the information about these attacks by wanting to protect themselves from them, thus increasing the demand for protection against the risks. Insurance companies have subsequently responded to this fact by developing the necessary products to satisfy the emerging needs of companies (Harrison, 2000).

Along with the expansion and development of the industry, the definition of cyber insurance was specified, described by Gartner (2015) as “protection against losses related to cyber risks such as data theft / loss, business interruption due to a computer failure or virus, and fines or lost revenue due to system failure, network intrusion or breach of information security.

When we look at the statistics and compare the European cyber security insurance market with the US market, there are several articles that confirm that the US market is by far the largest cyber insurance market, accounting for 90% of global premiums (AON, 2017). This statement is supported, for example, by Eling (2016), who claims that the American market is much more developed than its European counterpart. In his publication, he also stated a possible reason for this state of affairs. He states that the USA has for several years had requirements in place for reporting cyber attacks with relatively high fines for their violations. The new regulations have significantly raised awareness of cyber risk and increased demand, especially for third-party coverage. Several policies that already exist in Europe are more focused on covering first-party information.

Evidence of the constant growth of cyber insurance is offered by several sources. One of them is the Betterley Risk survey, which was conducted in 2014. This survey showed that gross premiums for cyber insurance in the US in 2013 amounted to 1.3 billion and in 2014 it was already 2 billion, which represents an increase by 10–25% per year (Betterley, 2014). Romanosky et al. in 2019, they again stated in their publication that the total cyber insurance market in the United States in 2016 was $ 2.49 billion and approximately $ 3.0 billion in 2017. Some estimates even indicate that by 2025 it may be as much as 20 billion dollars.

Although the US market is more widespread than the European market, there is still room for growth in cyber insurance in the US. Because only about one-third of American companies have purchased some type of cyber insurance (Romanosky, 2019). For example, barely 5% of manufacturing companies have cybernetic insurance coverage, while the healthcare, technology and retail sectors have achieved acceptance at almost 50% (Romanosky, 2019). The representation of companies that have purchased cyber insurance by sector is also shown in the figure below.



Source: PartnerRe & Advisen, 2018

Figure 3 Industry segmentation of cybersecurity buyers in 2018

The survey shown in the graph clearly shows the sectors with the highest interest in cyber insurance. For example, Chubb already provides a product called Cyber Security for Healthcare Organizations, which offers coverage for cyber risks related to medicine (Marrota, 2017). In fact, from the 145 insurance events related to data breaches analyzed by Greisinger (2013) in his report, the most frequently infringed sector was healthcare (29.3%). Other market sectors that are interested in cyber insurance are manufacturing, professional services, financial services, information technology, retail, etc.

3 Problems of cyber insurance

The cyber security insurance market is generally not meeting the expected results. This is also shown by the forecast from 2002, when the global cyber insurance market was expected to be worth $ 2.5 billion in 2005 (Kesan, 2004). However, this forecast turned out to be erroneous, as this forecast value was not reached even in 2008 (when it was even 5 times lower than the forecast for 2005) (Böhme, 2010).

The fact that this market is not growing at the rate expected is not that there is no need for potential in this area. From the information I obtained during the research of the professional literature, I assume that the reason for the difference between the expected values and the real ones are critical obstacles that have not yet been completely solved.

Wang (2019) cites a possible reason why cyber insurance faces such major obstacles. In his publication, he argued that the reason was the inherent nature of cyber risk insurance. This claim was based on several other articles that addressed the inherent challenges of cyber insurance (e.g., Eling and Schnell, 2016).

3.1 Critical barriers to the growth of the cyber insurance market

In this part of the article, I will describe the basic obstacles to market growth in the field of cyber insurance, which I encountered in a systematic analysis of the literature related to cyber insurance.

The first problem I encountered is the lack of historical data on losses. Only 19% of insurance companies have a claims history of more than 10 years (Strupczewski, 2018). According to surveys, the average number of years for which information on cyber attacks is available is 7 years (Strupczewski, 2018). The lack of statistical evidence can also be explained by the possibility of keeping evidence of an incident hidden (Marotta, 2017). Insufficient representative collection of statistical data is also related to this problem, due to the lack of similar systems that would be able to share data with each other (Marotta, 2017). In the absence of statistical data, the risk may then be underestimated. An example is the resumption of re-insurance in April 2018, when reinsurance prices in the event of excessive losses on the Internet fell by 5% - 10% due to the lack of large claims from which companies would draw the necessary statistics (Strupczewski, 2018).

As Wang (2019) states in his publication, the prices of insurance products are determined on the basis of actuarial tables, which are derived from a large amount of historical data, and this is another obstacle in the field of determine prices of cyber insurance. It may be almost impossible for a company to determine the right price for cyber insurance because the expected cyber loss depends on the actual level of cyber security investment over the life of the insurance contract (Wang, 2019).

The problem is not only determining the exact price or amount of insurance but also the unpredictable impact of the incident. The first problem with estimating the damage to cyber risks is that much of its impact is intangible. More and more assets of individual companies represent intangible assets, which are of high value, essential for business and are more exposed to cyber risk than tangible assets. However, determining the price of an intangible asset is particularly challenging (Strupczewski, 2018). The second problem is that the impact of the event can vary significantly from company to company (Marotta, 2017). This fact was also mentioned by Kurmaiev et al. (2020) in his publication, in which he argued that the individual nature of pricing for insurance services is indeed one of the problems of cyber insurance.

Another problem I have encountered in several publications is the ambiguity of insurance coverage. If we take into account the global cyber insurance market, we find that it is relatively complex. It has more than 600 insurance contract forms offered by more than a hundred insurance companies worldwide. These contracts contain different wordings and inconsistent interpretations of the scope of insurance coverage. This fact is crucial for companies because it creates uncertainty. Companies are losing confidence that their insurance policy guarantees protection against cyber-attacks (Wang, 2019). The problem of so called silent risk is also related to the unclear formulation of insurance contracts. This problem arises when traditional insurance contracts do not explicitly cover or exclude certain cyber risks. When an incident occurs, it is then difficult to determine the coverage of the insurance contract (Strupczewski, 2018).

Moral hazard is also a problem that companies should think about. This problem is related to the fact that if a company buys cyber insurance, it will reduce its investment in security (Strupczewski, 2018). Thus, the motivation to invest more in countermeasures that reduce the likelihood of loss is lost (Wang, 2019).

Eling et al. (2016) also raised the issue of the fact that existing insurance contracts cannot cover extreme scenarios well. This is due to the large number of exclusions and the dynamic nature of cyber risk.

The lack of experience and standards in the field of cyber insurance is also a problem. Because cyber insurance is a new type of insurance, insurance companies do not yet have standardized procedures. Therefore, contracts often differ, and this problem then reflects the language ambiguities in individual contracts (Toregas et al., 2014).

4 Opportunities for the growth of the cyber insurance market

From the information already contained in this article in previous sections, it follows that one of the opportunities is extreme cyber incidents. Insurance companies usually provide coverage for common incidents, but insurance for extreme incidents is lacking. Disclosure of information on extreme cyber-attacks could raise awareness of cyber-threats in the future, leading to a higher level of companies requiring cyber-threat insurance.

In his publication, Strupczewski (2018) also stated three possible directions for future development in the cyber insurance market. These are opportunities that would take this area to a higher level and thus increase interest in cyber risk insurance.

As a first step, he gave a clear definition of which insurance contracts deal with cyber risk. Related to this is the standardization and simplification of language in the field of cyber insurance. Increasing the clarity of the language would also increase customer awareness and understanding of cyber risk insurance itself.

The second direction is to introduce cyber insurance as a service (not just coverage). The issue of cyber insurance is so complex that it should not just mean a simple transfer of risk. The purchase of cyber policy should now add value to the organization by offering additional services such as risk consultation, monitoring and risk assessment, or prevention. This is also related to a close relationship with the customer.

The third direction and at the same time the next stage of development of cyber insurance could be cyber insurance of persons. This would be driven by the need to ensure the security of human privacy, financial resources and property of individuals.

Conclusion

In this paper, I have described a comprehensive view of the literature related to the field of cyber insurance. I have systematically described the historical development of cyber insurance and summarized statistics related to cyber risk. Since insurance is a way to prevent risk (by transferring it to another object), these two concepts are closely related and it is right that I mentioned in the article the statistics and development of cyber risks, as well as the development of cyber insurance . The historical development of cyber insurance has shown that this market is not growing as fast as previously expected. This is primarily due to the obstacles that prevent the sector from growing faster.

Despite the fact that the growth of the cyber insurance market is not growing according to historical estimates, there has been a year-on-year increase in the conclusion of insurance contracts in recent years. The reason, in my opinion, is that cyber insurance in itself provides a unique opportunity to cover risks and also to contribute to the well-being of society. It is clear from the literature that, although cyber insurance is desirable and increasingly preferred, this area has many open issues that need to be addressed. Therefore, new approaches and standards are needed to achieve market maturity. Finally, I listed possible directions that could solve the basic problems in the field of cyber insurance. I have described some solutions to the problems that actors in this area should focus on in order for cyber insurance to continue to be a growing market.

Acknowledgment

This article and the results achieved were supported by a grant within the project Quality Internal Grants of BUT (KInG BUT), Reg. No. CZ.02.2.69 / 0.0 / 0.0 / 19_073 / 0016948, which is financed from the OP RDE.

References

ALBERTS, CH. J., DOROFEE, A. J. (2001). *OCTAVE Criteria*. Technical Report.

ANDERSON, R., MOORE, T. (2006). The economics of information security. *Science*, 314(5799), 610-613. Doi 10.1126/science.1130992

AON (2017). Glob*al cyber market overview. Uncovering the hidden opportunities*. Retrieved from http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

BETTERLEY, R. S. (2014). Cyber / privacy insurance market survey – 2014: "Maybe Next Year" Turns into "I Need It Now". Betterley Risk Consultants. ISSN 1089-0513.

BÖHME, R., SCHWARTZ, G. (2010). Modeling Cyber-Insurance: Towards a Unifying Framework. In *WEIS*, 36 p.

Crane, C. (2020). *42 cyber attack statistics by year: A look at the last decade*. InfoSec Insights. Retrieved from: https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/

ELING, M., SCHNELL, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 5(17), 474-491. Doi 10.1108/JRF-09-2016-0122

FEDERAL BUREAU OF INVESTIGATION (2019). *IC3 annual report released*. Retrieved from: https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219/

GOHRING, N. (2002). *Cyberinsurance may cover damage of computer woes*. The Seattle Times.

GORDON, L. A., LOEB, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), 438-457. Doi 10.1145/581271.581274

GREISINGER, M. (2013). *Cyber liability & data breach insurance claims: A study of actual claim payouts*. NetDiligence, 25p.

HARRISON, A. (2000). Counterpane offers internet security insurance. *COMPUTERWORLD*.

HERATH, H., HERATH|, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance markets and companies: analyses and actuarial computations*, 2(1), 7-20.

KABAY, M. E. (1998). ICSA white paper threats, vulnerabilities and real-world responses: The foundations of the true secure process. ICSA.

KESAN, J. P., MAJUCA, R. P., YURCIK, W. J. (2004). *The economic case for cyber insurance*. University of Illinois College of Law.

KURMAIEV, P., SELIVERSTOVA, L., BONDARENKO, O., HUSAREVYCH, N. (2020). Cyber insurance: the current situation and prospects of development. *Amazonia Investiga*, 9(28), 65-73. Doi 10.34069/AI/2020.28.04.8

BODIN, L. D., GORDON, L. A., LOEB, M. P., WANG, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, 37(6), 527-544. Doi 10.1016/j.jaccpubpol.2018.10.004

LELARGE, M., BOLOT, J. (2009). Economic incentives to increase security in the internet: The case for insurance. In *IEEE INFOCOM 2009*, 1494-1502. Doi 10.1109/INFCOM.2009.5062066

LLOYD'S. (2017). *Counting the cost: Cyber exposure decoded*. Emerging Risks Report 2017. Retrieved from: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017---counting-the-cost.pdf

MAJUCA, R. P., YURCIK, W., KESAN, J. P. (2006). The evolution of cyberinsurance. *Computer Science*, 1-16.

MARROTA, A., MARTINELLI, F., NANNI, S., ORLANDO, A., YAUTSIUKHIN, A. (2017). Cyber-insurance survey. *Computer Science Review*, (24), 35-61. Doi 10.1016/j.cosrev.2017.01.001

PartnerRe & Advisen. (2018). *Survey of cyber insurance market trends*. New York: PartnerRe & Advisen, 15p.

ROMANOSKY, S., ABLON, L., KUEHN, A., JONES, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, 5(1), 1-19. Doi 10.1093/cybsec/tyz002

STRUPCZEWSKI, G. (2018).. Current state of the cyber insurance market. In *Proceedings of the Economics & Finance Conferences, Rome*, 491-501. Doi 10.20472/EFC.2018.010.034

TOREGAS, C., ZAHN, N. (2014). *Insurance for cyber attacks: The issue of setting premiums in context*. George Washington University.

VAUGHAN, E. J., VAUGHAN, T. (2007). *Fundamentals of risk and insurance*. John Wiley & Sons.

WANG, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, 1-12. Doi 10.1016/j.pacfin.2019.101173

WEF (2018). *The global risk report 2018*. 13th Edition. World Economic Forum, Geneva. Retrieved from: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

WHEELER, J. A. (2015). *Five tips for companies considering cyber insurance*. Gartner Blog Network. Retrieved from: https://blogs.gartner.com/john-wheeler/five-tips-for-companies-considering-cyber-insurance/