CYBER INSURANCE IN BUSINESS PROTECTION FUNCTION FROM CYBERNETIC ATTACKS IN THE DIGITAL AGE

CYBER OSIGURANJE U FUNKCIJI ZAŠTITE POSLOVANJA OD KIBERNETIČKIH NAPADA U DIGITALNOM DOBU

GENZIC, Jasna; MESIC, Matea & AKMACIC, Marko

Abstract: *Cyber space is a determining feature of modern life and key area of the global economy. Due to the dependence on information technology and electronic communication, business subjects are becoming increasingly exposed to various forms of cybercrime. This paper researches into the impact of cyber-attacks on business and explains the concept of cyber insurance as one of the possible tools of risk transfer. Cyber risk management is considered an essential proactive activity, which especially relates to those businesses whose activity is closely related to online business, and the assets of which are mostly intangible, i.e. in the form of data.*

Key words: *cyber space, cyber-attacks, cyber risks, cyber insurance, data protection*

Sažetak: *Kibernetički prostor određujuće je obilježje suvremenog života i ključno područje svjetskog gospodarstva. Zbog ovisnosti o informatičkoj tehnologiji i elektroničkim komunikacijama, poslovni subjekti postaju sve izloženiji raznim oblicima kibernetičkog kriminala. Ovaj rad istražuje utjecaj koji kibernetički napadi imaju na poslovanje te objašnjava pojam cyber osiguranja, kao jednog od mogućih alata za prijenos rizika. Smatra se nužnim proaktivnim djelovanjem upravljati kibernetičkim rizicima, a naročito se to odnosi na one poslovne subjekte čije je poslovanje usko povezano s radom na mreži, a imovina je većinski nematerijalna tj. podatkovna.*

Ključne riječi*: kibernetički prostor, kibernetički napadi, cyber rizici, cyber osiguranja, zaštita podataka*

Authors´ data: Genzić, Jasna mag.rel. int et dip. Libertas International Univeristy, Trg J.F.Kennedy 6b, jasna.genzic@gmail.com; **Mesić,** Matea, bacc.oec., Libertas International Univeristy, Trg J.F.Kennedy 6b, mesic.matea@gmail.com**, Akmačić,** Marko mag.oec., Libertas International Univeristy, Trg J.F.Kennedy 6b makmacic@libertas.hr

1. Introduction

Nowadays pretty much every business activity relays on digital data, information, computers and other devices, which, as a result, makes organizations of all sizes and industries susceptible to cyber-attacks. For a company to be susceptible to a cyber-attack, its size is not of essence, but rather the attractiveness of the information that company holds.[1] In the era of modern digitalization of almost all aspects of living, security and safety, ease of living and safe business conducting are essential in daily communication where all of the personal data and entire global commercial details are prone to be accessed by malicious individuals and, not only make fraudulent actions, but to disrupt local economy that would affect fiscal and monetary systems and consequently affect security of people on a higher scale. With growth of digitalization and new way of data "cloud" storing, mobile banking, networking, and digital socialization as conveniently it may be, it has hidden threats that would have irreversible immanent impact to our lives and future so it is of highest interest to find adequate ways of stopping cybernetic attacks and find ways to secure not only our assets, businesses and data but consequently our way of life itself. A cyber incident can cause devastating damage to any business entity.

The most common consequences are: disruption of business, theft or loss of customers' data, breach of customer data protection rules, damage to data or software, damage to company reputation, shutdown and disruption of operating systems, loss or theft of intellectual property, emotional distress of employees, extortion and demand for ransom, potential business interruption with supply chains and physical damage to property or employees. All of this leads to significant financial losses. Digital world abounds in cyber-attacks of all kinds. Just to name a few: cyber fraud, cyber espionage, cyber warfare, cyber terrorism, cyber-bullying, cyber data theft etc. Such attacks are becoming more and more sophisticated and advanced.

Therefore, there is a constant risk of security oversights that can compromise the functioning of a company.[2] Although the insurance policy alone cannot reduce the risk of cyber-attacks, it is emerging as one of the solutions that acts as a risk-transfer mechanism that protects companies from financial shock.

2. Cyber insurance in business protection function from cyber-attacks in the digital age

Global concerns about digital security are reflected in the Global Economic Forum's 2019 Global Risk Report, which reports that cyber-attacks and massive data fraud (theft) are among the top five biggest risks of the year, signaling their growing importance in the near future.[3] The European Commission has also stressed the importance of European cybersecurity rules, which are crucial for defending European economies and citizens against cyber threats across the EU.

Therefore, cybersecurity has, for the first time, become one of EU priorities, which led to an important progress in this field.[4] Understanding cyber threats and how cyber-attacks take place is only one piece of information-puzzle needed for developing effective protection against these threats. When it comes to cyber-attacks, it is really about trying to change the properties of a computer or about how will computer react to some of the illegal activities that take place on-line, that is, as long as the user is connected to the Internet. Cyber-attacks are greatly facilitated by human behavior. Regardless of the degree of protection, if the user (employee) is not careful, a cyber-attack could still happen, and their computer could be invaded.

Therefore, promoting awareness and educating employees is of key importance in reducing the risk of cyber-attacks and thus minimizing the consequences of cyber-attacks. In addition to human error, there are other significant threats, including financially motivated ones, third parties with authorized access, malicious contractor malpractice and an operational error in the system. Therefore, with the aforementioned employee education and awareness raising, it is also necessary to do the following: to introduce a more complex way to remotely access the network, to develop a strategic plan for responding to cyber-attacks, to improve ways to detect cyber-attacks and events, to implement data loss prevention solutions, to recognize vulnerabilities in time and working constantly on prevention of unintended consequences, to improve attack risk and liability insurance, and to encrypt computers and laptops.

However, what happens when an attack occurs? Can companies protect their business by contracting an appropriate insurance policy and how to do it? Are there any cyber insurance policies and what do they include?

2.1. Cyber insurance market

Insurance plays an important role in managing a company's risk because it acts as a risk transfer mechanism and compensates companies for the losses that will inevitably occur. Cyber insurance can cover various consequences of cyber risk, such as identity theft, breach of data security, or malware insertion that can affect your business. Unlike other types of insurance, there is no standard form under which the insurance industry obtains cyber coverage. On one side, this fact could prove to be an obstacle to buying cover, but on the other, it also allows more room for negotiating terms of the policy than there is in the case of more standard types of cover. Most cyber policies on the market (especially in the USA) offer some combination of traditional liability coverage as protection against third party claims and first party coverage as protection against losses suffered by policyholders. Thus, it can provide coverage for damage to digital assets, business disruption, and incident response costs.

In addition, some cyber insurance policies may provide services that help assess potential exposure to risks and provide technical and legal assistance, for example in public relations in the event of an incident.[5] The offer of the cyber policy depends

on the needs of the customers, the type of cyber risks they are exposed to and their level of digitization, as well as the size and type of services they provide.[6] Given the lack of classic policy standardization, the aspect of communication between insurers and policyholders is essential.

2.2. Cyber insurance market in the Republic of Croatia

Although neither companies nor institutions in the Republic of Croatia are immune to cyber-attacks as such attacks are part of the everyday life (not only of private entities, but also businesses) insurance companies in the Croatian insurance market do not yet offer special cyber insurance in their service portfolio. The problem of the lack of such insurance policies is extremely complex.

The first issue here is questionable cost-effectiveness of providing cyber insurance policies in the Republic of Croatia due to the size of the market, followed by convoluted assessments of potential losses arising from cyber incidents that tend to be uncertain and complex, and the increase in the frequency and severity of cyber-attacks just goes to show it.

2.3. Standardization problem cyber policies

The formation of the cyber insurance market is a continuous process that can only be characterized as volatile. Due to the complexity of risk assessments and the diversified needs of potential clients (companies), every standardization would inevitably very quickly become obsolete. [7] Insurers usually model and create their insurance policies by creating actuarial and historical data. With cyber risk, historical data is scarce, while actuarial data is almost non-existent, with very little publicly available data about cyber-attacks and consequential damage. Furthermore, some losses are difficult or impossible to quantify, especially intangible losses, such as a loss of business reputation, which is a frequent consequence of cyber-attacks.

3. Conclusion

A proactive approach to cyber security is crucial in the fight against various forms of cyber-attacks, which includes investment in security infrastructure. The changes that technological advances bring are constant and rapid. The same is true of hackers that in many ways dictate the speed of change in the virtual world. One of possible solutions would be to get some of the best of them on the side of the fight against cybercrime and thus improve resistance to malicious attacks.

Despite the fact that the cyber risk exposure assessment is very complex, that it is not easy to quantify losses and damage and that the cyber insurance market is still a relatively new area and product, it needs to invest in developing cyber insurance products and educate both employees and private entities about the dangers that threaten in all virtual corners.

4. References

[1] Nanji, S., Cyber Insurance 2015: Guide for Small and Medium Sized Businesses, Amazon Digital Services LLC, 2015.
[2] Christian C., Cyber Insurance Basics: an Installment in the Building Blocks Series of Insurance Content, Cricket Creations, 2014.
[3] Weforum. World Economic Forum's Global Risk Report. Available at: https://www.weforum.org/reports/the-global-risks-report-2019
[4] Svijet Osiguranja. Nedostatak podataka o kibernetičkim rizicima: glavna prepreka razvoju tržišta cyber osiguranja. Available at: https://www.svijetosiguranja.eu/nedostatak-podataka-o-kibernetickim-rizicima-glavna-prepreka-razvoju-trzista-cyber-osiguranja/
[5] Marsh, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk, HM Government, Marsh Ltd., 2015. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf
[6] Financial Times – Should individuals buy insurance against cyber attacks?. Available at: https://www.ft.com/content/72e11ca6-98ad-11e7-8c5c-c8d8fa6961bb
[7] Woodruffsawyer. Get Ready: Cyber Insurance Underwriting is Changing. Available at: https://woodruffsawyer.com/cyber-liability/cyber-insurance-underwriting-changes/

Photo 026. Katedrala Sv. Terezija Avilske u Požegi /