Chapter 19.

CYBERSECURITY AND DIGITAL VIRUSES DURING THE ANALOGOUS CORONAVIRUS PANDEMIC

The popularity and frequency of working from home, the mass use of mobile devices, and the constant improvement of infrastructure increasingly expose both individuals and companies to IT risks, such as viruses, ransomware, phishing and the like. A company is IT secure as much as can resist the threats and attacks of this malicious software. Today, every individual who uses electronic devices and the Internet is faced with this challenge. However, IT security is a much larger and more complex task that companies need to solve in order to ensure each employee and the company as a whole.

IT security is a set of measures that enable the data handled to be protected from unauthorized access, as well as to protect the confidentiality, integrity, and availability of that data so that the system functions as intended when provided and under the control of authorized persons.

When we talk about the confidentiality of data, we are talking about protection from exposure to unauthorized persons. The most common cyber-attacks are related to violating this rule. Examples of large global companies that were the targets of such attacks in 2020 and faced the theft of customer data are Marriott hotels, EasyJet, Zoom, etc.[1]

Integrity means the preservation of the original content and the completeness of the data. For example, if an attacker violated the integrity of the data, the consequence could be that the company's management makes bad decisions based on wrong information or that the presented content is compromising for the company. Violation of integrity is the most difficult to recognize because it is most often performed so that the data are not dramatically changed but enough to provoke the desired reaction of the company.

Availability is the property of data to be available and usable at the request of authorized persons when they need it. This feature is also of great value and is often associated with attacks that cause blocking of the information system.

---

[1] http: //www.keepnetlabs.com/the-biggest-data-breaches-in-the-first-half-of-2020

The evolution of information security

For several decades now, information system security has been an important area, but in the beginning, it was significantly more straightforward and more focused on the physical security of equipment.

During the 1960s, companies became aware of the need to protect their computers. There was no Internet or network at that time, so security was mainly focused on physical protection measures and preventing access to people who had enough knowledge to work on a computer. To achieve this, passwords and multiple layers of security protection have been added to the devices. The history of cybersecurity begins in the 1970s with the ARPANET research project[2] (The Advanced Research Projects Agency Network) which is the forerunner of the Internet. The ARPANET was designed as a military project. The initial idea was to connect American military bases. Later, realizing the possibilities of this project, the concept of connecting only military bases grew into an economically viable investment, which is today called by the unique name Internet. Researchers named Bob Thomas, and Raymond Samuel Tomlinson has been working on this network, examining its shortcomings. Their programs Creeper (the first simulation of a virus) and Reaper (the first example of antivirus software) are famous. Certain groups of people recognized the opportunity to sneak into these networks and steal critical data. That's how the first hackers came to be. In the years that followed, computers began to connect more and more, computer viruses became more and more advanced, and information protection systems could not keep up with the constant progress of innovative approaches to hacking. The year 1987 is significant because that is the moment when the first commercial antivirus programs were created. The 1990s brought a new concept of data protection using software known as a firewall. As the Internet became available to the public, more and more people began to put their personal data on remote servers and share information over the network. In the early 2000s, authorities began to crack down on hacking, using much stricter penal policies, including imprisonment and significant fines.

The 2010s are an era of significant data theft. Due to the constant advancement of technology, hacking became more and more complicated in the following years. Still, the security of information was constantly improving, so that many companies implemented a wide range of tools to prevent and mitigate attacks.

---

[2] Featherly, K. (2021). *ARPANET United States defense program*. www.britannica.com/topic/ARPANET

The evolution of information security continues, faster and more intense every day.[3]

CYBERSECURITY

In response to the great exposure of the business to these risks in the digital world, one class of information security has been vigorously developing in recent years - cybersecurity. While traditional IT security deals with all aspects of information system protection, from the physical security of equipment and network, protection from unintentional or intentional system loss to information protection, cybersecurity is its subset specifically focused on protecting data and networks from malicious influences coming digitally. The main actors in this fight are, on the one hand, cyber attackers known as hackers; while on the other hand, there are entire teams that companies are developing to protect information systems as effectively as possible. Cybersecurity is no longer just a matter of IT experts. It is a holistic concept that implies the readiness of the entire organization, both in terms of technology and in the educational development of each individual.

Cyberattacks

Like any other form of crime, cybercrime is the search for personal satisfaction through socially dysfunctional behavior. Motives can be different, from financial and reputational to ideological. Depending on the type of motive, there are various forms or categories of hacking: hacktivism (examples WikiLeaks and Anonymous), cybercrime, insider disclosure, cyber-warfare[4], cyber terrorism, and cyber espionage. Any of these motives for the attack cause three fundamental consequences for the victim. The economic impact is the most common and always present consequence, followed by reputational decline and finally regulatory problems.

Cyber-attack techniques

Hackers rarely use a single technique when performing attacks. The attack usually occurs in several phases, combining different methods that are not exclusively of a programming nature. An indispensable part is also psychological or social preparation, where the attacker first studies the

---

[3] Shakeel, I. (2016). *Evolution in the World of Cyber Crime.* https://resources.infosecinstitute.com/topic/evolution-in-the-world-of-cyber-crime

[4] Sheldon, J. (2016). *Cyberwar*. www.britannica.com/topic/cyberwar

company's weaknesses in terms of personnel and organization, which is a component known as social engineering.

Malware is malicious software that attacks a computer network and devices on the web trying to get into the information system itself. The range of malware is vibrant. These include viruses,[5] Trojans, worms, coin miners, and currently particularly dominant ransomware.

A malware called ransomware has attracted particular attention in recent years. The concept of this attack is for the attacker to take control of the system and then lock the computer by encrypting the files. In order for the files and the device to become operable again, the hacker requires a certain amount of money for redemption to give instructions and a code to unlock the system. As more and more data is clouded in our digital age, the number of attacks and the success of ransomware attacks are growing.[6] The redemption price ranges from several hundred to several million dollars and is paid to some of the cryptocurrencies, for example, bitcoin. Among these attacks, the most famous is the world attack WannaCry[7] in May 2017. In 2020, ransomware continued to thrive, so the most famous attacks were NetWalker, REvil, Maze, and WastedLocker.

DDoS (Distributed Denial of Service) is one of the older attack techniques. An attacker tries to block the system's operation by sending a massive number of requests to a server that provides an online service at once. In this way, the server becomes overbooked with requests, so its performance drops, and in the end, it is completely blocked and cannot accept any new request.

The Man-in-the-middle is a type of attack where an attacker intercepts online communication between two parties and uses it to obtain information exchanged in that communication.

A botnet (robot network) is an attack technique that involves creating many infected computers controlled by an attacker. In that way, he makes the so-called "army of zombies" he manages to attack the next victim further. This is often the preparatory phase for large-scale DDoS attacks.

---

[5] Scientific American (2001). *When did the term 'computer virus' arise?* www.scientificamerican.com/article/when-did-the-term-compute
[6] Johnson, J. (2021). *Many ransomware attacks per the year 2014-2020*. www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide
[7] Group of authors. (2017). *WannaCry: The ransomware cyber-attack explained.* https://dig.watch/trends/wannacry

Social engineering is a set of techniques that attack system users to reveal passwords, confidential data, or open a gateway for malicious programs. This area implies psychological manipulation of the victim so that by combining technical knowledge, the attacker reaches the final goal.

Phishing or identity theft fraud is an attack in which a target or targets is contacted by someone posing as a legitimate institution in order to entice individuals to provide sensitive personal information. The information is then used to access essential resources and can result in identity theft and financial loss. Phishing[8] was patented in 1995 by the American company America On-Line (AOL), which was the number one provider of Internet services. Phishing has not changed much since its launch until today. Organizations lose about $ 2 billion a year due to phishing.

A modern technique is baiting. The bait can be a free open network or a site for free downloading of interesting content or a USB device that someone left or shares for free in a public place.

After all, even digital junk like an old smartphone or laptop can be a source of information for hackers. This area is often called dumpster diving.

The company's response to IT vulnerabilities

To defend themselves from numerous attackers, companies must provide complex systems to protect their assets. The long-term strategy to combat the dangers lurking in the IT world is to create a culture of cybersecurity. This is a commitment to data protection throughout the organization in which technology, policies, and processes are designed with security threats in mind.
It is known that hackers will not sleep while organizations carry out digital transformation and switch their business to online and cloud services. What remains as a solution is an insurance against cyber-attacks. Only in this way can companies be sure that they will not have significant financial losses even if they do not defend themselves from hackers.

HISTORICAL DEVELOPMENT OF CYBER INSURANCE AND LITERATURE REVIEW

Cyber risks are excluded or partially covered by traditional property insurance. When insuring things, if the computer is the subject of insurance, hard disks and

[8] www.phishing.org

programs listed in the insurance offer are included. Losss caused by data loss, interruption of work, or loss of earnings may be expressly agreed upon. In traditional property insurance, for these losss to be covered by insurance, they must arise due to loss or destruction of the hardware. In the modern insurance market, various policies cover losss caused by loss, loss, or manipulation of data and cases when the hardware is not lossd.

The first contracts to cover cyber risk were concluded about forty years ago in the United States. They provided compensation in the event of monetary losses caused by personal or business data breaches, interruption due to hacker attacks or other causes, loss of business reputation, third party liability and legal protection insured. [9] Risks are insured regardless of the cause that led to the loss. In the modern insurance market, cyber risks that can lead to catastrophic loss, which occur in wartime circumstances resulting from terrorism or endangering infrastructure systems, are difficult to insure. It is considered that the government should establish mechanisms for their coverage.

Many authors in the world have been dealing with cyber insurance in the last twenty years. Bohme and Kataria were among the first to publish the paper[10] on cyber insurance in 2006. They proved that the cyber insurance market could not be established due to the high correlation of clients. Bandyopadhyay[11] in 2009 claimed that the premium of cyber insurance is usually higher than necessary to cover the risk because insurers overestimate possible losss due to the loss of reputation. Bolot and Lelarge[12] argued in the same year that cybersecurity could establish a major incentive for companies to improve their information security. Bohme and Schwartz[13] published a framework that includes various models and assumptions about cyber insurance from the then-available literature in 2010. Recent literature offers an empirical study of database burglaries[14], an overview

---

[9] Pak, J. (2014). *Internet risk insurance*. International Scientific Conference of Singidunum University Synthesis, p. 71-76

[10] Bohme, R., Kataria, G. (2006). *Models and Measures for Correlation in Cyber-insurance*. Workshop on Economics of Information Security - WIES

[11] Bandyopadhyay, T., Mookerjee, VS, Rao, RC (2009) Why IT managers don't go for cyber-insurance products. *Communication of ACM 52 (11),* p. 68–73.

[12] Bolot, J., Lelarge, M. (2009). *Cyber Insurance as an Incentive for Internet Security*. Springer: Managing information risk and the economics of security, p. 269–290.

[13] Böhme, R., Schwartz, G. (2010). *Modeling Cyber-Insurance: Towards a Unifying Framework*. Workshop on Economics of Information Security - WIES

[14] Edwards, B., Hofmeyr, S., Forrest, S. (2015). *Hype and heavy tails: a closer look at data breaches*. Workshop on the Economics of Information Security (WEIS)

of the cyber insurance market in Sweden[15], optimization of cyber insurance coverage using security controls[16], etc.

Domestic authors have published papers on the topic of cyber insurance in the last few years. The most recent, publicly available works were published in the previous year by Petrović,[17] on the topic of legal aspects of cyber insurance, and Stajšić Golijanin[18] on cyber risk management from different perspectives.

INCREASED IT RISKS AS A RESULT OF THE PANDEMIC

Definition of cyber risk

There are numerous definitions of cyber risk, adapted to the specific purposes or activities of individual organizations that bring them. The definition of the CRO Forum is[19]: "Cyber risk poses a risk of using and transmitting electronic data, including technological means such as the Internet and telecommunications networks." The Institute for Risk Management in London gave the following definition[20]: "Information risk means financial loss, loss or loss to the organization's reputation due to some kind of failure of its information technology systems." The definition from the free encyclopedia Wikipedia can also be interesting[21]: "Cyber risk is any type of offensive behavior of individuals or organized computer programmers, aimed at targeted computer information systems, infrastructure, computer networks and/or personal computers for theft, alteration or destruction, usually from unknown locations." Jovanović gave a domestic definition of information risk[22] as a danger of harmful use and manipulation of digital instructions and information that may cause financial loss to property and persons and loss related to the fulfillment of legal obligations.

---

[15] Franke, U. (2017). The Cyber Insurance Market in Sweden. *Computers & Security 68*, p. 130-144.
[16] Uuganbayar, G. (2021). Optimization of cyber insurance coverage with a selection of cost-effective security controls. *Computers & Security 101*, p. 102-121.
[17] Petrović, S. (2020). Cyber insurance. *Law and Economy 1/2020*, p. 206-217.
[18] Stajšić Golijanin, N. (2020). Insurance as a way to manage cyber risks. *Proceedings of the Faculty of Technical Sciences, vol. 35, no. 10.*
[19] CRO Forum. (2014) *Cyber resilience: The cyber risk challenge and the role of insurance*. Amsterdam: CRO Forum & KPMG Advisory NV
[20] The Institute of Risk Management. (2014) *IRM Cyber Risk: Executive Summary*. London: The Institute of Risk Management
[21] https://en.wikipedia.org/wiki/Cyber-attack
[22] Jovanović, S. (2017). Information risk insurance. *Topics, Mr. XLI, no. 3*, p. 823-837.

Cyber risk strategy

The previous considerations can be summarized in ten steps to establish cybersecurity[23] with an additional eleventh step, which complements the strategy to combat cyber threats:

1. Implement an efficient management structure in the company, ensure the engagement of the management in improving cybersecurity and adopt an information security policy
2. Organize regular training on IT security for employees
3. Adopt procedures for managing IT incidents, which include a method for recovering IT systems in the event of a disaster
4. Adopt a policy and procedure for computer network security
5. Monitor the implementation of policies and procedures related to the computer network and information system
6. Manage user privileges
7. Provide documentation for the configuration of the information system and computer network
8. Introduce procedures to protect against viruses and other malicious code
9. Control the use of removable media, USB memory, etc.
10. Check compliance with work from distance procedures
11. Arrange cyber risk insurance

MANAGEMENT OF INCREASED IT RISKS THROUGH CYBER INSURANCE

One of the most effective ways to manage increased IT risks is insurance coverage and protection in the event of loss. Any company that uses the Internet or cloud technology is exposed to cyber dangers. Examples of cyber risks may be extortion due to data misuse, hacker attacks that take money from bank account, other types of cyber theft, liability for data storage, disclosure of confidential data to site visitors, breach of integrity and confidentiality of electronic information, computer security breaches, industrial espionage, cyber terrorism, loss to the company's reputation, disruption in the supply chain, etc.

The target of cyber-attacks can be any company that uses modern information technologies. However, information assets are insured by only about 15% of companies, while the share of insured companies is significantly higher in fire

---

[23] Allianz Global Corporate & Specialty (2015). *A Guide to Cyber Risk*. http://www.agcs.allianz.com

insurance and is 59%, with the probability of realizing an insured fire event is less than the probability of realizing the cyber risk.[24]

Cyber insurance policy

Insurance protection is provided for two groups of risks that arise in cyberspace. The first group consists of risks that lead to direct property losses such as the costs of determining the cause of loss, notifying stakeholders, eliminating deficiencies and re-establishing a computer system, reducing income due to downtime, costs of injury and loss of data, money paid in the name of blackmail as and the cost of providing legal aid. The second group of risks consists of sources of danger from liability for losss that the insured is obliged to compensate to third parties due to violation of personal data, infringement of parts, and reputation and intellectual property rights.

The cyber insurance policy offers the following coverage:

1) Responsibility for professional IT services[25] - if the company provides IT services, the cyber insurance policy provides financial protection against professional liability, i.e., the company's liability for technology-based services, IT products, information security, etc. The cyber policy provides support in the following cases of breach of contract: negligence in the performance of obligations, error or omission in the provision of professional technical services or failure to provide them; unintentional breach of contract; slander, loss to reputation, inflicting mental pain; plagiarism, piracy or misappropriation of ideas.
2) Responsibility for multimedia content[26] - if multimedia is part of the company's service, e.g., design and development of websites, cyber insurance policies to provide coverage for incurred costs in the event of a lawsuit for defamation, loss to reputation, causing mental pain; violation or interference with the right to privacy or violation of the rights of a person in public; plagiarism, piracy or misappropriation of ideas; infringement of copyright, domain name, title or slogan; negligence of the service provider in connection with the publication of multimedia content on the Internet or in the print media; unfair competition.
3) Responsibility for the security and privacy of third party data - the security of personal data on the Internet is exposed to many risks such as unauthorized access or unauthorized use of the computer network; failure to

---

[24] Filipović, Z. (2018). *Cyber risks - Challenges of the digital age*. Other Serbian insurance days, Arandjelovac

[25] http://respect-serbia.rs/cyber-i-it-osiguranje/

[26] https://vib.rs/sajber-osiguranje/

prevent physical theft or loss of information or hardware; security vulnerabilities; failure to prevent fraudulent communication designed to obtain personal information from fraudulent users, etc. The cyber insurance policy reimburses the costs of the lawsuit due to negligence or inadequate storage and sharing of data.

4) Liability for spreading a virus or other malicious program code - covers the costs incurred by third parties due to claiming losss from a virus proven to originate from the company network.
5) Costs caused by theft of company data - hacker intrusions into the company's computer network can lead to the theft of various valuable confidential data stored on local servers. One example is the theft of data on the technological development of the company's products, i.e., industrial espionage.
6) Costs of necessary actions imposed by regulations - in case of a cyber incident in the company or compromise of customer data, the regulations require the implementation of specific procedures, e.g., in connection with privacy regulations. The implementation of such activities usually requires certain costs, so a cyber insurance policy is a reliable way to reimburse the mentioned costs.
7) Costs of representation in court and penalties of the competent state bodies - legal services of defense in court and all fees according to decisions made by judicial bodies or regulatory bodies can be provided.
8) Costs of informing users and crisis management that arise as a result of data privacy violation - one of the obligations of a company facing a cyber incident is to respond to a privacy violation, i.e., informing users and crisis management. Often such situations do not pass without the costs of hiring experts, as well as the costs of media announcements. Cyber insurance policies cover these costs.
9) Lost operating profit due to business interruption - the consequence of a cyber incident may be lost operating profit due to disruption of the regular operation of the company and the occurrence of possible additional operating costs. The cyber insurance policy provides financial support for recovery from a cyber incident and thus reduces the time required to re-establish the regular operation of the company and also compensates for lost business profits during the cyber incident. The policy covers the direct cost of the insured company, but not the loss due to lawsuits of lossd third parties.
10) Data recovery costs - one of the consequences of a cyber incident is the cost of re-establishing the business. The cyber insurance policy covers the following expenses of conducting the data recovery procedure: for re-returning, collecting, or replacing data, including costs for materials and working hours; for the use of rented equipment; for overtime work of employees; for hiring external experts, investigators, forensics…

11) Costs of cyber extortion - extortion of a certain amount for the return of compromised, lossd, or destroyed company data to its previous state, are one of the most expensive cyber incidents. It is most often the result of the spread of a computer virus, malicious program code, or the disabling of the use of information services (DoS). A cyber insurance policy offers the necessary financial protection even in the event of such enormous loss.
12) Responsibility for making electronic payments - the costs of stealing money from clients' accounts are covered if their data is compromised, e.g., about credit cards used to pay for the services of an insured company or an insured bank that processes payments through Internet sites.

It is expected that physical loss caused by a cyberattack is not covered by the policy, similarly, as physical loss from a cyber-attack is excluded by property policies. Exclusion always occurs for loss caused by criminal activities of the insured, as well as terrorist attacks. Exclusion for unauthorized collection of client data is often encountered, as well as the exclusion for loss that may occur due to non-compliance with the contract from the IT industry by the insured because the costs arising from these cases are caused by the insured's activities that are not following law or contract.

The highest probability for small and medium enterprises, of about 5%, is to realize the following risks: business interruption, cybercrime and fraud, and endangering personal data privacy.[27]

Cyber insurance policies are offered by the world's largest insurance companies such as AIG, Chubb, CNA, Allianz, Zurich, etc.

Policy activation

Cyber policies, similar to other liability insurance policies, can be contracted to be activated at the moment of data compromise or at the moment when the loss occurred due to data compromise. No matter what is agreed, that moment should be during the duration of the policy. Cyber policies can also have a third option of activation if they cover the costs of necessary actions imposed by regulations or the competent state authorities. Activation can then take place in accordance with regulations or an order of the regulatory body.

---

[27] Bara, D., Ćorić, S., Jurišić, G. (2015). *The role of cyber insurance in managing and mitigating cybersecurity risk with particular emphasis on the potential of Croatia and Serbia cyber insurance market.* Proceedings from IT / ICT Conference Kladovo 14-16.05.2015.

One example of activating a policy in the event of an error or negligence in the provision of services: An IT company provides a payment platform for e-commerce customers. The programmer inadvertently causes a system crash that lasts for several days. This drop causes customers to miss a large number of new jobs that week. The policy would cover claims that clients would file due to lost profits due to downtime due to the unavailability of the payment platform.

Appetite for cyber risk

Risk appetite is the level of tolerance of a company to a specific risk, i.e., how much risk a company can bear to accomplish a given business plan or how much money a company is willing to invest in managing a specific risk. The company's management should define risk appetite. Based on the adopted appetite for various risks, the company determines priorities in risk management, i.e., where it is most necessary to invest time and resources to reduce the defined tolerances' chances.

The appetite for cyber risk should be determined jointly by the President of the Executive Board, the member of the management board responsible for information security and the member of the management board responsible for risks. Determining the appetite for cyber risk is done through continuous assessment, using quantitative and qualitative methodologies whose validity has been confirmed in practice. Constant review is the key to successfully determining risk appetite.

CYBER INSURANCE PREMIUM

The cyber insurance market in the region is underdeveloped, so there is a very short history of losss paid by insurance companies. Therefore, the determination of the premium is based more on qualitative than quantitative methods.

The premium depends on many factors that more or less affect the size of the risk and thus the price of insurance.[28] As expected, the size of the company's revenue is directly proportional to the size of the risk. The activity of the insured is one of the most critical risk factors, for example. Cyber-attacks are known to do the most loss to healthcare, small and medium enterprises, as well as companies that have a large number of credit card payments. Geographical

[28] Franke, U. (2017). The Cyber Insurance Market in Sweden. *Computers & Security 68*, p. 130-144.

representation is also a significant risk factor, as it is more difficult for international companies to meet all the requirements of various local regulations and preserve their data, which travels a lot worldwide. As with other types of insurance, the coverage limit contracted by the insured affects the price of the policy because the higher the limit and the higher the risk, while on the other hand, if the insured's participation in the loss is contracted, the premium decreases. The level of information security of the company also significantly affects the premium. For information security management, companies that meet, e.g., ISO 27001 standard, have a lower risk of cyberattacks. Finally, as with other types of insurance, the technical result of the company from the past also affects the price of cyber insurance.

Insufficient data on cyber claims can only be overcome by involving reinsurers in the premium determination process, as they have significantly more experience in this matter than individual insurers. The typical premium rate recommended by the world's major reinsurance companies is of the order of 1%. This insurance is relatively expensive compared to other types of insurance, e.g., about three times more costly than a general liability and nearly six times more costly than property insurance.[29]

ALE method

The ALE (Annualized Loss Expected) method is most often used in practice. The premium rate is determined and then is adjusted by certain factors. This method of calculating the insurance premium uses the following formula for expected annual loss (ALE):

$$ALE = ARO * SLE$$

Where:
ARO from Annualized Rate of Occurrences - the average annual number of loss events
SLE from Single Loss Expectancy - the average amount of loss per realization of one risk

This formula represents a technical premium, to which it is necessary to add an overhead allowance, which is usually about 30% for this type of insurance.

[29] Paunović, M., Ralević, N. (2019). C*yber-risk management and actuarial analyzes*. XVII International Symposium "Insurance on the Threshold of the IV Industrial Revolution," Zlatibor

The basic premium obtained in this way is adjusted by specific factors, which refer to the company's business activity, company size, and annual revenues. [30] The following data on the IT performance of policyholders is an essential indicator of risk exposure that affects the possible adjustment of premiums: whether the development of information systems is entrusted to other companies, whether cloud computing technology is used, whether sensitive personal data is processed, and stored, whether access to data via the Internet, etc. Important factors that affect the premium are the insurance limit, participation in claims and available data on claims and incidents in the previous period. Finally, corrective factors are formed based on elements related to the assessment of IT vulnerability and security. The impact of individual risk factors is assessed using a risk matrix.

Risk matrix

The risk matrix is a qualitative model that combines the classification of the probability of risk occurrence with the risk occurrence consequences intensity classification to determine the classification of risk levels. In this matrix, the principle is that higher probability and higher intensity imply higher risk. The risk matrix can also be used as a pseudo-quantitative method because the classification of probabilities can be expressed in numbers. The key advantages of using a risk matrix are reliable identification of sources of threats, reduction of long-term costs due to preventive activities, increasing the company's ability to assess its weaknesses, which improves the risk management system through periodic review, improving compliance, and eliminating excessive reliance on the subjective assessment about the system they manage.

An example of a risk matrix is shown in Figure 1. The intensity of the loss occurrence consequence is shown in the columns and the probability of the risk occurrence in the rows of the matrix. Probability is defined as the possibility that a specific situation may occur or that a particular event may lead to negative consequences and may range from "very rarely" to "several times a year."[31] The intensity of the risk realization consequence shows how much loss will be done if the risk is realized and can range from "small consequences" to "catastrophic consequences."

---

[30] Romanosky S. et al. l (2017). Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? *SSRN Electronic Journal, January 2017*

[31] Draper, G. (2019). *Managing Cybersecurity Risks Using a Risk Matrix*. https://fortsafe.com/managing-cybersecurity-risks-using-a-risk-matrix/

The risk matrix is used to determine the priorities of preventive activities aimed at preventing the consequences of the realization of various risks. Figure 1 shows that the most important thing is to manage the risks that belong to the class of extreme intensities and medium or high probability (fields 11 and 12) and then high risks from fields 7, 8, 9, and 10.

Figure 1 Risk assessment matrix

Risk assessments:	**Low** 0-acceptable	**Medium** 1 - reasonably low	**High** 2 - generally unacceptable	**Extreme.** 3 - unacceptable

		Intensity:			
		Acceptable (no effect)	**Tolerant** (effects not critical)	**Unwanted.** (great effect)	**Intolerant.** (can lead to disaster)
Probability	**Improbable** (most likely won't happen)	Low (1)	Medium (4)	Medium (6)	High (10)
	Possible (risk will probably materialize)	Low (2)	Medium (5)	High (8)	Extreme (11)
	Probable (risk is likely to occur)	Medium (3)	High (7)	High (9)	Extreme (12)

Source: Draper, G. (2019). *Managing Cybersecurity Risks Using a Risk Matrix*. https://fortsafe.com/managing-cybersecurity-risks-using-a-risk-matrix/

CYBER REINSURANCE

Cyber reinsurance is relatively underdeveloped, as the dilemmas in the development of reinsurance products are identical as in insurance. Cyber risks are often excluded in property reinsurance contracts.

However, since the capacity of insurance companies is insufficient, reinsurance is often necessary in practice. That is why the share offered by reinsurers on a quota basis is often up to 30%. Reinsurers are conservative in terms of overall cyber risk exposure, so they often require limitations on harmful events for business interruption and various franchises (by amounts or by time) and exclude coverage in certain areas they consider riskier. They also introduce multiple exclusions, such as for devices such as non-encrypted USB storage. A large part of cyber reinsurance is placed in London and Bermuda.

CYBER INSURANCE IN SERBIA

Wiener Städtische osiguranje in Serbia offers cyber risk insurance. There are particular prerequisites that a company wishing to enter into a contract for this type of insurance with Wiener must meet: regularly updated antivirus software must be installed on every computer in the company, key data must be regularly copied and stored in a secure remote location, network traffic control must be established, and there must be a clear company information security policy.

In addition to fulfilling the prerequisites, the company fills out a questionnaire with basic information about its information system, applied protection, method of data transfer and storage, but also financial data, information on the impact on regular business, number and nature of personal data of third parties, etc. Based on this information, risk-takers decide on insurance admission and determine an adequate premium.

Wiener's cyber insurance policy[32] in Serbia can be concluded for the purpose of protection against theft, misuse, or alteration of company data. This policy covers the costs of hiring IT experts to determine the extent of the loss, its limitation and data recovery, removal of malicious code or virus, and the like. Cyber insurance also covers the loss that a company may suffer due to the endangerment of clients' personal data by reimbursing the costs of hiring legal advisors, crisis advisers, informing the persons whose data are endangered, and other expenses incurred to preserve the company's reputation. A cyber incident may indirectly trigger management liability. The manager's liability insurance policy covers the costs of management's defense in court and covers losses if the court finds the administration guilty. The direct financial consequences of a cyber incident are also covered. The cyber insurance policy also reimburses the fines imposed on companies by the competent state authorities, the costs of crisis management, the costs of informing users, and customer support costs. In the event of the spread of malicious code or a virus that losses or prevents access to computer systems and data due to the desire to extort, the cyber insurance policy compensates for the determined lost profit and pays the extortion costs if hired IT experts determine it is necessary.

LITERATURA

[32] https://www.ekapija.com/news/3051143/wiener-staedtische-osiguranje-vazno-je-osigurati-se-od-sajber-rizika

1. Allianz Global Corporate & Specialty (2015). *A Guide to Cyber Risk*. http://www.agcs.allianz.com
2. Bandyopadhyay, T., Mookerjee, V.S., Rao, R.C. (2009) Why IT managers don't go for cyber-insurance products. *Communication of ACM 52(11)*, p. 68–73.
3. Bara, D., Ćorić, S., Jurišić, G. (2015). *The role of cyber insurance in managing and mitigating cyber security risk with special emphasis on the potential of Croatia and Serbia cyber insurance market.* Proceedings from IT/ICT Conference Kladovo 14-16.05.2015.
4. insurance market, Proceedings from IT/ICT Conference Kladovo 14-16.05.2015.
5. Bohme, R., Kataria, G. (2006). *Models and Measures for Correlation in Cyber-insurance*. Workshop on Economics of Information Security (WIES)
6. Böhme, R., Schwartz, G. (2010). *Modeling Cyber-Insurance: Towards a Unifying Framework*. Workshop on Economics of Information Security (WEIS)
7. Bolot, J., Lelarge, M. (2009). *Cyber Insurance as an Incentive for Internet Security*. Springer: Managing information risk and the economics of security, p. 269–290.
8. CRO Forum. (2014). *Cyber resilience: The cyber risk challenge and the role of insurance*. Amsterdam: CRO Forum & KPMG Advisory N.V.
9. Draper, G. (2019). *Managing Cybersecurity Risks Using a Risk Matrix*. https://fortsafe.com/managing-cybersecurity-risks-using-a-risk-matrix/
10. Edwards, B., Hofmeyr, S., Forrest, S. (2015). *Hype and heavy tails: a closer look at data breaches*. Workshop on the Economics of Information Security (WEIS)
11. Featherly, K. (2021). *ARPANET United States defense program*. www.britannica.com/topic/ARPANET
12. Filipović, Z. (2018). *Cyber rizici – Izazovi digitalnog doba*. Drugi srpski dani osiguranja, Aranđelovac
13. Franke, U. (2017). The Cyber Insurance Market in Sweden. *Computers & Security 68*, p. 130-144.
14. Johnson, J. (2021). *Number of ransomware attacks per year 2014-2020*. www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide
15. Jovanović, S. (2017). Osiguranje od informatičkih rizika. *Teme, g. XLI, br. 3*, p. 823-837.
16. Krivokapić, D., Petrovski, A., Malinović, S. (2017). *Mere za zaštitu IKT sistema od posebnog značaja*. Share fondacija: Vodič za IKT sisteme od posebnog značaja, informaciona bezbednost, p. 19.
17. Marotta, A. et all. (2017). Cyber-insurance survey. *Computer Science Review 24(2017),* p. 35-61.

18. Pak, J. (2014). *Osiguranje Internet rizika*. Međunarodna naučna konferencija Univerziteta Singidunum Sinteza, s. 71-76
19. Paunović, M., Ralević, N. (2019). C*yber-Risk Management and Actuarial Analyses*. XVII međunarodni simpozijum „Osiguranje na pragu IV industrijske revolucije“, Zlatibor
20. Petrović, S. (2020). Sajber osiguranje. *Pravo i privreda 1/2020*, p. 206-217.
21. Romanosky S. et all (2017). Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? *SSRN Electronic Journal, January 2017*
22. Scientific American (2001). *When did the term 'computer virus' arise?* www.scientificamerican.com/article/when-did-the-term-compute
23. Shakeel, I. (2016). *Evulution in the World of Cyber Crime.* https://resources.infosecinstitute.com/topic/evolution-in-the-world-of-cyber-crime
24. Sheldon, J. (2016). *Cyberwar*. www.britannica.com/topic/cyberwar
25. Stajšić Golijanin, N. (2020). Osiguranje kao način upravljanja sajber rizicima. *Zbornik radova fakulteta tehničkih nauka, god. 35, br. 10.*
26. The Institute of Risk Management. (2014). *IRM Cyber Risk: Executive Summary*. London: The Institute of Risk Management
27. Uuganbayar, G. (2021). Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security 101*, p. 102-121.
28. http://www.keepnetlabs.com/the-biggest-data-breaches-in-the-first-half-of-2020
29. http://www.phishing.org
30. http://respect-serbia.rs/cyber-i-it-osiguranje/
31. https://vib.rs/sajber-osiguranje/
32. https://en.wikipedia.org/wiki/Cyber-attack
33. https://www.ekapija.com/news/3051143/wiener-staedtische-osiguranje-vazno-je-osigurati-se-od-sajber-rizika