Grzegorz Strupczewski*

The concept of cyber insurance and its role in the ISO-based risk management process: An industrial perspective[1]

Abstract

With cyber threats rapidly growing, cyber risk insurance is emerging as a solution that can complement traditional cyber security tools based on technical and organizational measures. Moreover, the well-established risk management standards, such as ISO 31000 and ISO 27000, identify cyber insurance as having an important role to play in financing the negative impact of cyber risk. Accordingly, the purpose of this paper is to present the concept of cyber insurance and its key features, such as scope of coverage, areas of application, underwriting and premium calculation principles. The analysis is focused on industrial enterprises, which in many cases belong to the state's critical infrastructure. They face not only pure cyber risk, but also cyber-physical risk, which means particularly high severity of potential losses. This study can have practical value in the context of requirements of the new NIS 2 Directive.

Key words: cybersecurity, cyber insurance, risk management, ISO 27000, ISO 31000

* Assoc. Prof. Grzegorz Strupczewski, PhD, Department of Risk Management & Insurance, The Cracow University of Economics, e-mail: Grzegorz.Strupczewski@uek.krakow.pl, ORCID: 0000-0002-7882-120X.

1 Publication financed by the Krakow University of Economics within the Support for Conference Activity Program WAK-2022.

Introduction

Cyber risk remains among the top risks facing business organizations today. The World Economic Forum's „Global Risk Report 2021" lists cybersecurity failure as a top „clear and present danger" and critical global threat[2].

Cyber risk is continually evolving, meaning insurers should understand emerging risks to keep pace with their clients' exposures. Continued trends of increased cloud adoption in industrial operations, the convergence of IT and OT, and the proliferation of IoT and smart manufacturing can exacerbate security concerns and increase exposure profiles. However, crossing the divide between information technology (IT) and operational technology (OT), along with increases in automation and the sophistication of threat actors, means it is paramount that insurers carefully consider how major losses may occur and the potential impacts. The risk of a cyber-physical ICS incident is increasing, especially for individual entities. Lloyds of London recognizes the prevalent cyber risks to Industrial Control Systems (ICS) and lists four key industries dependent upon ICS: Manufacturing, Shipping, Energy and Transportation.

The potential for physical perils represents a major turning point for the broader cyber insurance ecosystem. This risk has previously been considered unlikely to materially impact the market, with cyber perils traditionally emerging in the form of non-physical losses. According to Lloyds, three plausible scenarios consider:

1) a targeted supply-chain malware attack, in which malicious actors breach a device manufacturer and compromise that manufacturers product before distribution,

2) a targeted Internet of Things (IoT) vulnerability attack, in which attackers exploit a vulnerability in widely used IoT devices found in industrial settings,

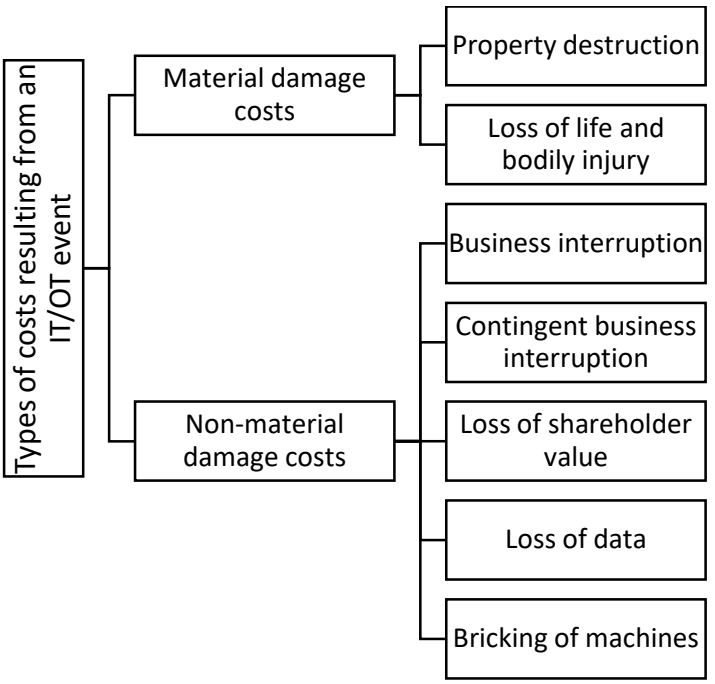
3) the infiltration of industrial IT networks to cross the OT „air-gap"[3].

An OT event could conceivably trigger a loss that leads to property damage and loss of life in one entity, and lead to extensive forensics, remediation, and

2 *Global Risks Report 2021*, World Economic Forum, http://www3.weforum.org/docs/WEF_The_Global_Risks_ Report_2021.pdf [access: 23.11.2022].

3 *Cyber risk. The emerging cyber threat to industrial control systems*, Report by Lloyd's & Guy Carpenter, https://assets.lloyds.com/media/542bea95-0d28-4ce1-a603-63db54aa24f9/The%20Emerging%20Cyber%20Threat%20to%20Industrial%20Control%20Systems_Final%2016.02.2021.pdf [access: 4.12.2022].

product recall as necessary to limit further damage. The types of costs that could conceivably arise following an IT/OT cyber event are shown at Figure 1.



Source: own work based on *Cyber risk. The emerging cyber threat*..., p. 13.

Fig. 1. Types of costs arising after an IT/OT cyber event

Cybersecurity is a challenge facing every organization today. In the era of digitization of enterprises, IT security plays an increasingly important role – it is no longer a challenge just for cybersecurity specialists, but often have an impact on business processes. Global losses from cyberattacks already amount to hundreds of billions of dollars.

World Economic Forum has designed a list of six principles to support board oversight of a cyber-resilient organization while driving strategic goals. These principles are:

1) Cybersecurity is a strategic business enabler – effective organizational cybersecurity directly contributes to both value preservation and new opportunities to create value for the enterprise and larger society;

2) Understand the economic drivers and impact of cyber risk – for organizations to make effective business decisions, risk determinations should

focus on the financial impact to the organization, including trade-offs between digital transformation and cyber risk;

3) Align cyber-risk management with business needs – by focusing on how to treat cyber risks (through avoidance, acceptance, mitigation or transfer), organizations can build a security profile that aligns with business needs and defined risk tolerances or risk appetite;

4) Ensure organizational design supports cybersecurity – organizations should design an internal governance structure that addresses cybersecurity on an enterprise-wide basis;

5) Incorporate cybersecurity expertise into board governance – boards must avail themselves of external industry and other guidance as well as the cybersecurity expertise of fellow directors, third parties and internal resources to effectively oversee the organization's cybersecurity within an appropriate structure focused on oversight;

6) Encourage systemic resilience and collaboration – the highly interconnected nature of modern organizations means we run the risk of failures that spread beyond one enterprise to affect entire industries, sectors and economies. It is no longer sufficient just to ensure the cybersecurity of your own enterprise; rather, cyber resilience demands that organizations work in concert[4].

Risk management and insurance have traditionally been seen as a cost center for the firm. It should be considered rather as an investment, since it heads off risks, losses, fraud, payment defaults, inefficiency, regulatory penalties, loss of image, etc. In short, it guarantees the firm's continuity and resilience.

The remainder of this paper is organized as follows. It starts with the brief overview of the ISO 31000 risk management standard and the ISO/IEC 27000 information security standard. The role of insurance in risk financing in these frameworks has been indicated. It is followed by the extensive cyber insurance description including subject and scope of insurance, main exclusions, cyber policy contracting and underwriting. The last section concludes.

4 *Principles for Board Governance of Cyber Risk*, Insight Report, World Economic Forum, March 2021, http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf [access: 27.11.2022].

The role of insurance in the ISO 31000 risk management framework

Risk is an inherent element of any business activity, and its complete avoidance is impossible and undesirable. The uncertainty of the outcomes of activities and the need to prevent the negative effects of threats and maximize opportunities increase the importance of risk management in modern organizations. Risk management allows for more efficient and effective conducting of business tasks and goals.

The implementation of a risk management program is related to the introduction of a comprehensive solution based on a systematic approach to the risk identification and description, data analysis, as well as evaluation and optimization of all risk groups to which the organization is exposed. The ISO 31000 standard is a globally recognized standard for risk management in an organization.

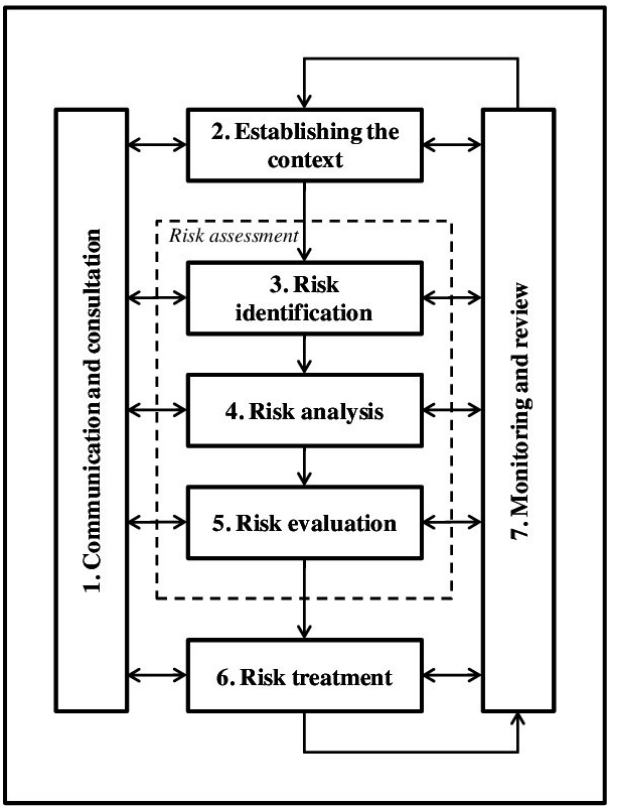
ISO 31000 is an international standard issued by ISO (International Organization for Standardization) and is intended to serve as a guide for the design, implementation and maintenance of risk management. Risk is involved in any activity of organizations of all types and sizes. ISO 31000 describes a systematic and logical process, during which organizations manage risk by identifying it, analyzing, and then evaluating whether the risk should be modified by risk treatment to satisfy their risk criteria. Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities. ISO 31000 provides principles and generic guidelines to assist organizations in establishing, implementing, operating, maintaining, and continually improving their risk management framework. It is not specific to any industry or sector, so it can be used by any public, private or community enterprise, association, group or individual.

ISO 31000 defines risk management as a set of coordinated activities to direct and control an organization regarding risk. According to George Rejda et al.: „risk management is a process that identifies loss exposures faced by an organization and selects the most appropriate technique for treating such

expenses”[5]. Risk management allows an organization to ensure that it knows and understands the risks it faces. It is a process that should be:

– an integral part of management,
– embedded in the culture and practices,
– tailored to the business processes of the organization.

The adoption of an effective risk management process within an organization will have numerous benefits.



Source: based on *ISO 31000:2018 – Risk management – Guidelines*, Geneva 2018.

Fig. 2. The process of risk management according to ISO 31000

5 G.E. Rejda, M.J. McNamara, W.H. Rabel, *Principles of Risk Management and Insurance*, Essex 2022, p. 68.

Risk management process comprises the following steps (see Fig. 2):

1) Communication and consultation: Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process;

2) Establishing the context: By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be considered when managing risk, and sets the scope and risk criteria for the remaining process;

3) Risk assessment: Risk assessment is the overall process of risk identification, analysis, and evaluation:

a) Risk identification: Through applying risk identification tools and techniques, the organization should identify risk sources, areas of impacts, events and causes, and their potential consequences,

b) Risk analysis: Risk analysis involves the development of understanding of the risk, consideration of the causes and risk sources, their positive and negative consequences, the likelihood that those consequences can occur, provides an input to risk evaluation and decision whether risks need to be treated, and on the most appropriate risk treatment strategies and methods,

c) Risk evaluation: The purpose of this step is to assist in decision making about which risks need treatment and priority for treatment implementation;

4) Risk treatment: Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementing and benefiting from these options;

5) Monitoring and review: Monitoring and review can be periodic or ad hoc and should be a planned part of the risk management process.

ISO 31000 lists several risk treatment methods that can be implemented to modify the risk. An appropriate risk treatment should be applied to reduce, remove, or retain each risk depending on a range of factors. An organization might choose to retain a risk if it is inevitable, unavoidable, or lies within the accepted risk tolerance level. Risk treatment methods that deal with negative consequences of risk include:

– risk avoidance – decision not to start or continue with the activity that gives rise to the risk; this strategy removes the source of risk;

– risk control – changing the likelihood or potential consequences of a risk by implementing technical or non-technical measures;

– risk retention – decision to retain the risk by informed decision;

– risk transfer – sharing or moving the risk (or its negative financial consequences) to another party, including insurance as a core risk financing method.

Risk treatment options are not necessarily mutually exclusive. They can be applied individually or in combination. Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, regarding legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. After the risk treatment implementation, residual risk remains which is a portion of inherent risk that is unavoidable or not handled.

Risk transfer reduces risk to an organization by passing the risk along to others. This can be accomplished contractually using hold harmless and indemnification clauses in leases and other contracts. But the most common risk transfer mechanism is buying insurance. Insurance, on which this chapter focuses, has become the primary tool for managing negative risks for individuals and businesses. It transfers the risk of financial losses arising from random events to an insurer. Insurance company is a professional risk carrier that collects individual risks, creates a portfolio of diversified risks and thus the aggregated risk can be spread over a larger group. Consequently, in exchange for a relatively small price (insurance premium) an insured is provided with a coverage (insurance compensation) against huge losses caused by random events. An insurance policy can cover multiple property, liability, and financial risks, including cyber risk.

The role of insurance in the ISO 27000 standard

Based on the ISO 31000 as a general framework, the ISO 27000 standard explains in detail how to conduct a risk assessment and a risk treatment (including insurance), within the context of information security.

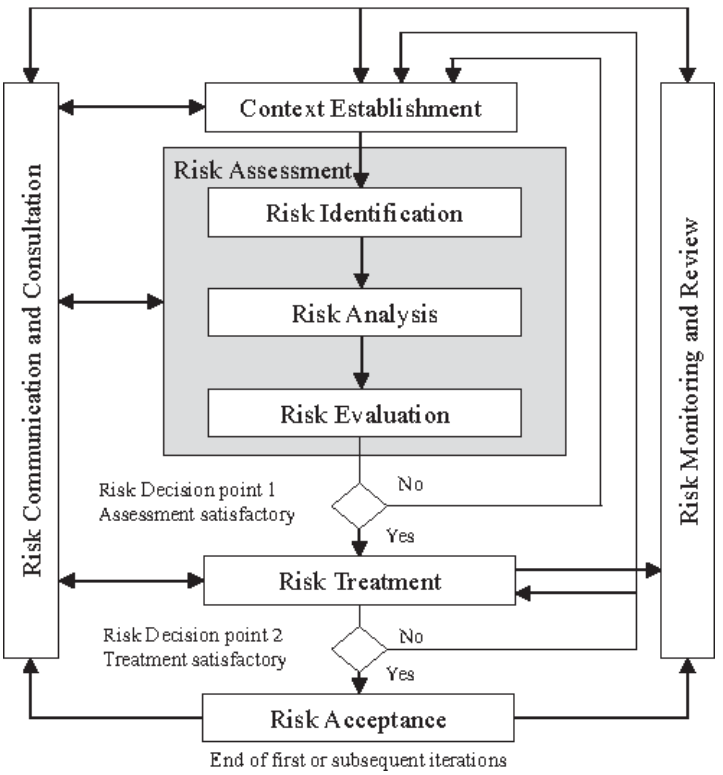
The ISO/IEC 27000 family of standards offers a holistic approach toward information security, protecting against vulnerabilities and incidents in information assets. With a set of proven best practices, it helps organizations improve their information security and minimize the risk of business disruptions.

Information security, as specified in ISO 27001, is critical in adding value to current quality systems in any organization, to identify and manage threats and vulnerabilities of prioritized information assets and to additionally increase

trust by the incorporation of interested parties. It also allows independent audits or reviews to be conducted in relation to those processes.

ISO/IEC 27000 specifies the requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a management system, as well as prepare, respond, and deal with the consequences of information security incidents.

The standard sets requirements for an Information Security Management System (ISMS) which should become a part of the overall management system. The ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: people, processes, and technology.



Source: V. Agrawal, *A Framework for the Information Classification in ISO 27005 Standard* [in:] *Proceedings of the IEEE 4th International Conference on Cyber Security and Cloud Computing, 26–28 June 2017*, New York 2017, p. 264–269.

Fig. 3. The ISO/IEC 27005 risk management framework

The ISO/IEC 27005 risk management framework in its process approach is comprised of several main blocks: Establishing Context, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Risk Acceptance, Risk Communication and Risk Monitoring & Review. Furthermore, each block is broken down into several subdomains and elements. This results in 35 subdomains and 82 elements in total.

General idea of the ISO/IEC 27005 risk management framework is like the well-established ISO 31000 standard. Some differences that occur are caused by the specific nature of the risk subject, namely information assets. At the risk identification stage, an organization should focus on the following areas of activities:

1) Identification of assets – locate every piece of information hold by an organization and determine whether it is a „primary" or „supporting" asset. Primary assets are information or business processes, and supporting assets are related IT systems, infrastructure, and people resources. Organizations are required to identify primary assets and supporting assets that could have an impact on the primary asset, typically giving details about asset ownership, location, and function;

2) Identification of threats – threats should be continuously monitored to consider new and emerging ones;

3) Identification of vulnerabilities – any weaknesses in technology, people (human error, malicious action, social engineering, etc.) and processes of an organization need to be identified;

4) Identification of existing controls – contrary to other risk assessment methodologies, an ISO 27005 risk assessment requires an organization to identify all its existing controls and to consider the protection provided by these controls before applying any new ones.

The information gathered about assets, vulnerabilities and threats in an organization should be used to prioritize the biggest risks. To do that, a risk assessment phase must be performed to quantify the organization's risk exposure in terms of probability and potential impact of an incident. The level of a particular risk is a product of the probability of a threat exploiting vulnerability and total impact of the vulnerability being exploited. Based on this classical formula, there are several specific cyber risk assessment methodologies such as OCTAVE, CORAS, MEHARI, ISRAM, etc.

If the level of risk exceeds an organization's risk tolerance, appropriate risk treatment techniques must be applied:

– Risk avoidance – ceasing any activity that creates the risk. This strategy is advisable if the risk is too big to manage it with security controls;

– Risk control – application of cyber security measures to reduce the probability of occurrence or mitigate the severity of potential damage resulting from a cyber incident;

– Risk retention – objective risk acceptance in accordance with the organization's policies, usually accompanied by the preparation of adequate financial provisions (risk capital);

– Risk transfer – transfer of risk to a third party by outsourcing the cyber security efforts to another organization or by purchasing cyber insurance to ensure appropriate compensation in the event of a cyber incident.

Moreover, cyber insurance can be also applied to cover a residual risk. It is a risk that remains after the risk treatment methods are applied and some portion of risk still exist. Residual risk can be retained or transferred to an insurance company. In this case, cyber insurance acts as a complement solution to baseline cyber risk mitigation techniques. Cyber policy ensures compliance not only with ISO/IEC 27000 guidelines, but also with the EU General Data Protection Regulation (GDPR) where a ISO/IEC 27000 based approach is recommended.

Description of cyber insurance

The presence of cyber insurance in the ISO 31000 and ISO/IEC 27000 standards indicates its relevance in a risk management process. The role of cyber insurance is to complement, not replace, technical and organizational cybersecurity solutions. In many cases, cyber insurance is used to protect against a residual risk, i.e. a risk that could not be eliminated by other solutions. As Latham and Watkins (2014) expressed it smartly, „when technology fails and IT security is breached, cyber insurance will be the last line of defense against suffering severe financial losses from a successful hacker attack"[6].

There are two main types of cyber insurance on the market. The first one is a specialized coverage known as stand-alone cyber policy. The second option is to extend the scope of coverage of classical non-life insurance policies (e.g.

6 D. Latham, P.R. Watkins, *Cyber Insurance: A Last Line of Defense When Technology Fails*, „White Paper" 2014, no. 1675.

property, general liability, professional liability and D&O lines) by including additional clauses (so called endorsements). The latter solution is popular in countries where specialist cyber insurance is still gaining the interest of buyers and their needs are not yet sufficiently formed. In this way, the lower willingness to buy this relatively expensive and complicated product can be overcome. The use of endorsements is also supported by the difficulty in distinguishing cyber risk from other insurance risks. Further, this chapter focuses on the stand-alone contracts as they are the key solution on the global insurance market.

The insurers' offer is addressed primarily to enterprises of all sizes, non-financial organizations and public institutions. The target industries are: e-commerce, manufacturing and trading companies, transportation, accommodation and catering, financial institutions, construction industry, professional services, health care and education. Being aware of the above-average level of risk and specific insurance needs, insurance companies exclude software producers, Internet providers, IT equipment manufacturers, data processing centers, electronic payment operators and entities related to social media.

Subject and scope of cyber insurance

Cyber insurance is a package policy, combining the elements of property insurance, liability insurance, financial insurance, and assistance insurance. It's worth to emphasize the unusual subject of insurance, namely intangible assets, which is a challenge when estimating the value of damage and amount of insurance compensation.

The scope of insurance may include the following components:

1) cyber liability insurance;
2) coverage of administrative penalties for breach of privacy;
3) electronic data protection;
4) cyber-related business interruption insurance;
5) cyber extortion insurance;
6) coverage of extra expenses related to a cyber incident.

In the first group, insurance policy covers random events which may result in the insured's third party liability. These include in particular:

– Liability for privacy breach. In most cases, this is the basic coverage to which a policyholder may add other elements of coverage. It includes liability for violation of the personal data protection law or other regulations on

privacy rights, consisting in unauthorized disclosure of personal data by the insured, defamation or unlawful use of the image;

– Liability for breach of data confidentiality. In the event of an act, error or omission of the insured leading to a breach of the confidentiality of data (other than personal data), the insurance company will pay compensation to the injured third party for the resulting damage. The condition for recognizing the claim is the occurrence of the strictly defined effect of failure to ensure confidentiality, which is the disclosure of data, no access to data for authorized persons, theft of computer hardware, loss or damage to third party data stored in the insured's IT system or infection with malware by the insured computer system of the victim;

– Liability for breach of network security. Insurance covers the actions or omissions of the insured in ensuring the security and proper operation of the IT system. The breach may consist, inter alia, in failure to provide protection against unauthorized access to the system or failure to prevent the transmission of malicious code (malware) from the insured party to a third party's system;

– Liability resulting from multimedia activities. Claims of third parties arising from multimedia activity of an insured, understood as the public sharing of texts, images, digital code, audio-video materials via e-mail, website or social media, if as a result of this activity there was defamation, plagiarism, violation of the privacy right, copyright, the right to own things or to be unfairly accused;

– Liability for administrative trials and penalties of third parties. Insurance covers events where as a result of a computer attack on a third party and leakage of personal data, caused by the insured, administrative proceedings were brought by the regulatory authority and administrative penalties were imposed on the third party or the obligation to notify the aggrieved about the leakage of their data;

– Liability for violating the security of electronic payments. Covers claims of the e-payment service provider against the insured alleging an inadvertent breach of the Payment Card Industry Data Security Standard (PCI DSS) that the insured is obliged to comply with (this applies to points of sale, banks, payment service providers).

In each of the above cases, an insurer additionally covers the costs of defense in civil law proceedings, such as the costs of legal advice and legal representation.

Coverage of administrative fines & penalties for privacy breach is another component of the insurance. It covers penalties and fines imposed on the insured by regulatory and administrative authorities as a direct result of an insured event, such as leakage of personal data. In the light of the GDPR, this is an incident threatened with high financial administrative penalties imposed by regulators. The insurer will cover the value of penalties and fines, plus legal costs in administrative proceedings.

The third component of the cyber insurance package is electronic data protection. The subject of insurance is electronic data understood as digital information located in a specific territory (Poland, the European Union, the whole world) processed outside the RAM memory of a computer. This means that you can insure data stored in data files, operating systems, software, applications produced in series or on an individual order. In the event of data loss or damage as a result of a cyber-attack, the insurer will cover the costs of: data restoration, data access restoration, new software purchase or malware removal. A special case of electronic data insurance, requiring the extension of the scope of protection by an additional contractual clause, is data stored in a computing cloud. This increasingly popular web service relies on an external company to provide remote digital resources, such as server computing power, disk space for data storage, licensed applications and resource administration services.

Insurance of business interruption resulting from cyber incident (i.e. cyber business interruption, CBI) is the most desirable component of package cyber insurance by entrepreneurs. This is due to the huge dependence of the business sector on IT systems and network communication, and the fact that any disruption in this area brings monetary losses for company's revenues. If cyber-attack has occurred, the CBI policy covers the loss of gross profit and increased operating costs incurred by the insured during the disruption or interruption in business within a 3-6 month period. The insurance compensation covers the decrease in gross profit, understood as the difference between the lost earnings and the variable costs not incurred due to the disruption. The victim additionally receives compensation for additional expenses incurred to mitigate the decline in turnover if they are economically justified. It is essential that the cause of the business interruption is in relation with cybersecurity. As a rule, the insurer is not responsible for the first 12–48 hours of a disruption (so-called waiting period).

Another section of cyber insurance relates to the so-called cyber extortion, i.e. targeting the insured with a credible threat to launch a hostile

computer attack and demanding a ransom for withdrawing from the attack. The threat of a cybercriminal may concern infection with malware, cutting off access to the Internet, destruction or damage to elements of the IT system, misuse of confidential data illegally intercepted from the insured. In this situation, the insurance company may cover the cost of ransom. The purchase of cyber extortion insurance must be kept secret in order not to incentivize cybercriminals.

The scope of a typical cyber insurance is often supplemented by a section that covers the costs of an extensive catalog of additional services related to the occurrence of an insured event. These are, among others: computer forensics (to determine the cause, perpetrators, and size of an incident), notification of data breach, hiring a call center, monitoring the effects of identity theft, including monitoring financial transactions, crisis management, public relations services to protect reputation, legal advice.

The scope of cyber coverage is limited by exclusions. There are many different policy wordings with a long list of exclusions. But still, it is possible to point out typical exclusions that appear in almost every cyber policy. These are as follows:

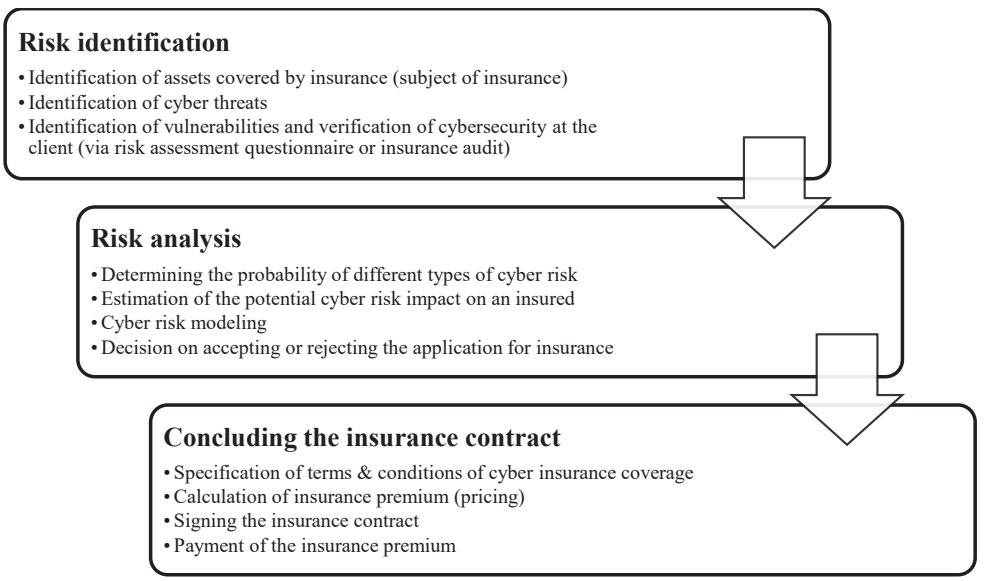
- patent, software, and copywright infringement;
- wars and invasions;
- lack of cyber security measures;
- personal injuries and damages;
- loss of electronic device;
- government entity or public authority;
- specific network interruption.

The cyber insurance market is characterized by a significant variety of terms of coverage and insured limits. The lack of standardization results from the immaturity of this insurance line, the multitude of insurance companies trying to develop a new market niche and distinguish it from competitors, as well as the individualization of insurance solutions in individual market segments. The clearest differences are visible between the insurance offer addressed to large corporations and the offer for small and medium-sized enterprises (SMEs). Specialized solutions with individual risk assessment, higher liability limits and a wider scope of protection are addressed to large enterprises. Entities in this segment usually invest more in advanced ICT security systems, while SMEs more often use outsourcing of IT infrastructure and cybersecurity services, and in many cases they limit themselves to ensuring only minimum standards of cyber protection. Therefore, insurers are targeting SMEs with an offer of

cyber insurance built into a larger package of small business property and liability insurance. It is a cheaper solution with a narrower scope of protection, a more extensive list of exclusions and lower liability limits, with no greater possibility of modifying the insurance conditions. On the other hand, the diversification of the product offer depending on the industry of the client's activity is rare in the current market. Only a few insurance companies, usually associated with London-based Lloyds, have an offer for specialized entities in their portfolio, such as software producers, data centers, network service providers, electronic payment operators.

Process of issuing cyber insurance contract

In cyber insurance, the process of concluding a contract, providing protection and claims handling go beyond the framework of the classic insurance paradigm. The intensity of relationship between the parties of insurance relationship is much greater. It is shown on Figure 4 depicting the process of concluding a cyber insurance contract.



Source: own work.

Fig. 4. The process of concluding a cyber insurance contract

At the underwriting stage, the insurer commissions an external company to diagnose the client's cybersecurity, identifying areas that require improvement. It results in recommendations, the implementation of which will improve the customer's cybersecurity, and thus meet the minimum requirements of the insurer or obtain discounts in the insurance premium. However, after identifying a cyber incident, it is important to accurately assess the situation and react quickly. Insurance companies are actively involved at the early stage of claim settlement, organizing and financing access to professional forensics, intrusion analysis, patching vulnerabilities, crisis management, public relations, and legal assistance. Considering the high cost of such services and their limited availability, it is evident that the policyholder receives not only insurance coverage, but also a significant added value in the form of insurance-related services.

Cyber insurance underwriting and pricing

All activities performed to assess and accept under appropriate conditions or reject an insurance risk are called underwriting. In cyber insurance underwriting, the key issue is to assess the policyholder's preventive actions and to identify the state of cybersecurity. In the underwriting process, insurance companies obtain various information from the insured. There are three stages at which the data on cyber risk are required.

1) Underwriting stage – insurers collect data to decide whether to conclude an insurance contract and to determine insurance premium. These are typical data characterizing an organization: annual revenue, size of employment, industry sector, subject of activity, number of processed data records. Information on the state of IT security implemented in an organization is equally important when assessing the risk. The presence of CISO (Chief Information Security Officer), employee trainings in cybersecurity, IT security technologies used (antiviruses, firewalls, application update frequency), dependence on subcontractors – these are examples of factors proving the level of an organization's cybersecurity culture, awareness of cyber threats and possible consequences implementation of cyber risk.

2) After a policy issuance and before its renewal. At this stage, insurers obtain very little information from their clients. The area of interest includes all kinds of cyber incidents that took place during the insurance period, as well as significant business events, such as mergers and acquisitions or a change in the business profile. Information about the actions taken after an incident to

remove vulnerabilities and security gaps are particularly valuable. The speed and scope of security improvements can be an important indicator of the organization's culture and its approach to cybersecurity.

3) After a cyber incident stage. In the event of an incident, insurers obtain a significant amount of information for the purpose of claim settlement and determining the insurer's liability. The scope of the data corresponds to the risk questionnaire completed before the conclusion of the insurance contract, which serves to verify the accuracy of the data and its compliance with reality. In addition, the insured reports in detail what steps have been taken in relation to the incident. Great importance is also attached to the quickest possible evaluation of the damage.

The methodology of cyber risk pricing has not been standardized. There are three main approaches to cyber insurance premium determination:

– system of a fixed rate (flat rate) – insurance premium is the same for all insured and corresponds to the sum insured and deductible provided in advance;

– system of differentiated base rates modified with selected risk factors – insurance premium depends on the base rate applied and additional risk factors that modify the base rate; the base rate reflects some parameters of an insured (annual revenue, total assets, size of employment);

– system of individualized rates – based on the risk assessment of the insured, in particular information security and cyber security culture; the insurance premium reflects the individual risk exposure of an insured (so it's called „fair premium"); it's the most advanced pricing system which requires a huge amount of input data.

The degree of premium differentiation in cyber insurance for different customer groups is lower than in traditional corporate insurance lines. It is caused by immaturity of the market. Factors that influence the most the cost of cyber insurance are:

– company size – measured by the number of employees or annual revenue; company size influences the risk of phishing or social engineering attacks;

– industry sector – it is related to the needs and costs of cybersecurity, it is also indirectly related to the type and number of data processed by the company;

– volume and type of processed data – low-risk companies, such as local businesses with a limited number of customers, will pay less premium for

their cyber insurance than, for example, a retail store that receives and stores customer credit card numbers;

– annual revenue – the higher the company's revenue, the more likely it is to be a victim of cybercriminals;

– level of cybersecurity – a high level of IT security reduces the insurance premium;

– conditions of insurance cover – the sum insured, deductibles, scope of coverage and insurance limits have direct impact on the amount of insurance premium.

Although cyber insurance is mostly a stand-alone policy, it is expected that soon a significant part of insurance lines will contain a portion of cyber risk. Meanwhile, the rapid pace of technological changes, the expansion of Internet of Things, more and more perfect methods of hacker attacks – increase the potential and complexity of the risk that insurers will have to face. In this situation, insurers require current and future policyholders to adapt to the minimum requirements of IT security, a kind of „cyber hygiene" and improve the cybersecurity policy in accordance with recognized international standards (e.g. ISO 27000). In this way, insurers play the role of a quasi-regulator. The degree of involvement of the insurance industry in this mission is growing to such an extent that we can even speak of „regulatory outsourcing"[7].

Conclusion

Hacker attacks and cyber incidents that affect the confidentiality, availability and integrity of data and IT systems are an inherent part of the digital economy. The rapid evolution of the cyber threat landscape, combined with the dependence of critical infrastructure and industry on interconnected technologies, may result in a further increase in the number of cyber incidents. In particular, those that result in physical damage to property and bodily injury. In response, the cyber insurance market has grown significantly but providing insurance coverage for so many different types of cyber risk is a major challenge.

7 G. Strupczewski, *Rola państwa w rozwoju rynku ubezpieczeń cybernetycznych*, Kraków 2020.

Cyber insurance enhances resilience against cyber threats and cyber security capabilities of an organization. Cyber insurance is an increasingly important weapon in the risk management arsenal of today's enterprises. Unknown just a decade ago, these popular policies now offer organizations a crucial hedge against risks that defy routine assessment, planning and mitigation tactics. The explosive growth of ransomware, along with sophisticated, well-funded attacks leveraging critical zero-day exploits has made insurance a must-have element of any mature cyber risk management strategy.

Bibliography

Agrawal V., *A Framework for the Information Classification in ISO 27005 Standard* [in:] *Proceedings of the IEEE 4th International Conference on Cyber Security and Cloud Computing, 26–28 June 2017*, New York 2017.

Cyber risk. The emerging cyber threat to industrial control systems, Report by Lloyd's & Guy Carpenter, https://assets.lloyds.com/media/542bea95-0d28-4ce1-a603-63db54aa24f9/The%20Emerging%20Cyber%20Threat%20to%20Industrial%20Control%20Systems_Final%2016.02.2021.pdf [access: 4.12.2022].

Global Risks Report 2021, World Economic Forum, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf [access: 23.11.2022].

ISO 31000:2018 – Risk management – Guidelines, Geneva 2018.

Latham D., Watkins P.R., *Cyber Insurance: A Last Line of Defense When Technology Fails*, „White Paper" 2014, no. 1675.

Principles for Board Governance of Cyber Risk. Insight Report, World Economic Forum, March 2021, http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf [access: 27.11.2022].

Rejda G.E., McNamara M.J., Rabel W.H., *Principles of Risk Management and Insurance*, Essex 2022.

Strupczewski G., *Rola państwa w rozwoju rynku ubezpieczeń cybernetycznych*, Kraków 2020.

Koncepcja ubezpieczenia cybernetycznego i jego rola w procesie zarządzania ryzykiem zgodnym z normami ISO z punktu widzenia przedsiębiorstw przemysłowych

Streszczenie

W obliczu eskalacji zagrożeń cybernetycznych ubezpieczenie ryzyk cybernetycznych staje się rozwiązaniem, które może uzupełniać tradycyjne narzędzia cyberbezpieczeństwa wykorzystujące instrumenty techniczne i organizacyjne. Co więcej, uznane standardy zarządzania ryzykiem takie jak ISO 31000 i ISO 27000 wskazują ubezpieczeniom cybernetycznym istotną rolę do odegrania w obszarze finansowania negatywnych skutków realizacji ryzyka cybernetycznego. W związku z tym celem artykułu jest przedstawienie koncepcji ubezpieczenia ryzyk cybernetycznych i podstawowych jego parametrów takich, jak: zakres ochrony, obszary zastosowań, zasady oceny ryzyka i kalkulacji wysokości składki ubezpieczeniowej. Analizę przeprowadzono z punktu widzenia przedsiębiorstw

przemysłowych, które w wielu przypadkach stanowią element infrastruktury krytycznej państwa. Zagraża im nie tylko czyste ryzyko cybernetyczne, lecz także ryzyko cyberfizyczne, co oznacza szczególnie dużą dotkliwość potencjalnych strat. Niniejsza praca ma znaczenie aplikacyjne w kontekście wymagań nowej dyrektywy NIS 2.

Słowa kluczowe: cyberbezpieczeństwo, ubezpieczenie ryzyk cybernetycznych, zarządzanie ryzykiem, ISO 27000, ISO 31000