ALEKSANDRA HĘĆKA-SADOWSKA
KRZYSZTOF ŁYSKAWA
https://doi.org/10.33995/wu2023.2.3
data wpływu: 26.04.2023
data akceptacji: 06.07.2023

Operational Cyber Risk in the differing business model of Insurance Companies: the example of Poland

Cybersecurity has become one of the greatest challenges in today's post pandemic, digital and interconnected world, and also a subject of strategic importance for the insurance industry. There is no doubt that the advance of technology and the increased use of big data and cloud computing have set up an opportunity for insurance business, but they also expanded insurance companies' vulnerabilities towards cyber risk. As insurers collect a large amount of confidential data, including protected personal sensitive information, they are a natural target for cyber-attacks. On the one hand, the aim of the article is to indicate how the risks associated with digitalisation affect the day-to-day operations in selected business areas of an insurance company, and which methods may be used to manage them, on the other. After a general review of cyber risk based on recent branch reports and survey results, the authors identified its global economic impact with particular regard to financial institutions, and also insurers' exposure and perception of cyber risk and cybersecurity spending. Moreover, administrative decisions issued by the President of the Personal Data Protection Office in Poland, selected jurisdictions and loss scenarios for insurance companies were examined with a deeper dive into underwriting, selling, administration and claims handling processes. The results of the literature study show that cyber risk is recognized to be one of the most significant non-financial risks (in terms of the source, not result of the risk) for insurers and that many proactive security measures can be implemented. However, due to the high vulnerability to leaks of confidential personal and financial data or unauthorized system access, which may cause not only financial loss, but also business interruptions and reputational damage, in the authors' opinion, loss prevention and reduction are insufficient. Thus, both insurance and non-insurance methods of external financing cyber risk results were indicated. On this basis, the cyber insurance

is considered by the authors to be the best tool providing both prevention and financial compensation in case of cyber incidents, also in insurance companies.

Keywords: cyber risk, operational risk, insurance company, risk management, cyber insurance

Introduction

The need for a safe and secure cyberspace has become more important than ever, especially as we face the 4th Industrial Revolution, which has been taking place since the start of the 21st century. As cyber/security incidents and data breaches continue to grow for companies and institutions, it is no longer a question of 'if' it will happen, but rather 'when'. Thus, cybersecurity, pushed by the pandemic, has entered the leadership agenda. Many surveys have revealed that cyber risk is a top-ranked business risk which concerns companies in Europe and around the world (based on reports: Allianz[1]; FERMA[2]; PWC[3]; World Economic Forum[4]). Strupczewski[5] provided a literature review of the definitions of cyber risk and proposed his own one, which focuses on one of the most relevant features of cyber risk, i.e. its place among operational risks. This approach was initiated by Cebula and Young[6] who define operational cybersecurity risks as: 'operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems'. Cyber risks are also considered as a top global risk for the financial sector[7,8,9]). As studies have shown, despite the fact that financial sector has a high cybersecurity maturity level and continues to spend more on cybersecurity programs[10],

1. *Allianz Risk Barometer 2022*, Allianz Global Corporate & Specialty 2022, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (30.08.2022), p. 10.
2. *FERMA European Risk Manager Survey Report*, FERMA 2022, https://www.ferma.eu/publication/european-risk-manager-report-2022/ (29.08.2022), p. 5 and pp. 20–22.
3. *2022 Global Risk Survey Report*. Embracing risk in the face of disruption, PwC 2022, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-risk-survey.html (06.07.2022), p. 2.
4. *The Global Risks Report 2022. 17th Edition.* Insight Report, World Economic Forum, Cologny/Geneva 2022, https://www.weforum.org/reports/global-risks-report-2022/ (29.08.2022), p. 25.
5. Strupczewski G., *Defining Cyber Risk,* "Safety Science", 2021, vol. 135, DOI: 10.1016/j.ssci.2020.105143, p. 6.
6. Cebula J. J. & Young J. J., *A taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN-028*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh 2010, https://www.semanticscholar.org/paper/A-Taxonomy-of-Operational-Cyber-Security-Risks-Cebula-Young/1e752a86215430f4dc59468ebf96df40fcb83b10 (07.07.2022), p. 1.
7. Curti F., Gerlach J., Kazinnik S., Lee M. & Mihov A., *Cyber risk definition and classification for financial risk management,* "Journal of Operational Risk", 2023, vol. 18, no 2, DOI: 10.21314/JOP.2022.036, p. 37.
8. Bouveret A., *Estimations of losses due to cyber risk for financial institution*, "Journal of Operational Risk", 2019, vol. 14, no 2, DOI: 10.21314/JOP.2019.224, p. 1–2.
9. *Allianz Risk Barometer Results appendix 2022*, Allianz Global Corporate & Specialty 2022, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (30.08.2022), p. 35.
10. *Financial Cyber Survey*, Deloitte 2021, https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/finance/FSI_cyber_finish_V5.pdf (02.09.2022), p. 7.

it is one of the top-attacked industry[11],[12] and the second-highest cost of a data breach industry when compared to other sectors[13]. However, it should also be pointed out that redesigning existing systems requires a lot of resources, and the insurance industry is identified as the one with the highest costs[14].

Cyber risk in the insurance industry can exist in two areas: as part of underwriting risk and as part of insurer's own operational risk. Based on research on risk factors and their evolution, those related to operational risk became extremely important in the current risk management in insurance companies[15]. Thus, this paper focuses on operational cyber risk in insurance companies, where extending reliance on digital solutions has also expanded the landscape of opportunities for cyber attackers. Due to the fact that insurers collect and handle vast amounts of information about their policyholders and insured persons, including personally identifiable information, this industry is a target for cybercriminals. After reviewing recent branch, benchmark reports and surveys about cybersecurity and cyber incidents (published both by business advisors and companies from the information technologies and information communication technologies (IT/ICT) sector), with particular regard to financial institutions, the authors examine the impact of this phenomenon on the global economy. The authors investigate administrative decisions issued by the President of the Polish Personal Data Protection Office (PDPO) taking a deeper dive into the four particular areas of its activity (sales, underwriting, policy processing and loss adjustment) and also provide a scenario of cyber incidents in insurance companies, and selected Polish jurisdictions in that field. As an institution of public trust, which creates and maintains trust relationships with its customers, it is a key challenge for the insurance industry to find a solution to cyber threats. The objective of this paper is to examine cyber risk in an insurance company and indicate cyber insurance as a method of external financing for its realization. Alternative risk transfer (ART)-related solutions such as securitization mentioned in the paper might be viewed as ongoing questions that require further research.

The paper is organized as follows. The research methodology is described in Section 1. Section 2 provides an overview of the economic impact of cyber incidents on financial institutions. Section 3 discusses cyber threats to insurance companies and Section 4 shows prevention and reduction methods of management cyber risk taken by insurers. In Section 5 external financing methods for handling own operational cyber risks in insurance company were described. The final Section summarizes and gives concluding remarks.

11. X-Force Threat Intelligence Index 2022 Full report, IBM, IBM Corporation, New York 2022, https://www.ibm.com/security/data-breach/threat-intelligence/ (17.08.2022), p. 42.
12. *Data Breach Investigations Report*. Verizon 2022, https://www.verizon.com/business/resources/reports/dbir/ (26.07.2022), p. 50.
13. *Cost of Data Breach Report 2022*, IBM, IBM Corporation, New York 2022, https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf (30.08.2022), p. 11.
14. Tsakalidis G., Nousias N. & Vergidis K., *Towards a Fitting Representation Method for Redesign Evaluation and Cost-Based Optimization*, Operational Research in the Era of Digital Transformation and Business Analytics. BALCOR 2020. Springer Proceedings in Business and Economics, Cham 2020, p. 33.
15. Wang Y., Li B., Li G., Zhu X. & Li J., *Risk factors identification and evolution analysis from textual risk disclosures for insurance industry*, "Procedia Computer Science", vol. 162, 2019, p. 31.

1. Methodology

While creating the methodological basis for this paper, we used the method of analysis as one of three methods of explanation in science. It consists of a set of actions considering the elementary features of the object or phenomenon aimed at discovering and exploring constitutive or conditioning factors or the regularity of relationships, and defining the indicated reality[16]. In the issue considered below, the basis for such action is content analysis, in which both external and internal techniques are used. The first one consists of describing sources, which means establishing who is an author and an audience, when, in which conditions and what this text was created for. These findings lead to identifying facts, ideas and purpose in the context of research carried out. A key element of content analysis, during which an analytical and comparative method is used, is an internal criticism, which includes interpretation, explanation and valuation of the text[17].

Therefore, the paper uses current studies and reports on the perception and management of cyber risk. One of the key outcomes of analysis in science is prediction. Therefore, through arguments arising from the laws and initial conditions and descriptions of the expected effects of events in the area of cybersecurity in financial institutions, we search for the existence of a logical symmetry between explaining and predicting. The content analysis is supplemented with a synthesis consisting of a comprehensive approach to the subject of the research and setting recommendations for further activities of insurance companies in this area. Using an inductive reasoning ('from the detail to the whole'), i.e., from the veracity of the observations and analyses carried out in the field of operational risk and the insurance companies' activities, an attempt was made to build true conclusions with regard to the entire operations of insurance companies in the area of cybersecurity. The above was carried out primarily in the summary.

2. The economic impact of cyber incidents in financial institutions

The economic impact of cyber incidents is significant and has become a major issue in recent years. Since then, the seriousness and financial costs of cyberattacks, as far as they can be estimated, have continued to rise. Cybersecurity Ventures' projection shows that cybercrime[18] will cost the global economy USD 10.5 trillion annually by 2025 (up from an estimated USD 3 trillion in 2015)[19], compared to predicted by International Monetary Fund global Gross Domestic Product

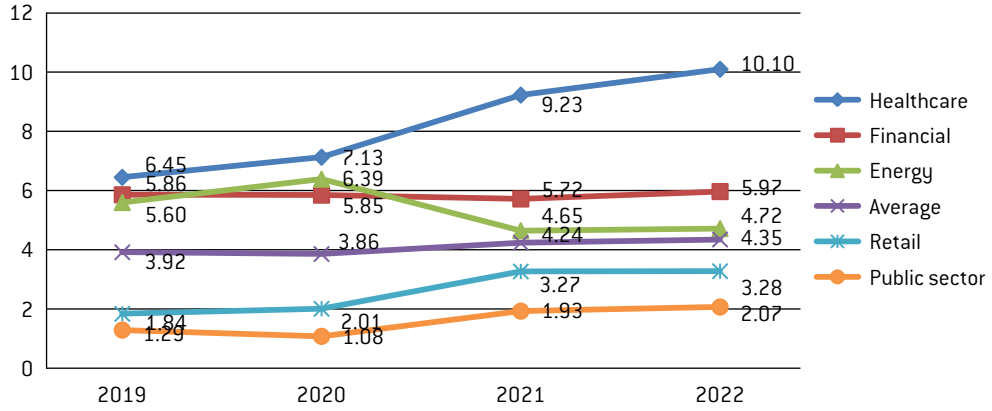
16. Kamiński S., *Jak filozofować. Studia z metodologii filozofii klasycznej*. TN KUL, Lublin 1989, pp. 158–159.
17. Kamiński S., *Analiza*. w: *Encyklopedia katolicka t. 1*, red. F. Gryglewicz, R. Łukaszyk, Z. Sułowski, TN KUL, Lublin 1989, pp. 484–485.
18. As stayed in the definition: "cybercrime cost include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm" (Morgan S., *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, 2020, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (01.09.2022)).
19. Morgan S., *2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/ (01.09.2022).

(GDP) of USD 123.3 trillion in 2025[20]. As claimed by Cybersecurity Ventures, global spending on cybersecurity will increase to USD 1.75 trillion cumulatively for the five-year period from 2021 to 2025[21]. The Cost of Data Breach Report has revealed that the global average total cost of a data breach[22] in 2022 was USD 4.35 million (the highest in the history of that research), which is a 2.6% raise from USD 4.24 million in 2021. At the same time, the global per record cost of a data breach grew by 1.9% (from USD 161 to USD 164)[23]. Further study shows that breaking down into four categories of data breach costs, the largest share (33.1%) in 2022 was detection and escalation (an increase of 16.1% from 2021). Dropping from first to second place for the first time in at least 6 years (a decrease of 10.7% from 2021), costs related to lost business still remained a large share (32.6%). Notification and post breach response costs shares in 2022 are similar to previous year and stand at 7.1% and 27.2% respectively[24]. Based on the survey, 83% of organizations have become victims of more than one data breach and 60% of respondents admitted that the cost of data breach was passed on to customers by increasing the price of products or services[25].

Cyber incidents have a different impact on various economic sectors (Figure 1). The average total cost of a breach in healthcare, which is subject to one of the most rigorous regulatory requirements and considered critical infrastructure both by the US government and by other countries, e.g. within the European Union, increased more than a half (from USD 6.45 million to USD 10.10 million) during the period observed.

20. *World Economic Outlook Database*, International Monetary Fund, 2022, https://www.imf.org/en/Publications/WEO/weo-database/2022/April (28.08.2022).
21. Morgan S., 2022, *op. cit.*
22. As explained in the research methodology, this research used an accounting method called activity-based costing, which identifies activities and assigns a cost according to actual use. Thus, the average cost of a data breach consists of four process-related activities associated with organization's data breach: 1) detection and escalation (e.g. forensic and investigative activities, assessment and audit services, crisis management, communications to executives and boards), 2) notification (e.g. emails, letters, outbound calls or general notice to data subjects, determination of regulatory requirements, communication with regulators, engagement of outside experts), 3) post breach response (e.g. help desk and inbound communications, credit monitoring and identity protection services, issuing new accounts or credit cards, legal expenditures, product discounts, regulatory fines), 4) lost business (e.g. business disruption and revenue losses from system downtime, cost of losing customers and acquiring new customers, reputation losses and diminished goodwill) (*Cost* ..., IBM, 2022, *op. cit.*, p. 54).
23. *Cost* ..., IBM, 2022, *op. cit.*, p. 9.
24. Ibidem, p. 12.
25. Ibidem, p. 4.

Figure 1. Average total cost of a data breach by selected industry worldwide (in USD million)



Source: Own work based on IBM Reports: 2019[26], 2021[27], 2022[28].

Figure 1 also presents the financial sector as the second most costly industry in recent years (except for 2020, when it dropped one place to third) with the average total cost of a breach almost unchanged. More highly regulated industries such as healthcare, financial, and energy industries experienced an average total cost of a data breach significantly higher than less regulated industries. Whereas lower costs of a data breach experienced by public sector are explained by low probability to loss of customers in case of a data breach[29]. Based on another study about economic crime and fraud, cybercrime is the second-biggest type of fraud experienced in the financial sector[30]. Financial institutions are exposed to a larger number of cyberattacks not only because they hold and share a robust amount of sensitive data and conduct many types of financial transactions but are also dependent on highly interconnected networks and critical infrastructures. Referring to Frey and Osborne[31], who have examined computerization's impact on future labour market, most of the jobs related to management, business and finance, where a high degree of social intelligence in generalist tasks is required, are not very susceptible to automation. However, there are a lot of jobs referring to finance and insurance precisely, which are in the high risk category (Table 1). This means that, for example, insurance or credit specialists, which are jobs at risk, are expected to be affected by emerging technology and with high probability could be automated.

26. *Cost of Data Breach Report 2019*, IBM, IBM Corporation, New York 2019, https://www.ibm.com/downloads/cas/RDEQK07R (31.08.2022), p. 26.
27. *Cost of Data Breach Report 2021*, IBM, IBM Corporation, New York 2021, https://www.ibm.com/pl-pl/security/data-breach (27.04.2022), p. 15.
28. *Cost* ..., IBM, 2022, *op. cit.*, p. 11.
29. *Cost* ..., IBM, 2019, *op. cit.*, p. 26.
30. *PwC's Global Economic Crime and Fraud Survey 2022*, PwC 2022, https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (30.08.2022), p. 6.
31. Frey C.B. & Osborne M.A., *The future of employment: How susceptible are jobs to computerisation?* "Technological forecasting and social change", 2017, vol. 114, pp. 254–280.

Table 1. Significant impact on business functioning (automation)

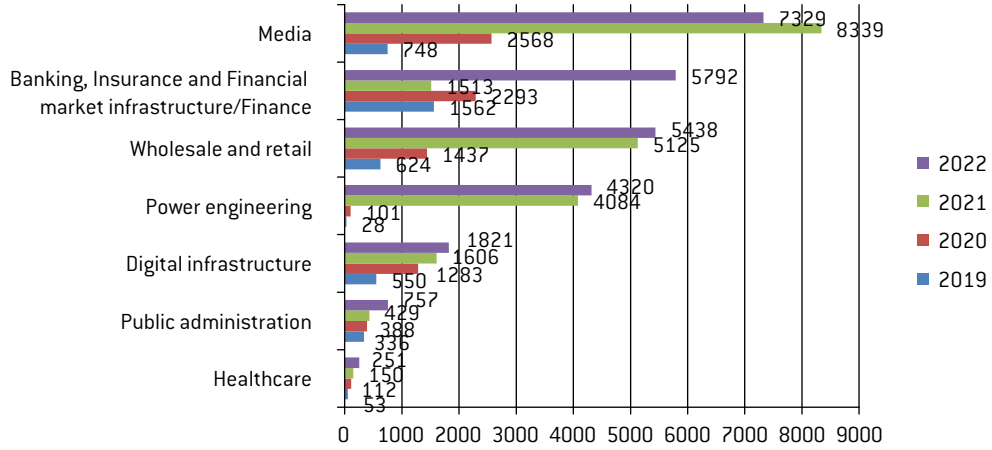
Profession	Rank	Tendency to automate
Insurance expert (underwriters)	5	99%
New Accounts Clerks	9	99%
Employee responsible for receiving damage / policy processing	14	98%
Loan Officers	17	98%
Tellers	20	98%
Appraiser (car damage)	18	98%
Credit Analysts	26	98%
Claims Adjusters, Examiners, and Investigators	28	98%
Credit Authorizers, Checkers, and Clerks	36	97%
Insurance salesman	138	92%

Source: own work based on: Frey C.B. & Osborne M.A., The future, *op. cit.*, pp. 254–280.

As this industry moves towards digital transformation (especially due to the pandemic, which has fast-forwarded digital transformation in the financial sector), the connection points for a breach increase. As reported by BAE Systems in their 2021 COVID Crime Index, the pandemic led to a rise in cybercrime and fraud in the financial sector; almost three-quarters of those surveyed claimed that they had experienced a rise in malicious activity since the pandemic started[32]. According to the 2022 X-Force's most attacked industry rankings, finance and insurance organizations drop to the second place attacked industry in 2021, representing 22.4% of the attacks X-Force remediated last year (a decrease from 23.0% in 2020). These attacks' breakdown by type of victim in more than two thirds were on banks, 16% were on insurance organizations and 14% were on other financial organizations. The authors of the survey suggest that the drop from first to second place is caused by the fact that financial institutions are better secured and, thanks to hybrid cloud environments, sensitive data management is more effective[33]. Similar conclusions can be drawn from data on cybersecurity-related incidents recorded in Poland breakdown by selected sector (Figure 2), where banking, insurance and financial market/finance were the first and second sectors in terms of number of incidents in 2019 and 2020 respectively, then dropped to fifth place in 2021, and came back to the second place in 2022. The share of financial sector in number of cyber accidents decreased from 23% and 22% (in 2019 and 2020 respectively) to only 5% in 2021, then rose up to 15% in 2022[34,35,36,37].

32. *The COVID Crime Index 2021*, BAE Systems, Surrey 2022, https://www.baesystems.com/en-financialservices/insights/the-covid-crime-index (22.08.2022), p. 5.
33. *X-ForceE*, IBM, *op. cit.* p. 44.
34. *Security of Polish Cyberspace*. Annual report 2019 on the activity of CERT Polska, https://cert.pl/en/annual-reports/ (13.09.2022), p. 14.
35. *Security landscape of the Polish Internet.* Annual report from the actions of CERT Polska 2020, https://cert.pl/en/annual-reports/ (13.09.2022), p. 26.
36. *The Polish Internet security landscape.* Annual report from the actions of CERT Polska 2021, https://cert.pl/en/annual-reports/ (28.07.2022), p. 22.
37. *Krajobraz bezpieczeństwa polskiego Internetu w 2022.* Raport roczny z działalności CERT Polska 2022, https://cert.pl/publikacje/ (04.07.2023), p. 37.

Figure 2. Number of cyber incidents reported by selected industries in Poland



Source: Own work based on CERT Reports: 2019[38], 2020[39], 2021[40], 2022[41].

Verizon's research shows that the financial sector continues to be a victim of organized crime, driven mostly (95%) by financial motives. This industry is often experiencing the actions of social engineering (phishing), hacking (using of stolen credentials) and malware (ransomware). Other still common patterns are miscellaneous errors, often in the form of mis-delivery[42].

3. Cyber threats to insurance companies

Due to the radically changing world, including technology, society and climate, the insurance sector has to provide security and resilience to both businesses and individuals alike. This demands that insurance companies make a strategic and urgent change and move to modernize technologies and business processes. A comprehensive literature review of the impact of digitalization on the insurance industry was provided by Eling and Lehmann[43]. Emerging digital opportunities help to improve the development of new products and transformation of key functions from marketing, distribution, underwriting and claims, to finance and accounting. Investments in risk management technology, data analytics and artificial intelligence (AI) may support insurance companies in customizing business processes and deliver digital insights into customers behaviour to provide them solutions better suited to their individual needs. It is in regard to more aware and

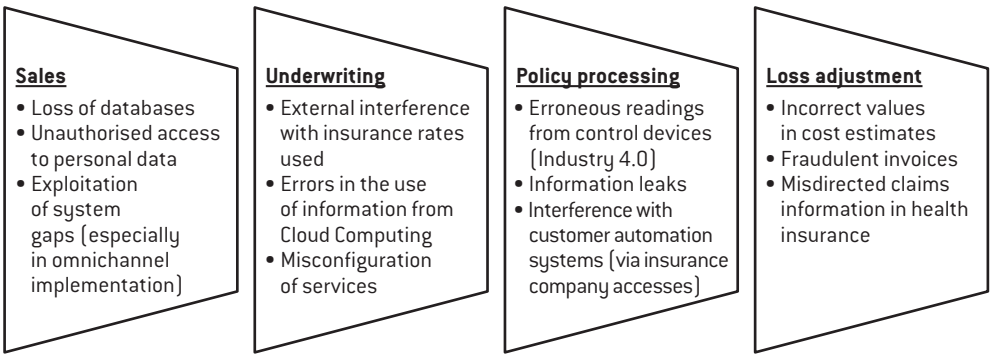
38. *Security*..., CERT, 2019, *op. cit.*
39. *Security*..., CERT, 2020, *op. cit.*
40. *The Polish*..., CERT, 2021, *op. cit.*
41. *Krajobraz*..., CERT, 2022, *op. cit.*
42. *Data*..., Verizon, *op. cit.*, p. 59.
43. Eling M. & Lehmann M., *The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks*, "The Geneva Papers on Risk and Insurance – Issues and Practice", 2018 3(43), DOI: 10.1057/s41288–017–0073–0, pp. 359–396.

demanding generation Z in particular, which is forthcoming with new expectations. Thus, insurers invest in digital solutions that will allow customers to report a claim, handle renewals or manage the policy by themselves. There are mobile applications, online forms, dedicated portals and more popular chatbots and virtual assistants (based on: Klapkiv & Klapkiv[44]; Eling & Lehmann[45]; Chojan, Lisowski & Manikowski[46]). However, the above-mentioned mean additional threats. Raising demand for technological innovations among financial institutions was also caused by Covid-19 pandemic, when many companies shifted to remote working and moved the majority of their activities to the digital world. There is no doubt that digital technology is an opportunity, however, increased reliance on computer systems also expands the range of threats and vulnerabilities, including the need for transparency around AI-driven decisions.

PWC's survey revealed that business and operational models (26%), cybersecurity and information management (23%) and markets (20%) were ranked as the most concerning risks faced by the insurance industry. Insurers admitted that they also worry about data security in particular. Their concerns mostly refer to data protection laws (73%) and cyber regulation (73%), and privacy rights and protection (71%)[47]. Other survey conducted by a leading insurance broker showed that cyberattacks/data breaches are number one in both the current top 10 risks and the predicted future risks[48].

Taking into consideration insurance company's business activity areas, the following are mostly vulnerable to cyber threats: sales, underwriting, policy processing and loss adjustment (for particular examples see Figure 3).

Figure 3. Selected elements of an insurance company's business model and examples of the cyber threats



Source: Own work.

44. Klapkiv L. & Klapkiv J., *Technological innovations in the insurance industry*, "Journal of Insurance, Financial Markets & Consumer Protection", 2017 4(26), https://depot.ceon.pl/bitstream/handle/123456789/14333/RU26–5.pdf?sequence=1&isAllowed=y, pp. 67–78.
45. Eling, M. & Lehmann M., *The Impact* ..., *op. cit.*
46. Chojan A., Lisowski J. & Manikowski P., *Digitalization trends in insurance and their impact on the functioning of the insurance markets entities*, "Wiadomości Ubezpieczeniowe", 2022 1, https://piu.org.pl/wp-content/uploads/2022/05/WU_2022–01_Chojan_Lisowski_en.pdf, pp. 3–15.
47. *Insurers aim to become masters of risk management*, PwC 2022, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-risk-survey/insurance-risk.html (01.09.2022).
48. *Global Risk Management Survey*. AON 2021, https://grms.aon.com/2021-global-risk-management-survey/cover/ (29.08.2022).

In the area of sales, special attention should be paid to unauthorized access to databases, due to human error or a lack of skill in operations, which may occur both in insurance companies and intermediaries. For this purpose, the authors investigated administrative decisions that have been issued by the President of the Polish PDPO in the almost 5-year period since the General Data Protection Regulation (GDPR) was implemented. Only in 2 out of 27 cases was a fine imposed on an insurance company (Table 2). The rest ended up with discontinuations of proceedings, refusals to grant the application against insurer or orders to re-notify the data subject of a personal data breach by insurer[49].

Table 2. Financial fines imposed by the President of Polish PDPO on insurance companies

Decision's number	Fined insurance company	Allegation/ Complaint	The amount of fine	Scope of data violated	Reason of data breach
DKN.5131.3.2021	STU ERGO Hestia S.A.	failure to notify the President of the PDPO about a personal data breach without undue delay, no later than 72 hours after the breach was discovered and data subjects of a personal data protection breach without undue delay	PLN 159,176	name, surname, ID number, town, postal code and other information concerning: the subject of insurance (a house), sum insured, premium	an e-mail containing analyses of insurance needs and an insurance offer with personal data has been sent by insurance broker company (which play two roles in data processing: 1) a controller of the name and surname and 2) entity processing for an insurance company) to an unauthorized address
DKN.5131.5.2021	TUiR Warta S.A.	failure to notify the President of the PDPO about a personal data breach without undue delay, no later than 72 hours after the breach was discovered and data subjects of a personal data protection breach without undue delay	PLN 85,588	refers to two persons: names, surnames, residential or correspondence addresses, ID numbers, telephone numbers, e-mail addresses and information concerning: the subject of insurance (passenger car), the scope of insurance, payments, assignments, as well as additional provisions resulting from the agreement	an e-mail with insurance policy containing personal data has been sent by an insurance agent (an entity processing for an insurance company) to an unauthorized address

Source: own work based on Decisions…, *op. cit.*

In the examples provided, only one or two persons were actually affected, but if in the same situation more customers are involved, the amount of the fine may be extremely high.

49. Decisions of the President of Polish PDPO, https://uodo.gov.pl/pl/p/decyzje (22.04.2023).

It is increasingly important nowadays, when one of the key elements of digital transformation is insurers' pursuit to increase the share of digital distribution channels and to provide omnichannel marketing, which will allow integrating all distribution and interaction channels with customers. This also means changes in agents' role in insurance sales, who should focus on more complex and profitable products when simple ones can be successfully automated and offered via self-service distribution channels[50]. To achieve a success, investments in digital tools supporting agents in servicing customers are crucial. The substantial source of threats in other areas of insurance company is constant access to various types of external databases, customers' IT systems or devices recording certain parameters of insurance items. A survey by Accenture revealed that 60% of insurers see the benefits of using data collected by Internet of Things (IoT) devices such as telematics technologies installed in vehicles, intelligent sensors in flats or various wearable technologies worn by customers. Additional information may be very useful during improving of underwriting and pricing model processes, as well as generating savings in insurance companies[51]. The authors of this paper would also like to draw attention to the preventive measures provided by such devices during the policy period. For example, information from sensors can be used by auto insurers to warn drivers about critical events in real time (e.g. low tire pressure or loss of operating fluids) or coach them about driving safely. Water leak detectors can help customers to identify and fix small water leaks or automatically cut off the water supply. Life insurers in connection with healthcare providers can use customers' data to help them live longer and healthier. It is also possible to prevent damages caused by storm, hail or flood, warning insured of the high probability of an imminent threat to life, health or property damage at an early stage. With regard to the use of modern devices to read certain parameters for the insurance sector, the idea of self-aware networks should be mentioned. On the one hand, the end device, which is installed in cars, homes or enterprises, is equipped with multiple sensors and can be used simultaneously by different recipients (e.g. vehicle manufacturers, insurers, road operators, multimedia content providers and others). This activity helps to increase resource efficiency. Other examples of devices are wireless devices for measuring human body parameters (used in life and medical insurance), weather stations (useful in crop insurance), the possibility to save photos from a mobile phone in the insurance company's system (e.g. for car inspections). However, on the other hand, the availability of readings to different audiences may involve opening up entry systems to other users. This means that security can be easily bypassed, which increases operational risk. One of the cyber risk scenarios for insurance companies, where a hack of a medium-sized UK-only motor insurer with a gross written premium equal to GBP 400 million was investigated by experts, confirms the above. In this scenario the hackers were able to break into the insurer's telematics device by guessing the username and password to the device, which were set to 'admin', 'admin'. This allowed them to remotely access images from the camera as well as location data, and then publish those data online. The total cost of recalling and replacing every device (physical damage), compensation for customers due to compromised and published information online and business interruption was estimated at almost GBP 70 million, which is ca. 18% of the annual premium. Moreover, according

50. *Cyfryzacja sektora ubezpieczeń w Polsce*, Accenture 2018, https://piu.org.pl/raporty/cyfryzacja-sektora-ubezpieczen-w-polsce/ (01.07.2022), p. 34.

51. Ibidem, p. 29.

to the scenario, the consequences of the incident were occurring up to 5 years after the incident, when the insurer's reputation was finally restored[52].

Another cyber threat in policy processing is insurers' pursuance to sever this area from paper documentation. It can be expected that under condition of compliance to some legal requirements, fully digital service will be introduced. In loss adjustment area insurer offers many solutions, including mobile applications, mobile appraisers, online claim registration or tracking of the entire claim settlement process[53],[54]. These typical insurance processes may be automated, digitized, better scaled with the help of the cloud and enriched with innovative cloud services. A proactive managing of loss adjuster process may help to avoid a customer's claim. But this requires real-time data processing and digital processes, which is a major challenge for traditional IT structures. Apart from the fine imposed by the President of the Polish Personal Data Protection Office, awarding compensation under civil law in connection with the violation of the provisions on the protection of personal data is not excluded. One of the examples of such a case was judgment of the District Court in Warsaw in August 2020. Then compensation to claimant was awarded for the violation of personal rights consisting in the provision of personal data by the insurance company whose employee sent loss adjustment documentation with personal data of the claimant (car owner) to the person injured in car accident[55].

Threats related to the use of technological solutions may also appear in other areas of the insurer's operations. In marketing, conducting market research in the form of an open survey can become a way for hackers to get inside the insurance company's system. Similarly, the use of the latest technological solutions in the recruitment of new employees may result in uncontrolled access to employee data resources[56]. But this type of interference applies to every company that uses new technologies, and insurance companies are not particularly different in this regard.

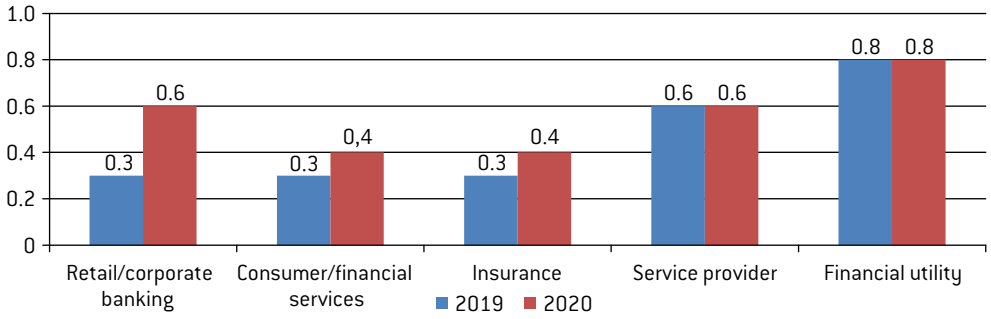
4. Measurement and mitigation of cyber risks in insurance companies

Due to the fact that adaptation to new operating conditions requires more and more financial resources allocated to cybersecurity management programs, based on Deloitte's survey, financial institutions keep increasing expenditures on cybersecurity. Percentage of both company overall revenue and IT spending on cybersecurity lifted on average from 0.3% and 10.1% (in 2019) to 0.5% and 10.9% respectively (in 2020)[57].

Figure 4 presents cybersecurity spending across financial institutions as a percentage of company revenue, which continues to grow or is stable depending on sector, however, the increase among the insurance industry is lower than average.

52. *Cyber operational risk scenarios for insurance companies*, Actuarial Post, 2018, https://www.actuarialpost.co.uk/article/cyber-operational-risk-scenarios-for-insurance-companies-15194.htm
53. Grzywaczewska K., *Ubezpieczyciel zmienia się dla klienta*, „Miesięcznik Ubezpieczeniowy", 2015 3, p. 5.
54. *Cyfryzacja*…, Accenture, *op. cit.* pp. 78–79.
55. Judgment of the District Court in Warsaw of August 6, 2020, XXV C 2596/19, LEX No. 3093515.
56. Eling, M. & Lehmann M., *The Impact*…, *op. cit.*, pp. 376–368.
57. *Reshaping the cybersecurity landscape. How digitalization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions*, Deloitte 2020, https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (17.08.2022), p. 5.

Figure 4. Revenue spent on cybersecurity on average across financial institutions (in %)



Source: Own worked based on *Reshaping* …, Deloitte, *op. cit.*. p. 5.

Looking at the share of cybersecurity spending in overall companies' IT budget across sectors, the largest increase (from 9.3% to 11.9% which is 2.6 pp) and share in 2020 was noticed in the insurance industry, whereas the rest of the surveyed companies (exclusive of consumer/financial services) reported decreases in this indicator (e.g. financial retail/corporate banking from 10.1% to 9.4%, service provider from 8.9% to 7.2%, and financial utility from 15.2% to 8.2%). Financial institutions mostly allocate cybersecurity resources to cyber monitoring and operations, and endpoint and network security (19% and 18% respectively). It is also worth noticing that share of identity and access management increased from 11% in 2018 to 16% in 2020. These three types of expenditures generally received more than 50% of the spending pie in the latest survey. Top investment priorities driven by emerging technologies, which are used to develop new products, services, and distribution channels, in financial institutions are: cloud, data/analytics and artificial intelligence/cognitive computing[58].

Rapid and extensive exposure to cyber breaches or attacks prompted the insurance industry to invest in and develop comprehensive risk management solutions. Operational cyber risk management in the insurance industry consists of several complex processes which include the identification, analysis and evaluation of the potential consequences (both financial and non-financial) of cyber risk and control over them. Based on EIOPA, all the insurers surveyed provided a self-assessment during risk management process. Moreover, all of them admitted that they add cyber risk to Operational Risk Management and 80% of respondents add it to their Own Risk and Solvency Assessment. Other common practices include collecting and investigating loss data and also using third parties' assessments (both methods were indicated by three of the four respondents). The survey results show that insurers use many types of risk assessment which include, for example, stress tests, worst case scenario analyses, and multiple scenario analyses, and others such as heatmaps, disaster recovery tests, penetration testing, crisis tests, and simulations[59]. The above-mentioned practices are used to verify a company's vulnerability to cyber incidents, estimate their probability and magnitude of impact, and based on that implement adequate risk control methods. One of them is loss prevention and reduction which has been highly developed

58. Ibidem, pp. 10–11.
59. *Cyber risk for insurers – challenges and opportunities*, EIOPA, Publications Office of the European Union, Luxembourg 2019, p. 8 and pp. 12–13.

and increasingly used during digital transformation (e.g. modern technologies like Blockchain, Artificial Intelligence (AI), analytics, Machine Learning (ML) and zero trust model, firewalls and secure gateways, updated software, systems and the security patches, encrypted sensitive data, backed up data, restricted and controlled access to data, employees trained on cyber incidents' prevention).

Deloitte's survey revealed that rapid IT changes and rising complexities have remained the biggest challenge in managing cybersecurity risk in large financial institutions[60]. Based on Polish society's opinion, the insurance sector was considered as a leader in cybersecurity only by 9% of respondents, whereas the banking sector was indicated by 57% of respondents[61]. To increase the digital operation resilience of the insurance sector against cyber threats and provide guidance on how insurance and reinsurance undertakings should apply the governance requirements foreseen in Directive 2009/138/EC5 'Solvency II Directive') and in Commission Delegated Regulation (EU) No 2015/356 ('Delegated Regulation') in the context of information and communication technology security and governance, on 12th October 2020 EIOPA issued Guidelines on Information and Communication Technology Security and Governance. They consist of rules and recommendations which should be implemented to mitigate technological risks appropriately and contain seven main areas: 1) governance and strategy, 2) ICT and security risk management, 3) ICT operations processes, 4) information security, 5) ICT project and change management, 6) business continuity management and 7) outsourcing. The guidelines represent a key step for the insurance sector to align with the European Commission's aim to boost and adjust the digital operational resilience of the EU's financial services (as envisioned by the legislative proposal for a Digital Operational Resilience Act)[62].

The aforementioned is one of several initiatives at the European level in this field, next to the key Directive on Security of Network and Information Systems (NIS Directive) and General Data Protection Regulation (GDPR). A set of loss prevention and reduction samples and recommended actions was issued by the Polish Financial Supervision Authority, based on the goals and tasks of supervision over the financial market and significant technology development. The Guidelines on the Management of Information Technology and ICT Environment Security for Insurance and Reinsurance Undertakings are 22 guidelines divided into 4 areas: 1) Strategy and Organization of the Information Technology and ICT Environment Security areas, 2) ICT Environment Development, 3) Maintenance and Exploitation of ICT Environment, and 4) ICT Environment Security Management. They were set to notify undertakings of expectations of the supervision authority with reference to information technology and ICT environment security risk management. In accordance with guideline No. 18, insurers should explore the profits arising from application of international standards with regard to information security (such as ISO/IEC 27000 standards[63]) and decide on whe-

60. *Reshaping*…, Deloitte, *op. cit.* pp. 8–9.

61. *Raport Cyberbezpieczny portfel*, Związek Banków Polskich 2022, https://zbp.pl/aktualnosci/wydarzenia/Raport-Cyberbezpieczny-Portfel-2022 (15.09.2022), p. 8.

62. *EIOPA Guidelines on Information and Communication Technology Security and Governance. Key insights and self-assessment checklist*, Deloitte 2021, https://www2.deloitte.com/lu/en/pages/insurance/articles/eiopa-guidelines-information-communication-technology-security-governance.html (16.09.2022), pp. 4–5.

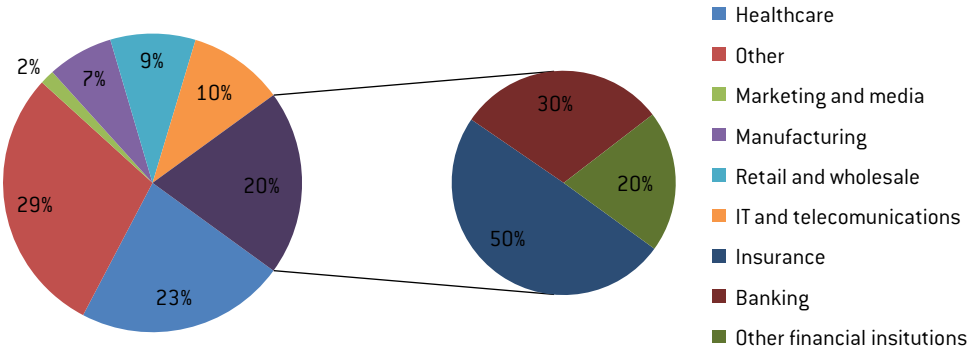
63. By the end of December 2021, there were 58,687 valid certificates, which makes ISO/IEC 27001:2013 the fourth most popular standard worldwide. ISO/IEC 27001:2013 has been revised by ISO/IEC 27001:2022. This document specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requi-

ther to adapt the ICT environment security management system functioning at the undertaking to the requirements of these standards[64]. However, due to significant financial losses (e.g. business interruption and costs related to incident response, data and system recovery, crisis management, third-party claims and legal expenses) and also reputational damage, physical cybersecurity solutions may turn out to be insufficient.

5. External financing methods of cyber risks in insurance industry

Even the best physical solutions will not provide companies with financial sources in case of data breaches and cyberattacks, but cyber insurance will. However, it is a key element of a broader risk management approach. Referring to survey results, 68% of insurers surveyed, admitted that they cover their own cyber risk through insurance[65]. Based on Willis Towers Watson's survey, the insurance industry was the biggest cyber insurance claims distributor between 2013–2019 (50% of all claims reported by the financial sector)[66].

Figure 5. Cyber insurance claims reported worldwide by selected industry in 2013–2019



Source: Own work based on: *Cyber*..., Willis Towers Watson, p. 14.

The great reliance on digital technology and communication leads to rapid growth in cyber insurance demand. According to Munich Re, the size of the global cyber insurance market is expected to rise from an estimated USD 9.2 billion (at the beginning of 2022) to approximately USD 22

rements for the assessment and treatment of information security risks tailored to the needs of the organization (International Organization for Standardization 2022, https://www.iso.org/home.html (01.10.2022)).

64. *Guidelines on the Management of Information Technology and ICT Environment Security for Insurance and Reinsurance Undertakings*, Polish Financial Supervision Authority 2016, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/wytyczne_dotyczace_zarzadzania_obszarami_IT (13.04.2022), pp. 4–5 and p. 55.
65. *Cyber*..., EIOPA, *op. cit.*, p. 13.
66. *Cyber claims analysis report Turning data into insight,* Willis Towers Watson 2020, https://www.wtwco.com/en-GB/Insights/2020/07/cyber-claims-analysis-report (15.09.2022), p. 14.

billion by 2025[67]. The world's leading cyber insurance provider in 2021 was Chubb Ltd. with USD 473,073 million direct premium written, which is almost 10% of total direct premiums written[68].

Table 3. Cyber insurance coverage in selected areas of business activities

Operational Risk	Liability Risk	Privacy & Network Security Risk
Network Business Interruption	Technology Errors & Omissions	Privacy and Network Security Liability
System Failure	Professional Liability	Privacy Regulatory Fines and Penalties
Dependent Business Interruption / System Failure	Media Liability	PCI Fines and Penalties
Cyber Extortion		Breach Event Expenses
Digital Asset Restoration		

Source: *Cyber Insurance in the World of Cyber Criminals*, AON 2019, https://www.slideshare.net/info_csnp/aon-cyber-insurance-in-the-world-of-cyber-criminals (15.10.2022), p. 5.

Cyber insurance provides cover in three areas of business activity (Table 3) and was designed to fill the gap that traditional insurance policies such as property damage and liability insurance do not cover. The scope of typical cyber insurance includes costs resulting from first-party damage and losses (direct losses incurred by the insured) such as data destruction, extortion, theft, hacking, and denial of service attacks, and third-party liability (liability coverage/losses to others) caused, for example, by errors and omissions, failure to safeguard data, or defamation. Among the first category of losses, we can indicate for example[69]:

- costs of reinstatement and replacement of data and intellectual property (e.g. software),
- the cost of new software purchase,
- the cost of transferring not-removed data to other servers,
- crisis management costs (e.g. costs of notifying stakeholders, investigating, IT experts, and post-incident public relations to reinstate reputation),
- the cost related to avoiding extortion or the extortion payment cost,
- increased cost of working / loss of profits,
- the cost of regulatory fines and penalties.

The second category of losses includes, but is not limited to:

- legal liability (also defense and claims expenses (fines), regulatory defense costs),
- vicarious liability and crisis control cost,
- cost resulting from data reinstatement.

The above-mentioned costs are examples and their list will certainly be expanded in the future.

67. *Cyber insurance: Risks and trends 2022*, Munich Re 2022, https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2022.html (15.10.2022).
68. *Top 10 Writers of Cybersecurity Insurance By Direct Premiums Written 2021*, Insurance Information Institute 2022, https://www.iii.org/table-archive/218710 (15.10.2022).
69. Eling M. & Wirfs J. H., *Cyber risk: Too big to insure?* Risk Transfer Options for a mercurial risk class, "I.VW HSG Schriftenreihe", 2016, no. 59, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, p. 23.

An important supplement in this regard may be the mapping of insurance coverage, where the type of events and the effectiveness of insurance coverage are indicated[70].

The discussion on how to hedge financial institutions (including insurance companies) operations to manage their own risk would not be completed without mentioning securitization. Referring to Banks it is: 'the process of removing assets, liabilities, or cash flows from the corporate balance sheet and conveying them to third parties through tradable securities'[71]. Insurance securitization may be defined as a financial operation that involves transfer of identified and assessed risk from an insurance company to the capital markets through the creation and issuance of financial securities.

Securitization is a relatively new risk transfer tool for insurers and reinsurers but it has been used in the financial market as early as the 1970s. Insurance securitization can take one of two forms: direct or indirect. In direct securitization or primary securitization, the cedent of the risk and the issuer of the securities are the same entity – the insurance or reinsurance company. The proceeds from the issue are invested in risk-free securities such as government bonds. This type of process is usually mediated by a bank as an advisor on the issue and a seller of securities. A huge disadvantage of this type of securitization is that the risk carried by the securities is not separated from the risk associated with the programmed originator's business activity. Therefore, the second form of insurance securitization is more popular. In an indirect securitization process, the originator (ceding company) establishes an independent special purpose vehicle (SPV or special purpose reinsurance vehicle – SPR). The SPV assumes the risk from the arranger of the securitization by entering into a reinsurance contract. It issues securities based on insurance premiums for insurance contracts relating to the transferred risks[72].

The conclusion of an agreement between the SPV and the originator of the transaction in the form of a reinsurance contract is necessary for legal reasons and for supervisory approval of the transfer. The SPV is usually a reinsurance company, reinsurance broker or captive. For tax reasons, SPVs are placed in tax havens. The company's activities are limited to issuing securities and investing the proceeds in safe financial instruments. The securitization process also involves intermediary entities, i.e. investment banks, rating agencies, advisory firms and insurance companies (called 'monolines' or 'wrappers') which guarantee the repayment of principal and interest to investors in the securities issued by the SPV. Repayment guarantees are only given to financial instruments with a high rating (usually AAA)[73].

As in the case of insurance or reinsurance contracts, securitization is therefore aimed at transferring part of the liability related to the financial (insurance) activity to other entities. Until now, the vast majority of securitizations have concerned the transfer of catastrophic risks such as hurricanes and earthquakes. However, due to the growing threat in the area of operational risk, it is also possible to use those instruments in this area. Nevertheless, there are certain limitations to such

70. Grimwade M., *Ten Laws of Operational Risk: Understanding Its Behaviours to Improve Its Management*, 2022, John Willey & Sons.

71. Banks E., *Alternative Risk Transfer: Integrated Risk Management through Insurance*, Reinsurance and the Capital Markets. John Wiley & Sons Ltd., Chichester 2004, p. 115.

72. Jobst A., *Back to Basics-What Is Securitization?*, "Finance and Development", vol. 45, no. 3, 2008.

73. *Securitization – new opportunities for insurers and investors*, Swiss Re, Sigma no. 7/2006, Swiss Reinsurance Company, Economic Research & Consulting, Zurich, p. 5.

operations. In Polish reality, in Art. 32 sec. 2 of the Act of 11 September 2015 on Insurance and Reinsurance Activity, we find a definition: Financial reinsurance means a long-term reinsurance contract, the characteristic feature of which is the limited transfer of insurance risk, and which has at least one of the following features: 1) takes into account the time value of money; 2) obliges the insurance undertaking to cover the negative balance of the reinsurer. Additionally, the legislator imposed on both parties to a financial reinsurance contract the obligation to properly define, measure, monitor and control the risk arising from such contracts.

It should be pointed out that securitization as a financing tool emerges above all when there are no insurance products to cover a given risk (e.g. climate intensity, catastrophic risks) or when the price for insurance is too high. A factor initiating this area of risk financing today may also be the search for attractive ways to invest spare funds. Consequently, it must be pointed out that none of these main factors for the development of securitization are present. Thus, this construct has a theoretical value at this point in time and is ready to be applied in the future.

Conclusions

Although cybersecurity threats are no longer a new phenomenon for enterprises, especially for the financial sector, large damage occurring (with losses counted in millions of USD) revealed how relevant it is to precisely define both the source of these threats and the tools of risk control – both in terms of physical and financial. The financial sector is specific in the context of cyber threats. The use of workplace automation is increasing and more and more workers are being replaced with computer systems or even AI. This excludes human errors as a part of physical risk control, but it also expands the exposure to the risk of (cyber) crime. This requires greater funds to provide additional security against external interference. Each cyber risk management tool should be properly adopted to the individual stages of the company's business model. The paper identifies threats in the key areas of an insurance company's operations, such as sales, underwriting, policy processing and loss adjustment and juxtaposes the possible loss scenarios from selected business area in insurance company with the scope of cover typical for cyber insurance. The lack of knowledge in insurance companies (for example the underwriting one, such as assessment of the subject of insurance, or the loss adjustment one, such as causes and consequences of an event) can be replaced with the use of Industry 4.0 solutions examined in the paper. Despite the fact that it improves the functioning of insurance companies, it can also lead to completely new claims events. Therefore, it is essential to establish appropriate methods for financing the results of cybersecurity incidents and damage. There are insurance products available for most industries that cover damages in the areas of data liability, business interruption, penalties, and fines. Insurance companies can also benefit from such solutions, although financial sector entities are also able to launch a mechanism to securitize this type of risk. In other words, the consequences of incidents and damages in the financial sector may also spread to other sectors, entities that will invest in new securities related to cyber damage. The paper may be used by insurance companies as an indication of the main factors creating operational cyber risk in an insurance company, which in turn may contribute to a re-analysis of the risk and exploring the methods of external financing its implementation.

References:

2022 Global Risk Survey Report. Embracing risk in the face of disruption, PwC 2022, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-risk-survey.html (06.07.2022),

Allianz Risk Barometer 2022, Allianz Global Corporate & Specialty 2022, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (30.08.2022),

Allianz Risk Barometer Results appendix 2022, Allianz Global Corporate & Specialty 2022, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (30.08.2022),

Banks E., *Alternative Risk Transfer: Integrated Risk Management through Insurance*, Reinsurance and the Capital Markets. John Wiley & Sons Ltd., Chichester 2004,

Bouveret A., *Estimations of losses due to cyber risk for financial institution*, "Journal of Operational Risk", 2019, vol. 14, No. 2, DOI: 10.21314/JOP.2019.224,

Cebula J. J. & Young J. J., *A taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN-028*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh 2010, https://www.semanticscholar.org/paper/A-Taxonomy-of-Operational-Cyber-Security-Risks-Cebula-Young/1e752a86215430f4dc59468ebf96df40fcb83b10 (07.07.2022),

Chojan A., Lisowski J. & Manikowski P., *Digitalization trends in insurance and their impact on the functioning of the insurance markets entities*, "Wiadomości Ubezpieczeniowe", 2022 1, https://piu.org.pl/wp-content/uploads/2022/05/WU_2022–01_Chojan_Lisowski_en.pdf,

Cost of Data Breach Report 2019, IBM, IBM Corporation, New York 2019, https://www.ibm.com/downloads/cas/RDEQK07R (31.08.2022),

Cost of Data Breach Report 2021, IBM, IBM Corporation, New York 2021, https://www.ibm.com/pl-pl/security/data-breach (27.04.2022),

Cost of Data Breach Report 2022, IBM, IBM Corporation, New York 2022, https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf (30.08.2022),

Curti F., Gerlach J., Kazinnik S., Lee M. & Mihov A., *Cyber risk definition and classification for financial risk management,* "Journal of Operational Risk", 2023, vol. 18, No. 2, DOI: 10.21314/JOP.2022.036,

Cyber claims analysis report Turning data into insight, Willis Towers Watson 2020, https://www.wtwco.com/en-GB/Insights/2020/07/cyber-claims-analysis-report (15.09.2022),

Cyber Insurance in the World of Cyber Criminals, AON 2019, https://www.slideshare.net/info_csnp/aon-cyber-insurance-in-the-world-of-cyber-criminals (15.10.2022),

Cyber insurance: Risks and trends 2022, Munich Re 2022, https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2022.html (15.10.2022),

Cyber risk for insurers – challenges and opportunities, EIOPA, Publications Office of the European Union, Luxembourg 2019,

Cyfryzacja sektora ubezpieczeń w Polsce, Accenture 2018, https://piu.org.pl/raporty/cyfryzacja-sektora-ubezpieczen-w-polsce/ (01.07.2022),

Data Breach Investigations Report. Verizon 2022, https://www.verizon.com/business/resources/reports/dbir/ (26.07.2022),

Decisions of the President of Polish PDPO, https://uodo.gov.pl/pl/p/decyzje (22.04.2023),

EIOPA Guidelines on Information and Communication Technology Security and Governance. Key insights and self-assessment checklist, Deloitte 2021, https://www2.deloitte.com/lu/en/

pages/insurance/articles/eiopa-guidelines-information-communication-technology-security-governance.html (16.09.2022),

Eling M. & Lehmann M., *The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks*, "The Geneva Papers on Risk and Insurance – Issues and Practice", 2018 3(43), DOI: 10.1057/s41288–017–0073–0,

Eling, M. & Wirfs, J. H., *Cyber risk: Too big to insure?* Risk Transfer Options for a mercurial risk class, "I.VW HSG Schriftenreihe", 2016, No. 59, Verlag Institut für Versicherungswirtschaft der Universität St. Gallen,

FERMA European Risk Manager Survey Report, FERMA 2022, https://www.ferma.eu/publication/european-risk-manager-report-2022/ (29.08.2022),

Financial Cyber Survey, Deloitte 2021, https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/finance/FSI_cyber_finish_V5.pdf (02.09.2022),

Frey C.B. & Osborne M.A., *The future of employment: How susceptible are jobs to computerisation?* "Technological forecasting and social change", 2017, vol. 114, https://doi.org/10.1016/j.techfore.2016.08.019,

Global Risk Management Survey. AON 2021, https://grms.aon.com/2021-global-risk-management-survey/cover/ (29.08.2022),

Grzywaczewska K., *Ubezpieczyciel zmienia się dla klienta*, „Miesięcznik Ubezpieczeniowy", 2015 3,

Guidelines on the Management of Information Technology and ICT Environment Security for Insurance and Reinsurance Undertakings, Polish Financial Supervision Authority 2016, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/wytyczne_dotyczace_zarzadzania_obszarami_IT (13.04.2022),

Insurers aim to become masters of risk management, PwC 2022, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-risk-survey/insurance-risk.html (01.09.2022),

International Organization for Standardization 2022, https://www.iso.org/home.html (01.10.2022),

Jobst A., *Back to Basics-What Is Securitization?*, "Finance and Development", vol. 45, No. 3, 2008,

Judgment of the District Court in Warsaw of August 6, 2020, XXV C 2596/19, LEX No. 3093515,

Kamiński S., *Analiza*. w: *Encyklopedia katolicka t. 1*, red. F. Gryglewicz, R. Łukaszyk, Z. Sułowski, TN KUL, Lublin 1989,

Kamiński S., *Jak filozofować. Studia z metodologii filozofii klasycznej*. TN KUL, Lublin 1989,

Klapkiv L. & Klapkiv J., *Technological innovations in the insurance industry*, "Journal of Insurance, Financial Markets & Consumer Protection", 2017 4(26), https://depot.ceon.pl/bitstream/handle/123456789/14333/RU26–5.pdf?sequence=1&isAllowed=y,

Krajobraz bezpieczeństwa polskiego Internetu w 2022. Raport roczny z działalności CERT Polska 2022, https://cert.pl/publikacje/ (04.07.2023),

Morgan S., *2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/ (01.09.2022),

Morgan S., *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, 2020, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (01.09.2022),

PwC's Global Economic Crime and Fraud Survey 2022, PwC 2022, https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html (30.08.2022),

Raport Cyberbezpieczny portfel, Związek Banków Polskich 2022, https://zbp.pl/aktualnosci/wydarzenia/Raport-Cyberbezpieczny-Portfel-2022 (15.09.2022),

Reshaping the cybersecurity landscape. How digitalization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions, Deloitte 2020, https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (17.08.2022),

Securitization – new opportunities for insurers and investors, Swiss Re, Sigma No. 7/2006, Swiss Reinsurance Company, Economic Research & Consulting, Zurich,

Security of Polish Cyberspace. Annual report 2019 on the activity of CERT Polska, https://cert.pl/en/annual-reports/ (13.09.2022),

Strupczewski G., *Defining Cyber Risk,* "Safety Science", 2021, vol. 135, DOI: 10.1016/j.ssci.2020.105143,

Tsakalidis G., Nousias N. & Vergidis K., *Towards a Fitting Representation Method for Redesign Evaluation and Cost-Based Optimization*, Operational Research in the Era of Digital Transformation and Business Analytics. BALCOR 2020. Springer Proceedings in Business and Economics, Cham 2020, DOI: 10.1007/978-3-031-24294-6_4,

The COVID Crime Index 2021, BAE Systems, Surrey 2022, https://www.baesystems.com/en-financialservices/insights/the-covid-crime-index (22.08.2022),

The Global Risks Report 2022. 17th Edition. Insight Report, World Economic Forum, Cologny/Geneva 2022, https://www.weforum.org/reports/global-risks-report-2022/ (29.08.2022),

The Polish Internet security landscape. Annual report from the actions of CERT Polska 2021, https://cert.pl/en/annual-reports/ (28.07.2022),

Top 10 Writers of Cybersecurity Insurance By Direct Premiums Written 2021, Insurance Information Institute 2022, https://www.iii.org/table-archive/218710 (15.10.2022),

Wang Y., Li B., Li G., Zhu X. & Li J., *Risk factors identification and evolution analysis from textual risk disclosures for insurance industry*, "Procedia Computer Science", vol. 162, 2019, https://doi.org/10.1016/j.procs.2019.11.253,

World Economic Outlook Database, International Monetary Fund, 2022, https://www.imf.org/en/Publications/WEO/weo-database/2022/April (28.08.2022),

X-Force Threat Intelligence Index 2022 Full report, IBM, IBM Corporation, New York 2022, https://www.ibm.com/security/data-breach/threat-intelligence/ (17.08.2022).

Operacyjne ryzyko cybernetyczne w odmiennym modelu biznesowym zakładów ubezpieczeń na przykładzie Polski

Cyberbezpieczeństwo stało się jednym z największych wyzwań dzisiejszego postpandemicznego, cyfrowego i połączonego świata, a także tematem o strategicznym znaczeniu dla branży ubezpieczeniowej. Nie ma wątpliwości, że postęp technologiczny, w tym zwiększone wykorzystanie dużych zbiorów danych i przetwarzanie ich w chmurze stwarzają możliwości dla branży ubezpieczeniowej, ale także zwiększają podatność zakładów ubezpieczeń na ryzyko cybernetyczne. Ponieważ ubezpieczyciele zbierają duże ilości poufnych danych, w tym dane osobowe, są naturalnym celem cyberataków. Celem

artykułu jest wskazanie z jednej strony, w jaki sposób zagrożenia związane z digitalizacją wpływają na codzienne funkcjonowanie zakładu ubezpieczeń w wybranych obszarach, a z drugiej jakie metody mogą służyć zarządzaniu nim. Po ogólnym przeglądzie ryzyka cybernetycznego na podstawie ostatnich raportów branżowych i wyników badań, autorzy zidentyfikowali jego globalny wpływ ekonomiczny ze szczególnym uwzględnieniem instytucji finansowych, a także ekspozycję i postrzeganie ryzyka cybernetycznego przez ubezpieczycieli oraz wydatki ponoszone na cyberbezpieczeństwo. Ponadto zbadano decyzje administracyjne wydane przez Prezesa Urzędu Ochrony Danych Osobowych w Polsce, wybrane orzeczenia i scenariusze szkodowe dla zakładów ubezpieczeń ze szczególnym uwzględnieniem procesu underwritingu, sprzedaży, administracji i likwidacji szkód. Wyniki badań literaturowych wskazują, że ryzyko cybernetyczne uznawane jest za jedno z najistotniejszych ryzyk niefinansowych (w kontekście źródła zagrożenia, a nie rezultatu) dla ubezpieczycieli, a także że dostępnych jest wiele proaktywnych środków bezpieczeństwa, które mogą oni wdrożyć. Jednak ze względu na dużą podatność na wycieki poufnych danych osobowych i finansowych lub nieautoryzowany dostęp do systemu, który może spowodować nie tylko straty finansowe, ale także przerwy w działalności i szkody wizerunkowe, zdaniem autorów zapobieganie i ograniczanie strat jest niewystarczające. Wskazano więc zarówno ubezpieczeniowe, jak i poza ubezpieczeniowe metody zewnętrznego finansowania skutków cyber ryzyka. Na tej podstawie cyber ubezpieczenie jest uważane przez autorów za najlepsze narzędzie zapewniające zarówno prewencję, jak i kompensację strat spowodowanych realizacją operacyjnego ryzyka cyber również w zakładach ubezpieczeń.

Słowa kluczowe: cyberryzko, ryzyko operacyjne, zakład ubezpieczeń, zarządzanie ryzykiem, ubezpieczenie cyber

DR ALEKSANDRA HĘĆKA-SADOWSKA – Poznań University of Economics and Business
e-mail: aleksandra.hecka-sadowska@ue.poznan.pl
ORCID:0000-0002-7649-9528

DR HAB. KRZYSZTOF ŁYSKAWA – Poznań University of Economics and Business
e-mail: Krzysztof.Lyskawa@ue.poznan.pl
ORCID: 0000-0002-7409-8624