Humanities and Social Sciences **2023**
Research Journal 30, No. 2 (2023), pp 99-107 **April-June**

Received: January 2023
Accepted: June 2023
DOI: 10.7862/rz.2023.hss.18

Dariusz PAUCH[1]

RANSOMWARE ATTACKS AS A CYBERSECURITY INSURANCE COVERAGE THREAT

The main purpose of this article is to analyze ransomware risk and its impact on the loss ratio in cyber insurance. To achieve this goal, the article indicates the scale of the threat of ransomware attacks and the prospects for change in the field of cyber insurance protection. Methodologically, the focus is on analysis and literature studies in order to properly describe and classify cyber threats, including ransomware risk. Statistical data were analyzed to find the scale of ransomware threats. Through the analysis, attention was drawn to the need for changes in the approach to cyber risk by both entrepreneurs and insurance companies. The originality of the study lies in its attempt to capture the necessity of changes in the field of cyber insurance, and justify their introduction. A research gap was identified, as the problem of ransomware attacks became particularly acute during the COVID-19 pandemic.

Keywords: hacker attack, ransomware attack, cyber risk, insurance, cybersecurity insurance coverage, COVID-19.

1. INTRODUCTION

Cyber attacks have a serious impact on both individual companies and the wider economy. Cyber risk (cyber risk) can be understood as the economic risk related to the possession, operation, use, and impact of IT devices and technologies in the enterprise (Marsh, 2015). Cyber risk is usually mistaken only for hackers infecting a computer with malware. Although this is a common manifestation of cyber risk, one should not forget other equally dangerous incidents. One such example is ransomware − a form of malware designed to encrypt a victim's files and make them unusable without payment (Oosthoek et al., 2022). Ransomware belongs to the class of malicious software that is designed specifically for financial gain (Liska, Gallo, 2016). The ciphers used by malware, when properly used, guarantee that the encrypted data cannot be decrypted without the decryption key, which is in the possession of criminals. While the first documented ransomware attack dates back to 1989, ransomware remained relatively uncommon until the mid 2000s (Kharraz et al., 2015). There are thousands of different ransomware strains in existence today, varying in design and sophistication (Bajpai et al., 2018).

[1] Dariusz Pauch, University of Szczecin, Poland; e-mail: dariusz.pauch@usz.edu.pl. ORCID: 0000--0002-0179-4784.

The most common source of malware attack of this type are (Cert, 2021):

- Vulnerability to attacks in publicly available services – VPN, RDP, mail server, etc. Often, vulnerabilities are exploited within hours or days after the public information about their existence becomes available.
- Insufficiently secured (usually a weak password) remote access channels to infrastructure and public services – RDP, VNC, FTP, databases, etc.
- E-mails urging you to download and run an attached or linked file

Additionally, during the COVID-19 crisis, another outbreak has happened in cyber space: a digital pandemic driven by ransomware. Malware attacks that encrypt company data and systems and demand a ransom payment for release are surging globally.

During the COVID-19 pandemic, an increase in cyber attacks on the information systems of large companies and banks was observed. Another aspect that increased the risk of cyber attacks, among others energy infrastructure is Russia's invasion of Ukraine. According to the World Economic Forum (World Economic Forum, 2023) in 2022, one of the main targets of cyberattacks were elements of critical infrastructure, such as hospitals, airports or power plants. This is caused by the increased number of attacks by Russian hackers on the infrastructure of countries helping Ukraine. An example is Poland, which has become the target of increased attacks by Russian hackers since the beginning of the war in Ukraine. This is confirmed by the Check Point Research data published in the Cyber Security Report (Check Point Research, 2022). The data shows that the number of attacks on critical infrastructure in the first few months of the war almost doubled. Hackers target criminal activity at entities with significant financial surpluses or persons responsible for making financial decisions. Successful blocking of key functions of Internet applications or internal IT systems of this type of entities means a high probability of extorting a ransom for removing the blockade. Cybercriminals are constantly improving the above-mentioned BEC e-mail method by sending infected spam directly to people making decisions in companies regarding payments for provided services (Leopando, 2016). According to data, in 2020 ransomware attacks on a global scale increased by 62% year-on-year (https://www.blackfog.com/the-state-of-ransomware-in-2020/). Therefore, a fundamental shift is occurring in the management of cyber risk. The idea that cyberattacks are increasingly likely – and perhaps inevitable – is beginning to take hold among executives and boards (Deloitte, 2016). Therefore, businesses are increasingly using cyber insurance.

The aim of this article is to analyze the risk of ransomware and its impact on the loss ratio in cyber insurance. To achieve the set goal, the scale of threats from ransomware attacks and the prospects for changes in the field of cyber insurance protection were indicated.

2. RANSOMWARE – THE SCALE OF THE THREAT TO INSURANCE COMPANIES

Cyber insurance increases awareness of risk and scale of threat, especially the need to implement tools to improve security in cyberspace (Malinowska, 2018). Increasing awareness and creating technical measures for companies against cyber related risks will significantly reduce the risks encountered, but will never be able to guarantee full protection. Moreover, small organizations usually do not have enough budget to invest in high-cost security measures such as next-generation firewalls; intrusion detection and prevention systems, and email security solutions. Through this point of view, the importance of cyber risk insurance for small organizations only increases. These are

a particular reasons cyber risk insurance is significant for business (Gavėnaitė-Sirvydienė, 2019):

1. Data are among our most important assets and result in financial losses if they are stolen or lost.
2. Information and communication technologies are critical in daily operations. The interruption of the system will cause many financial losses.
3. The obligation to protect data of third parties is stipulated in laws and if they are lost or stolen, they are exposed to serious penal and punitive sanctions.
4. All of these cyber-attacks that occur lead to material losses as well as the loss of reputation of the organization in the sector (Sloan, 2017).

According to the National Association of Insurance Commissioners (NAIC), the insurance market for cybersecurity policies recorded an increase in gross written premium by 29.1% year on year in 2020 (National Association of Insurance Commissioners, 2021). The above data were also confirmed by Allianz Global Corporate & Specialty (AGCS). Since 2016, the number of claims has been steadily growing (Fig. 1).

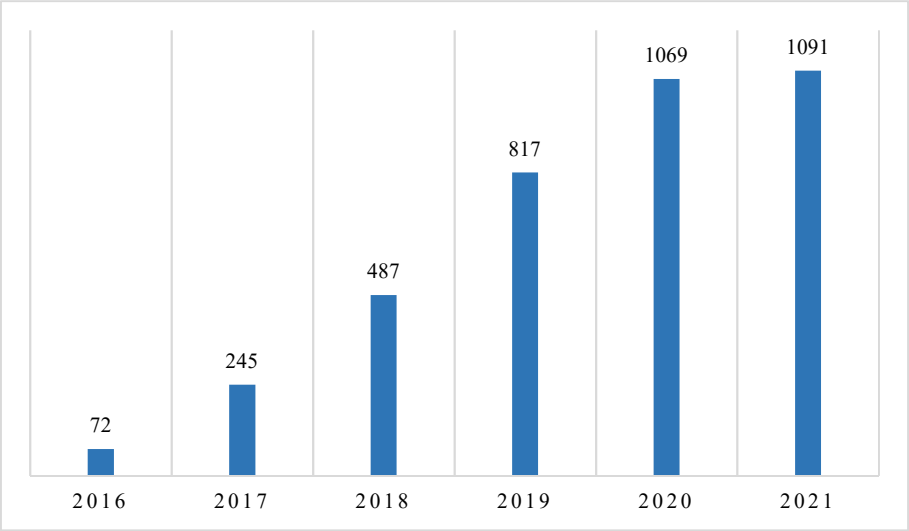

Fig. 1. Number of cyber-related claims against Allianz Global Corporate & Specialty (AGCS)

Source: *Ransomware trends: Risks and Resilience*, Allianz Global Corporate & Specialty, Munich 2021.

Among the 20 largest insurers in the USA offering cyber policies, loss ratios in the years 2017–2020 were in the range of 24.6% – 114.1%. The chart below presents the average loss ratio over the last four years (Fig. 2) (National Association of Insurance Commissioners, 2021).

It should be noted that the shaping of the cyber-cyber loss ratio is influenced only by individual attacks. In this insurance group, so far, no catastrophic claims have occurred. Table 1 presents the cybersecurity claims ratios for the five largest US insurance companies.

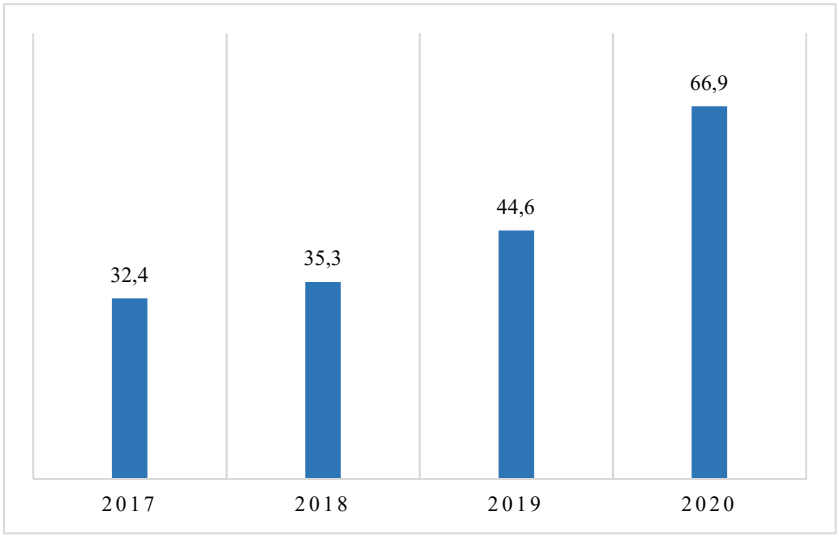

Fig. 2. Average value of the loss ratio for cyber policies (in percent)

Source: *Report on the Cybersecurity Insurance Market* (National Association of Insurance Commissioners (NAIC), 2021).

Table 1. The loss ratio among the five largest insurers selling cyber-policy in the US

	GROUP NAME	LOSS RATIO W/DCC (in %)	MARKET SHARE (in %)
1.	CHUBB LTD GRP	61	14,7
2.	AXA INS GRP	98,2	10,6
3.	AMERICAN INTRNL GRP	100,6	8,3
4.	ST PAUL TRAVELERS GRP	85,5	7,5
5.	BEAZLEY GRP	47,9	6,5

Source: *Report on the Cybersecurity Insurance Market*, National Association of Insurance Commissioners (NAIC), USA 2021.

You should also note some of the biggest examples of ransomware attacks in 2021 (Table 2). Every sector of the economy is exposed to attacks: financial, health, refining, oil, and IT.

The fact that cyber insurance is becoming an increasing risk for insurance companies is confirmed by media reports:

- Business Insurance: Ransomware losses disrupt the cyber liability market (Businessinsurance, 2022).
- Insurance Bussines Mag: Current cyber insurance model is ripe for change – cyber advisor (Insurancebusinessmag, 2022).
- Reuters: Insurers run from ransomware cover as losses mount (Reuters, 2022).
- Financial Times: Cyber Insurers recoil as ransomware attacks "skyrocket" (Financial Times, 2022).

Table 2. Ransomware: some of the largest single cases 2021

COMPANY	THE AMOUNT OF THE RANSOM
Colonial Pipeline	**$ 4.5m** (Ransom paid): Attack affected oil supply by halting the pipelines operations.
JBS USA	**$ 11m** (Ransom paid): Attack reduced the ability to package meat products.
CAN Financial	**$ 40m** (Ransom paid): The US Insurance company becam victim of a ransome group called "Phoenix".
Kaseya	**$ 70m** (Ransom demand): The software vendor was hit by a supply chain cyberattack spreading to around 1.500 business worldwide.
Health Service Executive (HSE) Ireland	**$ 600m** overall damage to Ireland's publicly funded healthcare system after a ransomware attack.

Source: Own elaboration based on Munich Re, 2022 [Access: 12.10.2022]. Access on the internet: https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2022.html.

In addition to the increased loss ratio, ransomware attacks pose four main threats to insurance companies and the entire insurance market:

1. Financing the development of criminal groups – funds obtained by criminal organizations make them even larger and more difficult to fight. The development of 'ransomware as a service' has made it easier for criminals to carry out attacks. Run like a commercial business, hacker groups such as REvil and Darkside sell or rent their hacking tools to others. They also provide a range of support services. As a result, many more malicious threat actors are operating.
2. Legal and political conditions – there are countries that prohibit paying the ransom for a ransomware attack. Examples are: USA – The Department of the Treasury's Office of Foreign Assets Control (OFAC), UK – The National Cyber Security Center (NCSC), and Netherlands – The Dutch Ministry of Justice and Security. However, there are no laws that prohibit paying an insurance company ransom.
3. The effectiveness of ransom payment law enforcement agencies typically advise against paying extortion demands to not further incentivize attacks. Even when a company decides to pay a ransom, the damage may already have been done. Restoring systems and enabling the recovery of the business is a huge undertaking, even when a company has the decryption key. As reported by Sophos in 2021 on average, organizations that paid got back only 61% of their data, down from 65% in 2020. Similarly, only 4% of those that paid the ransom got ALL their data back in 2021, down from 8% in 2020 (Sophos, 2022). There is no guarantee that your data will be unlocked after the ransom has been paid. Even if they do, the company will still be exposed to further attacks.
4. Possible loss of image – loss of reputation among customers and suppliers is as important a threat as production interruptions or complete paralysis of the company's operations.

In addition to the above, Allianz Global Corporate & Security (AGCS) identifies other trends related to attacks in the ransomware space (Allianz Global Corporate & Specialty, 2021):

- From single to double to triple extortion: 'Double extortion' tactics are on the rise. Criminals combine the initial encryption of data or systems, or increasingly even their back-ups, with a secondary form of extortion, such as the threat to release sensitive or personal data. In such a scenario, affected companies have to manage the possibility of both a major business interruption and a data breach event, which can significantly increase the final cost of the incident. 'Triple extortion' incidents can combine DDoS attacks, file encryption and data theft – and don't just target one company, but potentially also its customers and business partners. A notable case was a psychotherapy clinic in Finland – a ransom was demanded from the hospital. At the same time, smaller sums were also demanded from patients in return for not disclosing their personal information.
- Supply chain attacks the next big thing: There are two main types – those that target software/IT services providers and use them to spread the malware (for example, the Kaseya or Solarwinds attacks). Or those that target physical supply chains or critical infrastructure, such as the one which impacted Colonial Pipeline. Service providers are likely to become prime targets as they often supply hundreds or thousands of businesses with software solutions and therefore offer criminals the chance of a higher payout.
- Ransom dynamics: Ransom demands have rocketed over the past 18 months. According to Palo Alto Networks, the average extortion demand in the US was $5.3mn in the first half of 2021, a 518% increase on the 2020 average; the highest demand was $50mn, up from $30mn the previous year. The average amount paid to hackers is around 10 times lower than the average demand, but this general upward trend is alarming.

In connection with the above, insurance companies will strive to introduce changes in the field of cyber insurance.

3. PROSPECTS FOR CHANGES IN CYBER INSURANCE RELATED TO RANSOMWARE ATTACKS

Cyber insurance costs are rising in response to increasing cyber security breaches, data breaches and ransomware. In response, cyber insurers are encouraging companies to strengthen and invest in cybersecurity. However, the above actions turn out to be insufficient, therefore market insurers should focus on the following actions:

1. Restrictive insurance risk assessment – insurance companies should and will strive for a more restrictive insurance risk assessment. Before concluding the insurance contract, they will force the clients to verify their collaterals. An example is testing applications and websites against ransomware attacks.
2. Changes in sums, increased franchises, higher insurance premiums – along with loss ratio, the insurance company will lower sums and increase insurance premiums. The own share of the insured in the event will also be increased (up to 50%). The insurer will limit the ransom amount paid so that the customer also pays the cost.
3. Additional clauses in the content of the general terms and conditions of insurance contracts − insurance companies will introduce additional clauses, e.g., ransom payment will take place upon obtaining the consent of the police or other services

responsible for prosecuting such crimes. There may also be limitations in the form of ransomware attack protection only in the event of a cyber war. The concept of cyberwar has not been clearly defined so far. Steve Winterfeld and Jason Andress indicate that the definition of cyberwar is not easy to establish and that is why it is still the subject of scientific debate (Winterfeld, Andress, 2013). However, despite the many difficulties in trying to build a scientific description of it, they appear. By the concept of cyberwar, James A. Green understands the extension of policy through actions taken in cyberspace by state entities or by nonstate actors with significant state orientation or support that pose a serious threat to the security of another state, or an action of the same nature taken in response to a serious threat for state security (actual or perceived) (Green, 2015).

4. Non-payment of the ransom – in 2021, the French insurer AXA excluded the liability of paying the ransom in cyber insurance. Sometime later, Reuters reported that cyber criminals using ransomware called Avaddon had hacked the group's Asia operations and stolen three terabytes of data.
5. If the ransom is not paid, what can the insurer offer in return? Insurance companies will have to offer their clients something in return. In this case, the cyber policy should contain the following elements:
   - access to the response team in the event of an incident detection (in the form of assistance, hotline);
   - financial assistance in the event of business interruption (return of loss of profit, coverage of operating costs);
   - protection of the entrepreneur's reputation (financing the costs of an advertising campaign in order to regain customer trust).

The key challenges facing the cybersecurity market are data limitations, companies' limited awareness of cybersecurity risks, and the risk of high losses from a cyberattack by insurers, brokers, and other industry members.

4. CONCLUSIONS

In recent years, there has been a noticeable increase in the demand for cyber insurance. This was favored by low risk assessment requirements on the part of insurers, low price levels, and the growing number of insurance companies that wanted to build portfolios based on this product line.

The COVID-19 pandemic and the relocation of many online business activities resulted in an unprecedented scale of cyber attacks on corporate infrastructures. The number of reported cyber-crimes keeps growing because these criminals are expanding their networks, discovering new vulnerabilities to achieve their targets. Due to these causes, the cyber risk insurance market will continue to play a very significant role in the future to support companies in managing their exposure to possible cyber threats.

Due to the intensification of ransomware attacks in the last two years, insurers will have to react and introduce changes to their policies. The most important changes that will be introduced on the insurance services market include:

- Increase in insurance premiums.
- Restrictive insurance risk analysis.
- The insured's share of the ransom costs incurred.

- Extending the insurance cover with additional aspects, such as, for example, covering the costs of business interruptions, or extending the entrepreneur's civil liability due to lost sensitive data.

Additionally, insurance companies will have to start working with technology companies. The cooperation will be aimed at assessing the IT security of companies before concluding an insurance contract.

REFERENCES

Allianz Global Corporate & Specialty (2021). *Ransomware trends: Risks and Resilience*, Munich.

Andress, J., Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners: second edition,* Syngress, USA.

Bajpai, P., Sood, A.K., Enbody, R. (2018). *A key-management-based taxonomy for ransomware*, APWG Symposium on Electronic Crime Research (eCrime), IEEE.

Cert (2021). *Poradnik ransomware 2021* [Access: 4.10.2022]. Access on the internet: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf.

Check Point Research. (2022). *Cyber Security Report*.

Deloitte (2016). *Beneath the surface of a cyberattack A deeper look at business impacts* [Access: 7.10.2022]. Access on the internet: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf.

Gavėnaitė-Sirvydienė, J. (2019). *Evaluation of cyber insurance as a risk management tool providing cyber-security. "Social Transformations in Contemporary Society"*, 7.

Green, J. (2015). *Cyber Warfare: A multidisciplinary analysis*. New York: Routledge Taylor & Francis Group.

https://www.blackfog.com/the-state-of-ransomware-in-2020/ [Access: 08.10.2022].

https://www.businessinsurance.com/article/20211012/NEWS06/912345135/Ransomware-losses-disrupt-cyber-liability-market [Access: 14.10.2022].

https://www.ft.com/content/4f91c4e7-973b-4c1a-91c2-7742c3aa9922 [Access: 14.10.2022].

https://www.insurancebusinessmag.com/uk/news/cyber/current-cyber-insurance-model-is-ripe-for-change--cyber-advisors-317648.aspx [Access: 14.12.2022].

https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2022.html [Access: 12.10.2022].

https://www.reuters.com/article/us-axa-cyber-idUSKCN2CX0B0 [Access: 17.12.2022].

https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/ [Access: 14.12.2022].

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E. (2015). *Cutting the gordian knot: A look under the hood of ransomware attacks. Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, Milan. DOI: 10.1007/978-3-319-20550-2_1.

Leopando, J. (2016). *Patch Your Flash: Another Zero-Day Vulnerability Hits Adobe Flash*. In blog: "TrendLabs Security Intelligence Blog" [Access: 27.10.2016]. Access on the internet: http://blog.trendmicro.com/trendlabs-security-intelligence/patch-flash-another-zerodayvulnerability-hits-adobe-flash.

Liska, A., Gallo, T. (2016). *Ransomware. Defending Against Digital Extortion.* O'Reilly Media, USA.

Malinowska, K. (2018), *Aspekty prawne ubezpieczenia cyber ryzyk. „Prawo asekuracyjne",* 2/2018 (95).

Marsh (2015). *The role of insurance in managing and mitigating the risk*. UK cyber security [Access: 10.10.2022]. Access on the internet: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/ UK_Cyber_Security_Report_Final.pdf.

National Association of Insurance Commissioners (NAIC) (2021). *Report on the Cybersecurity Insurance Market.* USA.

Oosthoek, K., Cable, J., Smaragdakis, G. (2022). *A Tale of Two Markets: Investigating the Ransomware Payments Economy. "Computer Science"*. 10 May 2022. DOI: 10.48550/arXiv.2205.05028.

Sloan, R. (2017). *Cyber Matters: The Importance of Cyber insurance for SMEs*, Cubb INC USA [Access: 13.10.2022]. Access on the internet: https://www.cybersecurityjournal.org/cybermatters-he-importance-ofcyber insurance.

Sophos (2022). *The state of ransomware 2022* [Access: 14.10.2022]. Access on the internet: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf.

World Economic Forum (2023). *Global Cybersecurity Outlook 2023. Insight Report.*