Social Transformations in Contemporary Society, 2019 (7)
ISSN 2345-0126 (online)

EVALUATION OF CYBER INSURANCE AS A RISK MANAGEMENT TOOL PROVIDING CYBER-SECURITY

Julija Gavėnaitė-Sirvydienė

Mykolas Romeris University, Lithuania
julija.gavenaite@gmail.com

Abstract

Purpose – to clarify the characteristics of cyber risk and cyber insurance. More specifically to identify key parts of cyber insurance contract and analyse cyber insurance market.

Design/methodology/approach: methodologically this research paper concentrates on analyses and study of scientific literature in order to provide the proper description and classification of cyber risks. Also statistical data was collected and analysed to provide a cyber-risk insurance market overview. Moreover, to prepare the underwriting methodology part in this paper, the scientific literature deduction was used, to reach conclusions from collected information sources.

Findings: firstly, this research paper provides an explicit definition of a cyber-risk and cyber insurance. In general, financial institutions and regulators of insurance market categorize cyber type risks as a part of operational risk because it is related to technology and information assets. Therefore, cyber risk is described as operational risk that affects technology assets, information, databases and other sensitive online storage. According to guidelines provided in Solvency II and Basel II documents, cyber risks can be put into four categories: technology and system failures, unsuccessful internal processes, act of people, external processes. These four categories of potential cyber risks are described particularly in this article. Secondly, the comprehensive cyber insurance market analyses is provided following the article. According to AXA Insurance Solutions company there was 170 insurers offering cyber liability policies in 2017 and about 30 more new carriers joined the market in 2018. According to the Cyber Policy Inc. the number 5 cyber insurance carriers in the marker is: AIG; Chubb; Hiscox, Liberty Mutual, HSB. With the beginning of 2019 it is expected from buyers to keep pressuring the insurance companies to deliver even more comprehensive services, more coverage options and potential. In general, cyber insurance market is supposed to remain stable, but the quality of policy language should evolve together with other endorsements to general cyber insurance policy. Thirdly, the general guidelines of underwriting the cyber insurance coverage policy is provided within this paper. In order to implement any form of risk reduction for cyber risk (also including insurance), the company at first should very clearly expose its potential vulnerabilities and weaknesses. Three types of general internal company's information can be marked out for preparing the cyber insurance coverage background: IT related information; human resources; finance, internal audit, legal issues. For insurance company to better understand the company the general business information is most important part. In order to extent the company's disclosure to cyber threats and to better prepare the solutions if insurance this business profile information should be conducted very carefully. Prevention is one of the most important factors of a cyber-risk insurance policy. Companies that are buying cyber risk insurance may get access to pre-breach assessments, prevented suppliers or cybersecurity information for this purpose.

Research limitations: this research paper concentrates on the European Union insurance market and experience of the insurer located in the EU. Moreover, this field of research is very unstable and the changing very fast together with continuously development of IT services sector. More studies and analyses should be made together with the changing environment of cyber security.

ISSN 2345-0126 (online)

Practical implications: this research paper may serve not only for further studies and scientific discussion. Moreover, it could be useful for the businesses as a valuable tool to better understand what cyber insurance is, how to prepare for implementing cyber security policy in the company.

Keywords: insurance, risk management, business, cyber security, cyber insurance policy, cyber insurance market.

Research type: research paper.

Introduction

During the past year, society and business have a growing dependence on IT, Internet, mobile devices. Therefore, the possibility of cyber-attacks and cyber risk for business increases drastically. According to the Global Risk report presented by the World Economic Forum, cyber security is one of the five biggest risks faced by governments and businesses across the world during the past year. Officers are implementing requirements regarding business to prevent from cyber-attacks, especially if they are processing personal data. In the EU General Data Protection Regulation was one of the major actions to ensure the security of personal data. These new regulations are expected not only to be one of the instruments of cyber security management but also to make an impact to companies to become aware and concerned about their data security.

According to Price Waterhouse Couper's report, there are more than one-third of companies in the USA that are using cyber insurance protection. Also, cyber insurance is expected to reach 7,5 billion USD of premiums paid by 2020. Despite the growing importance of cyber security, the market of Cyber Risk Insurance in Europe is still in the developing stage and the full potential is not reached yet. It is calculated that almost 90% of cyber insurance policies are issued in the USA, and approximately 5% to 9% in Europe. Because of this significant difference of market size, most of information, reports and surveys are based on USA cyber insurance market or the global view and a very little attention is given specifically to European market. Therefore, European insurers are in a very need of deeper understanding and managing of cyber security.

Cyber security and cyber risk management should become one of the top priorities to a businesses and individuals. In particular, a profound understanding of cyber risk is necessary to achieve for both supply and demand parts. This means a higher assessment and treatment of cyber related risks, not to mention a deeper analysis of the buyer's needs and expectations. Driven by the effective regulations and increasing awareness of businesses and individual's cyber insurance industry is expected gradually growth. Together with expected significant economy increase the importance and relevance of cyber coverage is supposed to develop and expand.

Categorising Cyber risks

The term of cyber risk is related to various of different sources that may affect the technology assets, information databases or other online storage of a firm or an individual. Generally, financial institutions and regulators of insurance market categorize cyber type risks as a part of operational risk because it is related to technology and information assets. Therefore, cyber risk may be defined as operational risk to technology assets and information that have subsequence to availability, integrity and confidentiality of information. Generally, cyber risks can be divided into two general groups depending on the source of the risk: insider (financial damage, fraud, data and identity theft made be the employees) or outsider

(company's confidential information, money). Because of these cyber risks businesses may not only loss secret information and money but also experience a loss of reputation, respectful name and credibility. (Cebula, J. J. and Young, L. R. 2010)

According to guidelines provided in Solvency II and Basel II documents, cyber risks can be put into four categories: technology and system failures, unsuccessful internal processes, act of people, external processes.

Table 1. Categories of cyber risk

Category	Definition	Factors
Act of people		
1. Inadvertent	Actions taken without harmful intentions	Errors, mistakes
2. Intentional	Actions taken intentionally to cause harm	Fraud, theft, vandalism
3. Inaction	Failure to act in a harmful situation	Lack of skills and knowledge
Technology and system failures		
1. Hardware	Risks traced to failures in manual equipment	Failure because of performance, capacity, maintenance
2. Software	Risks caused by programs, applications, operating systems	Security settings, coding, testing, configuration management
3. System	Failures as integrated systems does not perform as expected	Integration, design, specifications
Unsuccessful internal processes		
1. Process design	Failure due to poor process design or execution	Documentation, information flow, responsibilities, alerts, notifications.
2. Process control	Poor control of the process operations	Periodic review, process ownership, monitoring
3. Process support	Failure to deliver appropriate resources to supporting process	Accounting, staffing, training, development
External processes		
1. Catastrophes	Human and natural events over which the organization has no control	Weather event, fire, flood
2. Legal issues	Risks caused by legal arguments	Legalisation, regulations, litigations
3. Business issues	Risks caused by the changes in business environment	Supplier failure, market condition, economic causes
4. Service reliance	Risks arising from the organization's reliance on external parties	Utilities, fuel, emergency services, transportation, other suppliers

The insurance policy for cyber risk (also may be referred as cyber liability insurance coverage – CLIC) is created as a protection tool that reduces losses caused by cyber interruptions, network damages. Cyber insurance is designed to reduce the harm of cyber-attacks and data breaches. It first emerged because existing insurance policies did not include such losses as coverable.

ISSN 2345-0126 (online)

Cyber risk insurance significance for risk management strategies

First recommendations on the use of cyber risk insurance to encourage cyber security was made in 1994. In 1997, the first cyber risk insurance policy was written by Steve Haase, employed at a US-based insurance company, even if it can be described as a traditional third-party liability policy (Wells, 2018). This approach of risk management, especially used in the financial sector, could also be used for internet related risks was first announced by Dan Geer in 1998. (Geer, 1998). In 2001, Bruce Schneier presented the concept of cyber-risk insurance into the academic debate. (Schneier, 2001). Despite the fact that the history of academicals researches on cyber risk insurance has been available for more than twenty years, cyber insurance products still have not reached the level of other insurance products. More thank 25% of companies in Europe are not even aware of the existence of such type of insurance for cyber risk, and only 10% have purchased a cyber-risk insurance coverage. (Tøndel et al, 2015).

Increasing awareness and creating technical measures for companies against cyber related risks will significantly reduce the risks encountered, but will never be able to guarantee full protection. Moreover, small organizations usually do not have enough budget to invest in high-cost security measures such as next-generation firewalls; intrusion detection and prevention systems, and email security solutions. Through this point of view, the importance of cyber risk insurance for small organizations only increases. These are a particular reasons cyber risk insurance is significant for business:

1. Data are among our most important assets and results in financial losses if it is stolen or lost.
2. Information and communication technologies are critical in daily operations. The interruption of the system will cause a lot of financial loss.
3. The obligation to protect data of third parties is stipulated in laws and if they are lost or stolen, are exposed to serious penal and punitive sanctions.
4. All of these cyber-attacks which are occurred lead to material losses as well as the loss of reputation of the organization in the sector (Sloan, 2017).

The reputational losses mentioned above sometimes even overtake financial losses and can cause very damaging consequences for the company. The financial loss caused by cyber-attacks to organizations can be extremely significant to the financial stability and credibility, and a loss of brand value can negatively affect the organization's revenues for many years, and excessive resources may need to be spent to repair it.

Despite the fact organizations have taken a number of measures to ensure safety in cyberspace, they can still be affected by cyber threats. When they are affected by these cyber threats, there is a cyber-risk insurance to cover permanent damages. The resulting risk will be transferred to the cyber risk insurance and the financial and moral losses mentioned above will be totally or partially acceptable.

Cyber insurance market overview

In the 2017, the industry of insurance faced a major threat of ransomware (a type of harmful software created to block access to a computer system until a requested amount of money is paid). The names of these harmful viruses are better known as Petya, NotPetya, and WannaCry malware attacks. These dangerous programs infected computer software's in more than 150 countries across different types of industries as governments, hospitals, universities and private industries. It is very difficult to calculate the final and exact general loss caused by all these cyber-attacks, but approximately it is estimated that the NotPetya caused about 10

ISSN 2345-0126 (online)

billion dollars, WannaCry virus caused 4 billion dollars. Despite these major losses the market of cyber insurance is still in the development stage. (Eling, M., Wirfs, J. H. 2016) According to AXA Insurance Solutions company there was 170 insurers offering cyber liability policies in 2017 and about 30 more new carriers joined the market in 2018. According to the CyberPolicy Inc. the number five cyber insurance carriers in the marker is:

1. AIG: multinational corporation is a key player in the insurance industry and carries about 22% of the cyber insurance market during 2019
2. Chubb: is the world's largest publicly traded property and casualty insurer. It also covers about 12% of the cyber insurance market.
3. Hiscox: the company is well known for specializing in niche areas of coverage including classic cars, fine art, aerospace, kidnapping, ransom, and hacking. Their cyber policy is designed to cover privacy, data, and network exposures up to a $10 million capacity. It's also built to cover business interruptions, employee negligence, third-party data breaches, and more.
4. Liberty Mutual: insurer released Data Compromise and CyberOne, two products designed to mitigate the damages associated with data breach.
5. HSB: is now part of Munich Re. HSB's cyber insurance covers computer-attacks, cyber extortion, data breach response, misdirected payment fraud, identity recovery, network security liability, electronic media liability, and more.

It appears that in the past few years' cyber insurance market was developing very fast, offering vide range of coverage, but actually it does not mean that this abundance of supply automatically means that all the possible risks are covered. The types and possibilities of cyber-attacks also have changed and together brought these major and significant changes in the cyber insurance market during 2018:

1. **Increased number of ransomware attacks.** Even though there was no major and significant impact to a market last year, the number and severity of cyber-attacks should be alerting. The frequency of cyber-attacks has significantly increased. It should be also noted that most of the cyber-attacks recently were ransomware attacks. This is because the ransoms have gone up exponentially.
2. **The thieves become more sophisticated.** In 2018 social engineering reached its pitch. Attention now is paid not to hacking exactly, but into developing smart systems and software's, building them to explore within the company or individual, destroy possible security utilities and help to reach financial gain.
3. **Changes in the regulatory environment.** With the increase of cyber-attacks, the security of important company or personal data is also in a higher danger. As the harmful software are developed the accessibility of personal information has become easier and faster. In May 2018 the General Data Protection Regulation (GDPR) became in force. This new regulation put a responsibility and obligations to companies to protect the data there are disposable that are related to European Union (EU) citizens.

Cyber insurance market predictions for 2019

With the beginning of 2019 it was expected from buyers to keep pressuring the insurance companies to deliver even more comprehensive services, more coverage options and potential. Companies that are buying cyber risk protection should continuously turn into insurers for better risk management offers and services. In general, cyber insurance market is supposed to remain stable, but the quality of policy language should evolve together with other endorsements to general cyber insurance policy.

ISSN 2345-0126 (online)

Clearing and building the cyber risk policy language should be one of the most priority questions for the insurers. This is because there are still plenty of conditions and descriptions to be clarified and described. For example, all the cyber risk events that do not typically fall under this policy umbrella – most relevant will be the crime and property policies. The insurers must keep clarifying the policy language as it would be totally clear under what policy the risk should be insured – the property or liability? The buyers of insurance should also play a role here to help their insurers better understand the type and shadings of the insured business to better avoid incidents in the future when claims happen.

As the need to clarify and upgrade cyber insurance policies become one of the priorities, the data and analytics will be helpful and important. The use of data analytics to create a cyber coverage contract is expected to increase significantly in 2019. As the insurance companies tries to reduce the impact of an aggregate event that could affect multiple policies, they will keep trusting on outsourcing data analytics to keep more efficiency and finally more profitable underwriting processes. The traditional methods that are usually used to underwrite risks and create the insurance contract, such as questionnaires are supposed to be replaced by more sophisticated risk engineering decisions, data analytics methods that work case-by-case and can provide higher efficiency and accuracy in risk underwriting.

Underwriting cyber risk insurance policy

In order to implement any form of risk reduction for cyber risk (also including insurance), the company at first should very clearly expose its potential vulnerabilities and weaknesses. Therefore, the first step to cyber risk management is organizing the internal research in the company to put up a picture of possible cyber risks and any other possible threats. If the company does not have a responsible person of risk management, conducting this research may be challenging. There are a vide spectrum of information that can be found in the organization and is very essential for managing cyber risk and implementing insurance protection in the organization.

Three types of general internal company's information can be marked out for preparing the cyber insurance coverage background (Ridd, J., 2002).

Table 2. Internal information types for cyber risk contract

IT related information	Human resources	Finance, internal audit, legal issues
• Information system security • IT suppliers • Management of IT updates	• The corporate culture and approach on cybersecurity • The human issue (possibility to rise awareness and organize trainings)	• General business information (profile, links between market, cyber threats) • Oversight and internal audit • Personal data

Conducting all this information from internal company's sources is the crucial background to create an accurate cyber risk insurance contract that would include coverage for all possible threats and meet all the requirements that company may have or is vialing to discover.

ISSN 2345-0126 (online)

Business information and profile for cyber risk coverage

For insurance company to better understand the client, basic business information is most important part. In order to extent the company's disclosure to cyber threats and to better prepare the solutions if insurance this business profile information should be conducted very carefully. (Varian, H. 2000).

To shape the insurer's profile this general information is most important:

1. Company's main activities: services that company provide, business sector, business type, general business market, competitors. This kind of information helps to understand what potential claims and third-party losses may occur.
2. Business to client rate: this percentage of the amount of business that are customer end type enables to evaluate the personal data that company may dispose – consumer's personal information, banking data, payment systems. This information characterizes the possible third-party loss risk.
3. Business to business activity: this type of information can clarify the possible first party loss possibility.
4. Geographical information: specifically, information about branches, the locations of offices, supply chains, assets and processes of production. This helps to evaluate legal and political risks.
5. Financial details: income, turnover, profit. The annual turnover is generally the most significant indicator of the company's potential exposure.
6. The budget of IT security: to the insurance company this number clarifies the financial commitment of the company to cybersecurity. Moreover, this is a great indicator that shows the risk maturity of the client.

Cyber insurance policy

The insurance coverage may be very specific or vide, but there are some significant parts and types of information that must reflect in the insurance policy. It is strongly recommended to a buying company to look very carefully though the cyber insurance proposal because they can:

1. Change between different offers or insurers
2. Control the affect how the insurance policy responds in the event of specific cyber issue
3. Useful to find and notice possible gaps or drawbacks

The risk factors discussed in table 3 are a very useful tool for the company to consider how cyber risk insurance coverage could implement in their organization's security politics and other essential factors of their activity.

Table 3. Risk factors in cyber insurance contract

Prevention	Assistance	Operations	Liability
• Assessments before violation • Access to prevent vendors • Information of cybersecurity	• Judiciary investigators • Legal services • Notifications • Monitoring of the credit • Call centre services • Public relations, crisis management	• Costs incurred to keep or return the business to operational • Loss of turnover, income, revenue • Restoring/recreating information, data	• Damages or legal costs from claims alleging privacy breach or network security failure

ISSN 2345-0126 (online)

Prevention is one of the most important factors of a cyber-risk insurance policy. Companies that are buying cyber risk insurance may get access to pre-breach assessments, prevented suppliers or cybersecurity information for this purpose. On the other hand, it often does come down to cost. Commonly, cyber risk insurance policies, which are likely to include the scope of a various cyberattack, may often be too expensive to afford for a small business. But even then, the small companies are able to take some cybersecurity actions and put measures of protection in place. Here are some effective and simple tools to reduce cyber risk on a smaller budged if a company cannot afford the cyber insurance:

1. **Create internal data protection regulations:** put a limit of how many employees can handle personal data, limit the access to customer data storage. Organize trainings to employees on how they should handle working with personal data or any other sensitive information.

2. Invest in latest antivirus software: responsibly take care that all the devices used in the company are provided with latest antivirus programs, regularly update this software.

3. Usage of firewalls: this protection tool may make it harder to hackers to reach company's networks. Encrypting all data and putting passwords on wi-fi network is also helpful.

4. Personnel training: organizing trainings to a staff as they would be able to notice and identify a potential threat. Also put a reasonable and strong requirement on how personnel should crate their passwords and any other security tools.

These tools are a very good and useful options for the small to mid-sized businesses to create a protection from cyber risks. Even if a company does not stock a large online data it still has a certain level of cyber risk that could be very harmful and unprofitable to the business. The activity without any measures of coverage is very unsafe to any type or size of company. Even simple and consistent tools of cybersecurity can help a company to keep it safe and less risky.

Conclusions

The digital transformation in the world is continuing with no signs of slowing down. Every day the consumption of online data, services and activities is increasing. Businesses are becoming more and more dependent on online tools, modern technologies and inter-connectivity. Together with these changes the online hackers are also becoming more sophisticated. The amount of reported cyber-crimes keeps growing because these criminals are expanding their networks, discovering new vulnerabilities to achieve their targets. Continually changing environment of online technologies makes it even more challenging for businesses to keep up with newest protection utilities, security options and cyber insurance solutions. Because of these causes the cyber risk insurance market will keep a very significant role in the future to support companies in managing their exposure to possible cyber threats.

In order to make cyber risk insurance product more accessible in the future, the following items should be indicated in the cyber security coverage contract and also carefully discussed between the insurer and a buying company:

1. According to cyber risk categories – what risk factors are most possible to occur, taking into account company's profile, activity, vulnerabilities and possible threats.

2. Insurer is supposed to clarify and explain the importance of cyber security to the company, also involving a research of sensitive data or information that the company may are disposable of.

3. The internal information that are curtails for underwriting cyber risk policy should be carefully collected, discussed and analysed to ensure that all the potential risks are considered and taken under insurance policy protection.

To summarize, cyber risk insurance is one of the most effective tool to ensure cyber security for business, to protect essential data, and to guarantee sustainable activity. Furthermore, it should be strongly recommended to companies that are involved in doing online business or in any case dispose a significant data to pay more attention to possible cyber-threats, take into consideration any possible cyber security measures.

References

Anderson R.; Moore T. 2018. *Information security economics and beyond.* Information Security Summit.

Biener, C.; Eling, M.; Wirfs, J. H. 2015. *Insurability of Cyber Risk – An Empirical Analysis.* The Geneva Papers on Risk and Insurance – Issues and Practice 40(1). Geneva.

Bohme R.; Schwartz G. 2010. *Modeling cyber-insurance: Towards a unifying framework.* WEIS.

Borghesi A.; Gaudenzi B. 2013. *Risk Management: How to Assess, Transfer and Communicate Critical Risks*. Springer-Verlag: Milan.

Cebula, J. J.; Young, L. R. 2010. *A Taxonomy of Operational Cyber Security Risks', Technical Note CMU/SEI-2010-TN-028.* Software Engineering Institute, Carnegie Mellon University

Chapelle, A.; Crama, Y.; Huebner, G.; Peters, J.-P. 2018. *Practical methods for measuring and managing operational risk in the financial sector: a clinical study.* Banking & Finance 32(6).

Chavez-Demoulin, V.; Embrechts, P.; Hofert, M. 2015. *An Extreme Value Approach for Modeling Operational Risk Losses Depending on Covariates.* Journal of Risk and Insurance, DOI: 10.1111/jori.12059.

Eling, M.; Wirfs, J. H. 2016. C*yber Risk: Too Big to Insure? – Risk Transfer Options for a Mercurial Risk Class*. I.VW Schriftenreihe, Band 59, St. Gallen.

European Union (2016) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Geer D. Risk Management is Where the Money Is. [interactive]. *Talk Before Digital Commerce Society of Boston,* 2018 [accessed 2019-06-18]. < https://www.researchgate.net/publication/2956022_Risk_Management_is_Still_Where_the_Money_is>

Marsh&McLennan. Companies Global Risk Center. MMC Cyber Handbook. 2018. *Perspectives On The Next Wave Of Center.*

Majuca, R. P.; Yurcik, W., & Kesan, J. 2006. *The evolution of cyberinsurance*. ACM Computing Research Repository (CoRR), Technical Report cs.CR/0601020.

McNeil, A. J.; Frey, R.; Embrechts, P. 2015.*Quantitative Risk Management: Concepts, Techniques, Tools – Revised Edition*, Princeton University Press.

Muermann, A.; Kunreuther, H. 2008.*Self-protection and insurance with interdependencies.* Journal of Risk and Uncertainty, 36(2), p.103-123.

Ogut, H.; Raghunathan, S.; Menon, N. M. 2005. *Information security risk management through self-protection and insurance.* The University of Texas at Dallas.

Romanosky S.; Ablon L.; Kuehn A.; Jones T. Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber-risk? [interactive]. *Axa Insurance solutions*. [accessed2019-03-18]. <https://www.rand.org/pubs/working_papers/WR1208.html>.

Ridd, J., 2002. Insuring Digital Risk: A Roadmap for Auction. *Information Assurance Advisory Council*. 28, 771-780.

Schneier B. 2001. Insurance and the Computer Industry. *Communications of the ACM. 44(3): 114-115.*

Sloan R. Cyber Matters: The Importance of Cyber insurance for SMEs. [interactive]. *Cubb INC USA.* [accessed 2019.05.13] <https://www.cybersecurityjournal.org/cybermatters-he-importance-ofcyber insurance>

Tanaka, H.; Matsuura, K.; Sudoh, O. 2005. Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy,* 24(1), p. 37-59.

Tøndel IA; Meland PH; Omerovic A; Gjære EA; Solhaug B. Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research [interactive]. *The New York Times.* [accessed 2019-03-18]. <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>

Vaughn, R.; Henning, R.; Siraj, A. 2003. *Information assurance measures and metrics: State of practice and proposed taxonomy.* HICSS '03, Hawaii, p. 34-52.

Zhao, X., Xue, L.; Whinston, A. 2009. *Managing Interdependent Information Security Risks: An Investigation of Commercial Cyber insurance and Risk Pooling Arrangement Thirtieth*. International Conference on Information Systems, p. 189-239.

Wells A. What Agent Who Wrote First Cyber Policy Thinks About Cyber Insurance Now [interactive]. *Insurance Journal.* [accessed 2019-05-07] < https://www.insurancejournal.com/news/national/2018/03/01/481886.htm>