Humanities and Social Sciences **2019**
HSS, vol. XXIV, 26 (4/2019), p. 19-32 **October-December**

Bartłomiej BALAWEJDER[1]
Robert DANKIEWICZ[2]
Anna OSTROWSKA-DANKIEWICZ[3]
Tomasz TOMCZYK[4]

THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT IN ENTERPRISES

Modern enterprises run their activities in an innovative environment. The use of modern technologies is, therefore, becoming a prerequisite for maintaining the current market position and ensuring competitiveness with other entities. However, the use of innovative IT solutions creates the risk that certain disturbances in the functioning of computer programs or the occurrence of cyber attacks will bring losses to the company, thus negatively affecting financial results. Materialisation of cyber risk may also have a negative impact on the company's image and, consequently, a potential decrease in sales of goods. Therefore, a proper assessment and management of cyber risk in modern enterprises is important. One of the methods to manage this risk is cyber insurance. A large number of cyber attacks and the development of new technologies has resulted in enterprises using cyber insurance, as evidenced by the significant increase in gross written premium in recent years. The research conducted by various institutions forecasts a dynamic growth of cybernetic insurance premiums in the coming years, suggesting that cyber insurance will grow in popularity.

The purpose of the article is to present the necessary conditions and risks for the functioning of innovative enterprises in the current economic environment. In addition, the article analyses the occurrence of individual risks in business operations and their financial effects. The research also presents a scale in the use of cyber security in managing cybernetic risk of enterprises and provides future development directions of cyber security products. The research utilised methods of analysis and synthesis of secondary data in formulating conditions.

Keywords: cybernetic risk, cyber security, enterprise risk management.

[1] Bartłomiej Balawejder, Bachelor, Cracow University of Economics, College of Economics, Finance and Law, e-mail: bbalawejder123@gmail.com. ORCID: 0000-0003-3488-6308.

[2] Robert Dankiewicz PhD, Rzeszow University of Technology, The Faculty of Management; al. Powstańców Warszawy 12, 35-959 Rzeszów; e-mail: rdankiew@prz.edu.pl. ORCID: 0000-0003--3453-2892.

[3] Anna Ostrowska-Dankiewicz PhD, Rzeszow University of Technology, The Faculty of Management; al. Powstańców Warszawy 12, 35-959 Rzeszów; e-mail: adankiew@prz.edu.pl. ORCID: 0000-0002-2131-4522.

[4] Tomasz Tomczyk, MSc, Department of Finance, Banking and Accounting, Rzeszow University of Technology, al. Powstańców Warszawy 12, 35-959 Rzeszów; e-mail: ttomczyk@prz.edu.pl. ORCID: 0000-0003-4134-7628.

1. INTRODUCTION

Virtually every enterprise uses computer programs in its operations. This use of IT tools can take place at different levels and with the use of IT programs of various levels. However, in the age of constant development of new technologies and the emergence of more and more advanced IT systems, enterprises are implementing more and more processes using the latest technological achievements. Automation and transferring more and more operations to a virtual environment creates the risk that various types of disturbances in the functioning of systems will negatively affect the enterprise and will be reflected in the results achieved.

New technologies used on a larger scale began to dominate the strategies of enterprises at the beginning of the 21st century. The change in the business concept and an approach to strategy formulation was influenced by many factors, but the most important of these were globalization and extremely fast technology development, civilization progress and focus on innovation (Puto, 2017). The direct consequence of changing the approach in formulating the strategy was also the emergence of new trends in the way of managing the enterprise. Difficulties in this field are a consequence of the occurrence of the risk phenomenon, the implementation of which in extreme cases may lead to bankruptcy of the entity at risk, with simultaneous consequences for the business environment (Dankiewicz, 2018). New approaches to enterprise management have begun to be oriented towards the innovation of the organization, knowledge and innovation management, and conducting research aimed at increasing the innovation potential of the enterprise. The changes observed in recent years related to the dynamic growth of innovation of European enterprises have been a kind of reflection of the priorities assumed by the Europe 2020 strategy. What's more, the ability to create and implement innovations has become one of the main challenges of modern enterprises (Pomykalski, Blażniak, 2014). The literature even mentions that innovation is a key process for the survival of an organization (Machová, Huszárik, Šimonová, 2016).

The purpose of the article is to present the conditions for the functioning of innovative enterprises in the current economic environment, as well as to define the risks that are inherent in the business. In addition, the article analyzes the occurrence of individual risks in business operations and their financial effects. The scale of using cyber security in managing cybernetic risk of enterprises was also presented and future development directions of these products in the world were determined.

2. LITERATURE REVIEW

The technological progress observed in the economic environment forces the companies to constant, dynamic development associated with the use of new solutions in conducting business activity. These processes condition changes in modern enterprises, and the growing global market means that the roles and tasks of enterprises and their managers change, among others, by introducing new technologies. Therefore, it becomes important to create new structures that are designed to respond to the challenges posed by a competitive market, where unfair market practices appear more and more often (Ostrowska-Dankiewicz, 2019), and the vision of the enterprises of the future tends towards learning, intelligent and virtual (Kubik, 2012).

The use of modern technologies can create great opportunities, especially for small and medium enterprises. The progressing globalization means that the expectations of customers and business partners are changing, and the implementation of new technologies enables

small and medium-sized enterprises to access information infrastructure comparable to that used by the largest enterprises. The use of internet tools, in turn, can help increase the efficiency of operations carried out by enterprises, change the organizational chart or completely redefine the way in which the organization conducts its activities (Kos-Łabędowicz, 2013).

The impact of changes on the market on modern enterprises is shown in figure 1.

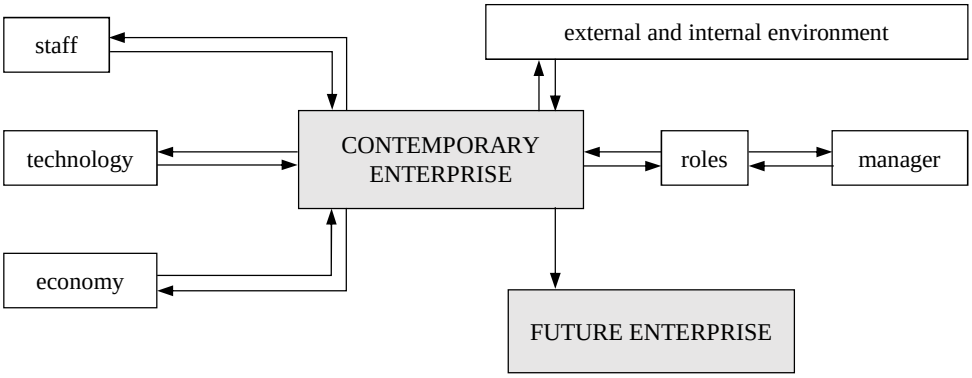

Figure 1. Changes taking place in a modern enterprise

Source: Own elaboration based on (Kubik, 2012).

Modern enterprises use many innovative solutions, which include cloud computing, artificial intelligence (AI) or Internet of Things (IoT). All the technological innovations available in the market can bring many benefits to enterprises, but one should remember about the threats that result from process automation and their transfer to virtual environments. I am talking in particular about cyber attacks, which can have particularly severe consequences in the case of organizations that base their activities mainly on IT systems. Therefore, cyber risk management seems to be one of the key aspects of enterprise management, and in the case of enterprises using modern technologies to a large extent, it is possible that even the most important aspect of doing business

The analysis of the literature shows that cyber risk does not have an unambiguous, precise definition, which is the result of a very wide range of risk, as well as various defining perspectives. Cyber risk may have a different nature depending on the organization it covers. From the point of view of enterprises, this is an operational risk of anthropogenic origin, while for insurance companies it is an insurance risk defined by a catalog of various forms of its materialization. However, in the narrowest sense, cyber risk can be defined as the risk of occurrence of electronic events that cause disruptions in business operations or financial losses, or as a risk that is associated with the possession and use of IT equipment and technology in the organization (Strupczewski, 2017a).

As a result of cybernetic materialization, cybercrime occurs, which may involve various activities that affect both individuals and businesses. In the case of individual persons, in particular, the crime of identity and personal data theft is mentioned, while in the case of enterprises, e.g. theft of intellectual property can be talked about (Wierzbicka, 2017).

For enterprises, the threat of cyber attacks is high and it is still growing. Such attacks can have many negative consequences for enterprises, which may manifest themselves in closing energy networks, disclosing offers to competitive enterprises or disabling websites that may be necessary to conduct standard business. What's more, it is noted that hackers are now becoming more sophisticated, which means that enterprises will have to constantly focus on cyber security and increase the expenditure associated with securing themselves against these attacks (Brockett et al., 2012).

The targets of cyber attacks can be different. The idea behind such an attack may be hackers' desire to raise money, data or technology. However, if the purpose of such an attack is personal data or confidential business data, then one can speak of an incident of data breach (Strupczewski, 2017b). This, in turn, may impose penalties on entities that have insufficiently secured such information.

Considering the danger of losing any information processed within the enterprise and incurring the related costs, the goal of all enterprises, and especially those that use IT systems to a large extent, should be to manage cyber risk in such a way as to ensure the state of cyber security of the organization . Cyber security can be understood as a set of defensive methods that aim to reduce the risk of malicious attacks on software, computers or networks (Craigen et al., 2014).

Many organizations have their own crisis management structures whose task is to facilitate appropriate response to internal crises, regardless of their cause and nature. It is, therefore, important that these mechanisms are coordinated so that they are able to act also in the event of cyber risk incidents. To determine when and what safeguards to apply, organizations may take some action to prioritize and assess threats and, as a consequence, seek cyber security (Public Safety Canada, 2016). These actions are shown in figure 2.

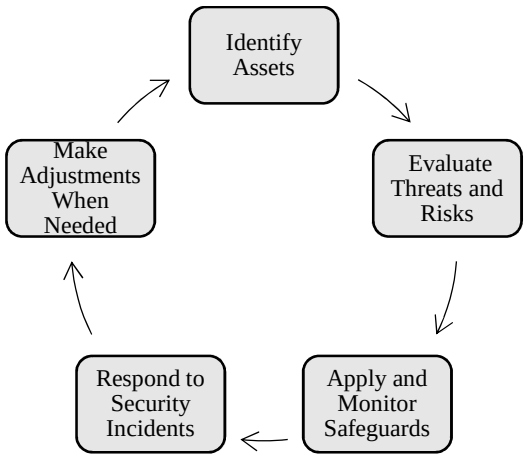

Figure 2. Cyber Security Fundamentals

Source: Own elaboration based on (Public Safety Canada, 2016).

The literature distinguishes at least two basic features that distinguish cybernetics risk assessment and management from other types of risk management. First of all, the attention should be paid to the far-reaching range of cyberspace, which means that sources of threats

can also be very widely spread, even on a global scale. The second feature is a very large number of potential threats, both threatening and harmless. These features make it necessary to develop techniques and procedures that provide guidance on how to properly assess and manage cyber risk (Refsdal et al., 2015).

The process of appropriate risk management is a very important element of business operations. This applies to risks of different origins, including cyber risk. However, in the event of events that cause disruption to business operations, they must face some financial losses or other additional costs. The determination of potential costs related to the materialization of cyber risk was the subject of research in the literature. In his research, S. Romanosky focused on four types of cyber attacks: *data breaches* understood as disclosure of personal information, security incidents, i.e. malicious attacks directed at the enterprise, violation of privacy and phishing/skimming. The author points out that by far the most common of all cyber threats tested were data incidents, in particular personal information such as credit card numbers or medical information. However, when it comes to costs resulting from cyber threats, the author indicates that they may have a different nature. In the event of a data breach, the costs incurred by an undertaking may include the costs of a criminal investigation, the cost of notifying consumers. In addition to these, these may also be the costs of settlement between the parties, fines or fees imposed by government agencies. Moreover, in a sample of 12,000 cybernetic events studied, the cost of a typical incident was less than 200,000. USD (Romanosky, 2016).

However, it is noted that the costs of cyber security breaches for one enterprise can reach billions of dollars. Moreover, such studies are most often conducted using surveys, which causes some distortion of the picture of real costs as the participants of the study often take into account only the direct costs associated with the materialization of cyber risk, such as the costs of detecting such violations or any loss of assets. Often, costs such as a potential decrease in sales or potential future obligations arising from a breach of cyber security are not estimated (Gordon et al., 2015).

The subject of research of scientists is also the impact of cyber attacks on the price of shares of an enterprise. The research conducted showed that the market provided a negative return on investment in the period after data breach as a result of cyber attacks (Kammoun, 2019). Another direction of research includes the impact of cyber risk on return on shares of enterprises that suffer from some information gaps (Colivicchi, Vignaroli, 2019).

Some scientists have also tried to develop a flexible and transparent methodology for estimating both current and future global costs of cyber risk. The research conducted showed that cybercrime directly affected gross domestic product. On a global scale, direct baskets were USD 6.6 trillion, while total cybercrime costs can range from USD 799 million to even USD 22.5 trillion (Dreyer et al., 2019).

The costs incurred by enterprises related to the cyber risk materialization should be minimized accordingly. The company's goal should be to limit the frequency and scale of cyber incidents. However, when such actions are not entirely possible, enterprises should manage cyber risk in such a way as to at least limit the financial consequences of such phenomena. Cyber insurance is a way to manage risk in this area.

Cyber insurance has been studied both in the context of the risk transfer method, but also as a mechanism to motivate the improvement of cyber security (Khalili et al., 2017). Although there are more than 10,000 cyber attacks per day around the world, most corporations are just beginning to realize the vulnerability to such incidents. Therefore, cyber insurance seems to be one of the future areas of development when it comes to cyber risk

management. As a result, insurers will be able to generate revenues from the provision of services consisting in monitoring cyber attacks and appropriate active response to them (Nylor, 2017). However, it should be noted that the cyber insurance market is a relatively young market and faces many challenges. These include the lack of data, the problem of defining a contractual language or specification of standards in the field of risk assessment (underwriting). These challenges are practical, and to meet them requires insurers to gain more experience in this field. On the other hand, there are also theoretical challenges related to correlated risk, as well as the interdependence of information security and asymmetry. A thorough theoretical analysis is required to enable market development and benefit from social benefits (Martinelli et al., 2018).

Literature analysis shows that at the beginning of the 21st century, insurers began to offer products that they felt were protected against financial losses that resulted from data breaches. The types of risk that cover such policies include, first and foremost: identity theft, business interruption, loss of reputation, litigation costs, malware or human errors (IIROC, 2015). The scope of liability of insurers under cyber insurance can include both direct losses incurred by the policyholder (First Part Loss) and coverage of losses on third party items (Third Party Loss). The detailed scope of responsibility is presented in table 1.

Table 1. Examples of cyber-insurance coverage

First Part Loss	Third Party Loss
• Loss of business income due to cyber incident Business interruption • Damage to intangible assets • Damage to tangible assets (products liability) • Loss due to outside provider security or system failure • Loss due to system failure or human error • Cost of ransom payment • Cyber specialist • Loss due to accidental damage of computer system • Financial loss from fraudulent electronic transfer of funds • Data restoration • Extra expense • System clean-up costs • Administrative investigation and penalties	• Liability claims • Fines • Media liability • Wrongful collection of information • Media content infringement/defamatory content Yes Violation of notification obligations

Source: (EIOPA, 2018).

In addition, the use of cyber security can bring other costs and services benefits to enterprises. The benefits reported by cybernetic insurance clients are presented in figure 3.

In addition, the use of cyber security on the macro-social scale provides three very important benefits. Cyber insurance stimulates the increase of investment in IT systems security, creation of a code of good practices in managing cyber risk in an enterprise, as well as raising the level of society's wealth (Strupczewski, 2017a).

Figure 3. Benefits of cyber insurance for enterprises

Source: (EIOPA, 2018).

However, it should be noted, however, that effective cyber risk management in an enterprise should be based on the use of cyber security, not only to transfer risk, but also to create incentives to invest in cyber security. However, this is difficult because of the asymmetry of information that makes it difficult for insurers to monitor their cyber security activities (Shetty et al., 2018). On the other hand, companies' reluctance to use cyber security can have various reasons. Customers may have concerns about costs and revenues – some companies believe that such insurance is too luxurious. Another important factor may be the uncertainty as to the payment of benefits in the event of materialization of cyber risk, which is directly related to the fact that cyber insurance is a relatively young service, so the market itself is not fully tested. Some companies in the high technology industry are characterized by a relatively high risk appetite, which in their opinion insurance does not seem to be a necessary investment. The last reason is the matter of maturity. Some companies may not be aware of the possibilities of cyber risk insurance, while others may not be aware of being exposed to this type of risk (Meland et al., 2017).

3. THE SCALE AND COSTS OF CYBER ATTACKS FOR BUSINESSES

The cyber threats that enterprises may face in their business activity may have many common features, however the risk characterization depends to a large extent on the profile of their activity. Slightly different threats will affect financial institutions, and other manufacturing or service enterprises. The threats to individual industries are presented in table 2.

Cyber threats are affecting companies located all over the world. However, studies show that the incidence of cyber security incidents varies from country to country. Most malware attacks occur in Bangladesh and Algeria, while the smallest number of attacks was observed in Denmark and Ukraine (https://financesonline.com). The most common types of cyber

attacks in the United States and their share of the total number of attacks are shown in chart 1.

Table 2. Cybernetic risk exposure in specific industries

Industry	Exposures	Common claims
Financial institutions	High exposure to cyber risk due to a combination of factors: cyber crime, hacktivism and sophisticated attackers carrying out espionage on behalf of a beneficiary. Vulnerabilities to cyber event can be high as many financial institutions are dependent on highly interconnected networks and critical infrastructures.	Social – Phishing and Human Error
Healthcare	Increased reliance of Healthcare companies on computer systems to collect and transact highly sensitive personal health and medical data. There is a high exposure to administrative errors.	Human Error and Misuse
Retail	Retail companies often have many locations that may or may not operate on centralised IT systems; a potential dependency on websites due to the increasing number of online sales, and an aggregated amount of sensitive personal information	Hacking and Social – Phishing
Hospitality	Cyber related exposures include large volumes of consumer and employee information, often heavy reliance on websites for customer bookings, and loyalty program information can lead to privacy issues	Social – Phishing and Hacking
Pro services	Confidential data hold by a law firm or an accountant can be lucrative for an attacker, and the reputational consequences for a firm suffering a breach can be highly damaging.	Human Error and Hacking
Manufacturing	One of the largest industries being targeted by cyber criminals. Many manufacturers are leveraging the Internet of Things (IoT), digitalisation, and cloud services, which all increase the impact of certain cyber events.	Malware and Social – Phishing
Education	Educational establishments are at risk due to the sensitive data they hold on students and staff; schools and universities often have limited IT budget and resources.	Social – Phishing and Hacking
Media/Entertainment	Cyber extortion threats that may target sensitive material and content. Attacks or computer system outages may significantly impact broadcasting activities and timely content delivery. The possession of sensitive personal information of subscribers compounds the exposure.	Human Error and Social – Phishing
Technology	Technology companies are trusted by their clients and customers to be industry leaders in the cyber security and protection of data, increasing the reputational damage that could follow a cyber event.	Hacking and Human Error

Source: Own elaboration based on (CHUBB).

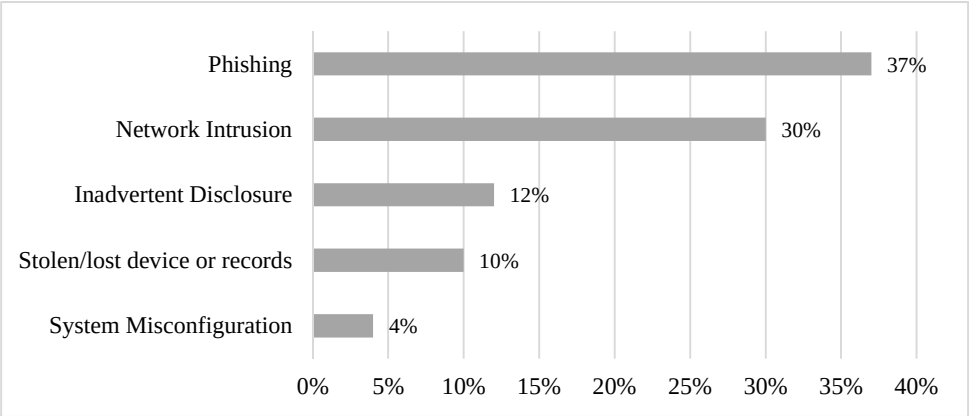

Chart 1. Most common cyber attacks experienced by the US companies

Source: Statista (2018).

An important issue related to the analysis of cyber risk is the financial consequences that must be taken into account by enterprises that have been affected by any cyber attack. Both the analysis of the literature and the market situation indicate that incidents violating cyber security are costly for enterprises and may significantly burden their financial result. The average organizational cost of enterprises in the United States after a data breach incident is shown in chart 2.

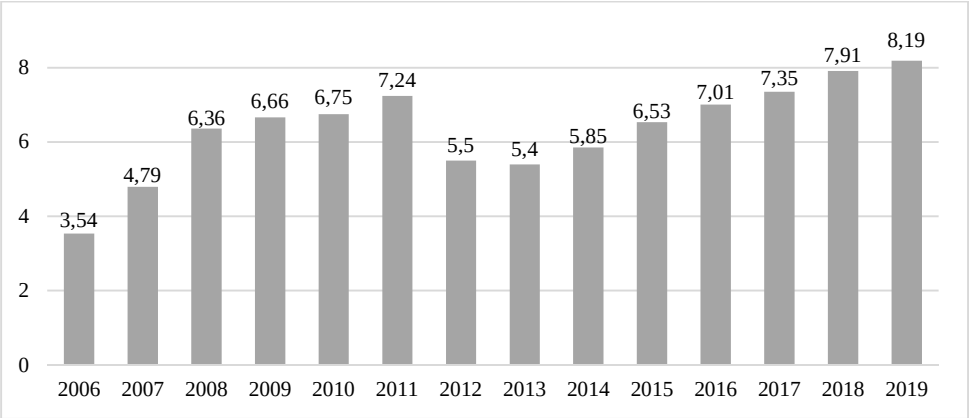

Chart 2. Average organizational cost to a business in the United States after a data breach from 2006 to 2019 (in milion U.S. dollars)

Source: Statista (2019).

An analysis of the costs incurred by American enterprises shows that despite the fact that in 2012 costs began to decrease, in 2019 they were already more than 2 times higher than in 2006. It shows how dangerous cyber threats can be to enterprises, as well as their dynamic growth in the last years. The United States is also a country where cyber incidents

occur most frequently and generate the highest costs for organizations. The summary of average annual costs related to cyber attacks in selected countries is presented in chart 3.

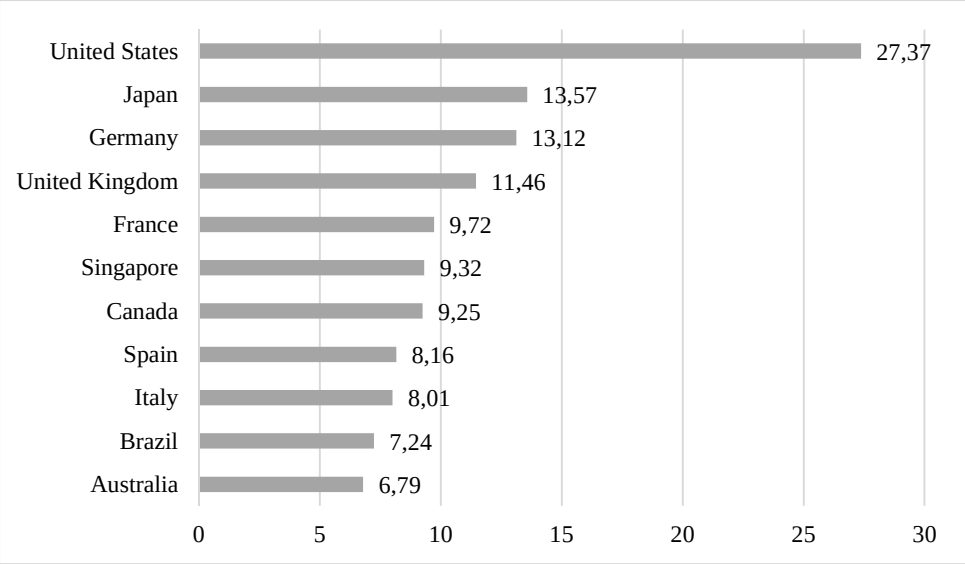

Chart 3. Average annualized cost of cyber attacks on companies in selected countries in 2018 (in millon U.S. dollars)

Source: Statista (2019).

When analyzing the annual costs in selected countries, it can be seen that in the case of European countries cyber attacks generate much lower costs than in countries such as the USA or Japan. It should be noted, however, that Germany bears the largest costs associated with the implementation of cyber risk among all European countries.

4. INSURANCE DEVELOPMENT POTENTIAL IN CYBER RISK MANAGEMENT

One of the methods of managing cyber risk in enterprises is cyber insurance. Despite the significant benefits of these products, their use is relatively low. The share of expenditure on cyber insurance in relation to the total costs incurred to ensure an appropriate level of cyber security in the organization is presented in chart 4.

An analysis of cyber security expenses incurred by enterprises shows that these expenses are constantly increasing. However, it should be noted that the gross written premium for cyber insurance (Gross Written Premium, GWP) accounts for a very small percentage of total expenditure. In 2015, expenses related to the purchase of cyber-insurance accounted for only about 3% of total expenditure, while in 2019 – just over 4%. Over the years 2015-2019, the overall level of expenditure increased by more than 58%, while the gross written premium due to cyber-insurance doubled. In addition, the forecasts show that in 2020 the gross written premium should increase by 60% compared to 2019. Therefore, it can be seen that cyber insurance is constantly evolving and it can be assumed that their

share in expenditure related to cyber security, and therefore their role in the cyber risk management process will grow.

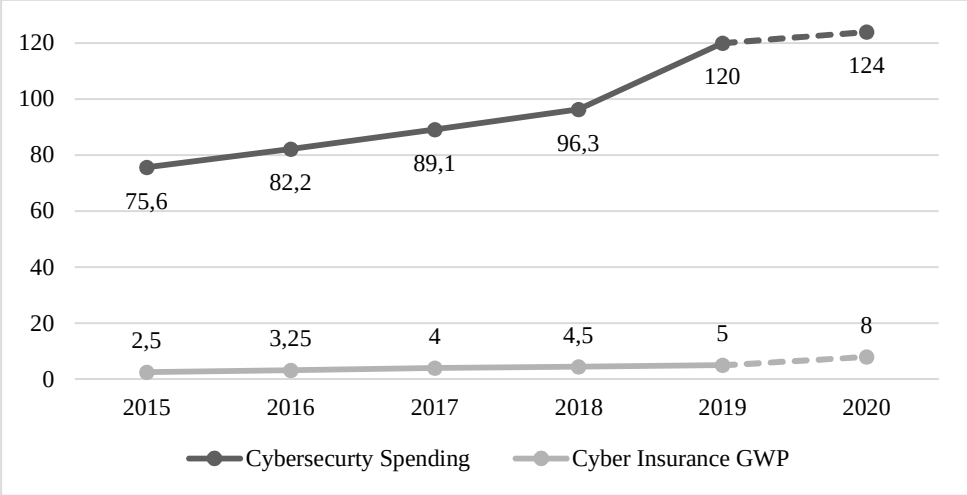

Chart 4. Annual cyber security spending (in $bn)

Source: Own elaboration based on (Marsh, 2019).

The development of the cyber insurance market is also forecast by Aon. The research conducted shows that the largest market for the aforementioned insurance is the United States, while the remaining countries have so far had a marginal share in the global written premium. These studies also show that European Union countries began to have any significant share in the global premium only from 2013. Detailed data on the increase in global premium written in cyber insurance are presented in chart 5.

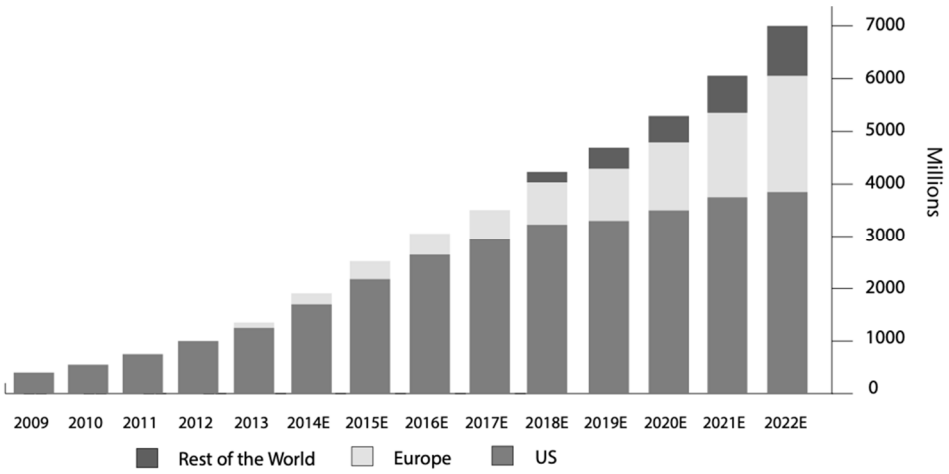

Chart 5. Global cyber written premiums 2009 – 2022

Source: (Aon, 2018).

The analysis of the research by Aon shows that the development of cyber insurance will be the most dynamic in those markets that so far have had a small share in the global written premium. In the United States, where cyber risk insurance has been popular for years, this increase will not be as noticeable. However, in the case of European Union countries, the value of the market in 2022 should double, similarly to other countries of the world. Research shows that in 2022, the global value of the cyber-insurance market measured by gross written premium will be around USD 7,000 million.

5. CONCLUSIONS

Cyber risk is now a significant threat to all enterprises, not just those that use the most modern technologies. Moreover, the effects of materialization of such risk may also significantly affect natural persons. Violation of data processed in enterprises may lead to the disclosure of personal or confidential information, which may endanger the interests of society. In turn, such incidents can significantly affect the results achieved by an enterprise. The deterioration of profits may be the result of not only the direct costs associated with the materialization of risk within the enterprise, but also may be the result of the need to pay compensation or sanctions imposed by institutions supervising various market segments. Therefore, proper cyber risk management is extremely important in order to minimize the negative financial consequences for enterprises.

Cyber security is one of the methods that enables this. Although these products are not very popular, especially in countries other than the United States, their dynamic development is noticed, as evidenced by an increase in gross written premium both globally and in individual countries. The coverage of material consequences of cyber risk guaranteed by insurance can minimize business losses, and can also improve reputation as customers and shareholders feel safer seeing that the company has collateral in the form of a policy purchased.

Therefore, the development of the cyber risk insurance market creates huge opportunities for organizations to secure their financial interests against the negative effects of risk materialization, and thus also to be able to conduct standard operations even when there is a real threat of cyber attacks.

REFERENCES

Aon (2018). Cyber Insurance Market Insights – Q3 2018. (http://aoninsights.com.au)

Brockett, P.L., Golden, L.L., Wolman, W. (2012). *Enterprise Cyber Risk Management* [In:] Emblemsvag, J., ed, *Risk Management for the Future – Theory and Cases*, InTech.

CHUBB. *Cyber Risk Management. Guide for Brokers* (https://www.chubb.com)

Colivicchi, I., Vignaroli, R. (2019). *Forecasting the Impact of Information Security Breaches on Stock Market Returns and VaR Backtest*. "*Journal of Mathematical Finance*", 9. DOI: 10.4236/jmf.2019.93024.

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). *Defining Cybersecurity*. "*Technology Innovation Management Review*", 4(10). DOI: 10.22215/timreview/835.

Dankiewicz, R. (2018), A phenomenon of corporate bankruptcy in Poland directions and causes of changes [in:] Majerova, I., ed., Proceedings of 16th International Conference Economic Policy in the European Union Member Countries, Karvina, Silesian University.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J.W., Winkelman, Z. (2018). *Estimating the Global Cost of Cyber Risk: Methodology and Examples*. Santa Monica, CA: RAND Corporation.

EIOPA (2018). *Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies*. Luxembourg: Publications Office of the European Union.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Zhou, L. (2015). *Increasing cybersecurity investments in private sector firms*. "*Journal of Cybersecurity*", 1(1). DOI: 10.1093/cybsec/tyv011.

https://financesonline.com

https://www.statista.com

IIROC (2015). *Cybersecurity Best Practices Guide For IIROC Dealer Members*. https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf.

Kammoun, N., Bounfour, A., Özaygen, A., Dieye, R. (2019). *Financial market reaction to cyberattacks*. "*Cogent Economics & Finance*", 7 : 1645584. DOI: 10.1080/23322039.2019.1645584

Khalili, M.M., Naghizadeh, P., Liu, M. (2017). *Designing Cyber Insurance Policies: Mitigating Moral Hazard Through SecurityPre-Screening*. In L. Duan, A. Sanjab, H. Li, X. Chen, D. Materassi, R. Elazouzi (Eds.), *Game Theory for Networks*, Springer. DOI: https://doi.org/10.1007/978-3-319-67540-4.

Kos-Łabędowicz, J. (2013). *Influence of Modern Technologies on Internationalization of Small and Medium Enterprises*. "*Information Systems in Management*", Vol. 2 (1).

Kubik, K. (2012). *Współczesne przedsiębiorstwa wobec wyzwań globalnej konkurencji*. "*Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie*", No. 19 (92).

Machová, R., Huszárik, E.S., Šimonová, M. (2016). *Selected aspects of innovation policy for small and medium sized enterprises*. "*Journal of International Studies*", Vol. 9, No 2. DOI: 10.14254/2071-8330.2016/9-2/17.

Marsh (2019). 2019 Global Cyber Risk Perception Survey. Marsh LLC.

Martinelli, F., Uuganbayar, G., Yautsiukhin, A. (2018). *Optimal Security Configuration for Cyber Insurance* [In:] Janczewski, L.J., Kutyłowski, M., eds., *ICT Systems Security and Privacy Protection*, Springer. DOI: 10.1007/978-3-319-99828-2.

Meland, P.H., Tøndel, I.A., Moe, M., Seehusen, F. (2017). *Facing Uncertainty in Cyber Insurance Policies* [In:] Livraga, G., Mitchell, Ch., eds., *Security and Trust Management*, Springer. DOI 10.1007/978-3-319-68063-7.

Naylor, M. (2017). *Insurance Transformed: Technological Disruption*. Palgrave Macmillan. DOI 10.1007/978-3-319-63835-5.

Ostrowska-Dankiewicz, A. (2019), *Consumer protection policy in the Polish life insurance market in the aspect of current legal regulations. "Investment Management and Financial Innovations"*, Vol. 16, Issue 4. DOI: 10.21511/imfi.16(4).2019.15

Pomykalski, A., Blażlak, R. (2014). *Współczesne tendencje zarządzania organizacjami poprzez innowacje*. "*Studia Ekonomiczn Uniwersytet Ekonomiczny w Katowicach*", No. 183.

Public Safety Canada (2016). *Fundamentals of Cyber Security for Canada's Critical Infrastructure Community*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf.

Puto, A. (2017). *Cele rozwojowe współczesnych przedsiębiorstw – wyniki badań własnych*. "*Handel Wewnętrzny"*, No. 3 (1).

Refsdal, A., Solhaug, B., Stølen, K. (2015). *Cyber-Risk Management*, Springer. DOI 10.1007/978-3-319-23570-7.

Romanosky, S. (2016). *Examining the costs and causes of cyber incidents*. "*Journal of Cybersecurity*", Vol. 2 (2). DOI: 10.1093/cybsec/tyw001.

Shettya, S., McShanea, M., Zhangb, L., Kesanb, J.P., Kamhouac, C.A., Kwiatc, K., Njillac, L.L. (2018). *Reducing Informational Disadvantages to Improve Cyber Risk Management*. "*The Geneva Papers*", 43.

Strupczewski, G. (2017a). *Ryzyko cybernetyczne jako wyzwanie dla branży ubezpieczeń w Polsce i na świecie*. "*FINANSE Czasopismo Komitetu Nauk o Finansach PAN*", No. 1 (10).

—— (2017b). *Zagrożenia cybernetyczne instytucji finansowych*. "*Journal of Insurance, Financial Markets and Consumer Protection*", No. 2 (24).

Wierzbicka, E. (2017). *Rola ubezpieczeń w zarządzaniu ryzykiem przedsiębiorstwa*. "*Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie*", No 4.

DOI: 10.7862/rz.2019.hss.33

The text was submitted to the editorial office: December 2019.
The text was accepted for publication: December 2019.