MIS Quarterly Executive

Volume 24 | Issue 1 Article 5

March 2025

Unraveling the Role of Cyber Insurance in Fortifying Organizational Cybersecurity

Wojciech Strzelczyk

Karolina Puławska

MIS Quarterly Executive

Unraveling the Role of Cyber Insurance in Fortifying Organizational Cybersecurity

Cyberattacks pose significant threats to businesses, undermining their financial stability, operational continuity and data integrity. Though many people think that cyber insurance serves primarily to compensate victims in the event of a cyber incident, this article explores the three stages at which cyber insurance helps to improve an organization's cybersecurity—(1) pre-purchase, (2) post-purchase and (3) post-cyberattack. Collectively, these stages allow cyber insurance to enhance a company's overall cyber-risk management.[1,2]

Wojciech Strzelczyk
Kozminski University (Poland)

Karolina Puławska
University of Warsaw (Poland)

Inadequate Cybersecurity Remains a Big Problem

While many companies boast about their achievements in digital transformation, for business-risk managers, there is a dark side to the rapid incorporation of new technologies: an increased risk of cyberattacks.[3] Such attacks can result in financial loss, harm to an organization's reputation, or, in the case of data breaches,[4] regulatory penalties.

Data firm Statista predicts a significant surge in the global cost of cybercrime over the next four years. In response, the cybersecurity market is expected to experience significant revenue growth during the same period.[5] Consider a few statistics. In 2024, the global average cost of a data breach hit a record high of $4.88 million,[6] with some 74% of breaches caused by human error.[7] It also takes an average of 207 days to identify breaches and 277 days to contain

1 Stuart Madnick is the senior accepting editor for this article.

2 The article contributes to the December 2024 Special Issue on "Cybersecurity and Digital Risk." The research for this article was financed by the National Science Centre, Poland (grant number: UMO-2022/45/B/HS4/00965). An earlier version of this article was presented before the International Conference on Information Systems at the MISQE and SIM Academic Workshop on Cybersecurity in Hyderabad, India, in December 2023. We thank the workshop participants for their valuable comments and suggestions for improving the article.

3 According to IBM, a "cyberattack" is "any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device." *What Is a Cyberattack?* IBM, available at https://www.ibm.com/topics/cyber-attack.

4 According to IBM, a "data breach" is "any security incident in which unauthorized parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information)." *What Is a Data Breach?* IBM, available at https://www.ibm.com/topics/data-breach.

5 *Cybersecurity – Worldwide*, Statista, available at https://www.statista.com/outlook/tmo/cybersecurity/worldwide.

6 *Cost of a Data Breach Report 2024*, IBM, available at https://www.ibm.com/reports/data-breach.

7 *2023 Data Breach Investigations Report: Frequency and Cost of Social Engineering Attacks Skyrocket*, Verizon, June 6, 2023, available at https://www.verizon.com/about/news/2023-data-breach-investigations-report.

DOI: 10.17705/2msqe.00110

them.[8] In 2023, a Thomson Reuters survey gathered perspectives from compliance officers and general counsels regarding cybersecurity threats. The findings showed that 50% of companies foresee greater participation from compliance and general counsel in assessing cyber resilience. Additionally, 33% of respondents indicated that they currently receive such information on a monthly basis.[9]

Despite widespread awareness about cyberthreats, the fact that cyberattacks continue to occur and often achieve success suggests that many businesses have inadequate cybersecurity. A potential tool for managing cybersecurity—which simultaneously enables companies to mitigate cyber risk and also cover losses caused by cyberattacks—is "cyber insurance," a specialty insurance product aimed at protecting businesses from risks relating to information technology (IT) infrastructure and activities.

Insurers may thus have an opportunity to improve cybersecurity for their customers, because cyber insurance might incentivize higher levels of both cybersecurity investment and cyber hygiene.[10] Indeed, research shows that insurers expect cyber insurance policyholders to continuously monitor and improve their cybersecurity standards and systems.[11] It is therefore essential to determine if cyber insurance does, indeed, enhance an organization's cybersecurity.

To learn more, we carried out two rounds of in-depth interviews (19 in total). The first was with various experts in the cyber-insurance industry; the second was with active buyers of cyber insurance. The interviews highlighted how cyber insurance can improve a company's cybersecurity, as well as form an important part of a company's broader risk-management strategy.

Our research revealed that cyber insurance is far more than simply a tool for covering claims after a cyber event. Instead, cyber insurance strengthens an organization's cybersecurity during three key phases: (1) the "pre-purchase" phase, by revealing vulnerabilities and areas for improvement during underwriting; (2) the "post-purchase" phase, through continuous monitoring and vulnerability detection; and (3) the "post-attack" phase, by providing emergency insurance assistance and expert IT support in response to an incident. By exploring these stages, this article illustrates how cyber insurance can play a significant role in improving a company's overall cyber-risk management.

The Role of Cyber Insurance in Cybersecurity Governance

Achieving cybersecurity that enables the protection of a company's digital systems, networks and data from a range of threats is a complex and multifaceted challenge—one that requires coordination with various stakeholders.[12] That's why companies are often encouraged to adopt a combination of multistakeholder models, in order to improve their cybersecurity governance.[13]

Experience shows that cyber insurance is an important risk-management tool that can improve cybersecurity governance. Cyber insurance—a financial contract between an insurer and policyholder—is offered primarily by insurance intermediaries; cyber insurance allows organizations to transfer cyber risk to the insurer in exchange for the remuneration included in the insurance premium paid by the policyholder.[14]

The process of purchasing cyber insurance usually begins when a company (the potential policyholder) requests a quote—or when a

8 *Cost of a Data Breach Report 2024*, IBM.

9 DiMauro, J. *Cybersecurity Strategy for a Threatening Landscape*, Thomson Reuters Regulatory Intelligence, available at https://legal.thomsonreuters.com/en/insights/articles/cybersecurity-strategy-for-a-threatening-landscape.

10 Woods, D.W. and Moore, T. "Does insurance have a future in governing cybersecurity?" *IEEE Security & Privacy* (18:1), 2019, pp. 21-27; Camillo, M. "Cyber risk and the changing role of insurance," *Journal of Cyber Policy* (2:1), 2017, 53-63; *Top Tips for Cyber Hygiene to Keep Yourself Safe Online*, Kaspersky, available at https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits. According to Kaspersky, "cyber hygiene" refers to the "steps that users of computers and other devices can take to improve their online security and maintain system health and means adopting a security-centric mindset and habits that help individuals and organizations mitigate potential online breaches."

11 Hatzivasilis, G. et al. *Cyber Insurance of Information Systems*, Conference Paper, March 5, 2021; Böhme, R. and Schwartz, G. *Modeling Cyber-Insurance: Towards a Unifying Framework*, Workshop on the Economics of Information Security, May 21, 2010.

12 Kumar, I. "Emerging threats in cybersecurity: A review article," *International Journal of Applied and Natural Sciences* (1:1), 2023, pp. 1-8.

13 Jayawardane, S., Larik, J., and Jackson, E. *Challenges, Solutions, and Lessons for Effective Global Governance*, The Hague Institute for Global Justice Policy Brief, no. 20, 2015.

14 Hedrick, A. *Cyberinsurance: A Risk Management Tool?* 4th Annual Conference on Information Security Curriculum Development, September 2007, pp. 1-4.

proposal is initiated by an insurance broker or directly by the insurer. When a company wishes to purchase cyber insurance to cover specific risks, it asks the insurer for an offer. From information collected by a broker, the insurer then evaluates the company's cyber-risk exposure. Once complete, the insurer prepares a contract. After that, negotiations between the insurer and the company proceed, often involving a broker. When both parties agree, the contract is finalized and signed.

Later, if the insured cyber incident occurs, the claims' handling process is initiated. The company must inform a cyber-incident manager and activate the insurance policy. Various parties might be involved in this process, such as legal counsel specializing in breach management, as well as forensic investigators; in certain situations, a notice to regulatory authorities (e.g., the Securities and Exchange Commission) may also be required. The insurer then evaluates the situation, based on the gathered information and policy terms, to determine the appropriate payout.[15] In the event of a covered incident, cyber insurance enables the provision of compensation for losses resulting from the attack.[16]

Cyber insurance has advantages and drawbacks. On the plus side, cyber insurance can incentivize security investments and encourage compliance with privacy laws.[17] Cyber insurance also tends to serve as a *de facto* regulator by setting cyber-hygiene standards.[18] Insurers, moreover, expect policyholders to continuously monitor and improve their cybersecurity standards and systems.[19] In these ways, a robust cyber insurance policy can reduce the number of successful cyberattacks by incentivizing policyholders to adopt preventive measures and implement cybersecurity best practices.[20]

On the negative side, cyber insurance may normalize ransomware payments—whereas the goal of cybersecurity is the opposite (to disincentivize such payments, in order to make ransomware less profitable).[21] Other potential negatives with cyber insurance are connected to the status of the contract.[22] For example, challenges emerging before the contract is signed can include an organization's eligibility and the design of the contract itself (such as weak cybersecurity systems, coverage limits and various exclusions). Potential challenges arising after the contract is signed can include self-reporting (which necessitates a significant commitment of time, as well as transparency with the insurer), external-security audits (which can affect premium adjustments) and, of course, an insurer's refusal to pay a claim.[23]

Despite these challenges, the cyber insurance market is growing and is seen as a key component of organizations' cyber-risk management.[24] According to reinsurance firm Munich Re, the global cyber insurance market reached $14 billion in 2023 and will climb to $29 billion by 2027.[25]

About Our Research

We applied a case-study methodology to investigate how companies' cybersecurity can be enhanced by cyber insurance, starting from the process undertaken just before the purchase

15 Vasileiadis, N., Couce Vieira, A., and Baylon, C. "Introduction," in Rios Insua, D., Baylon, C., and Vila, J. (eds.) *Security Risk Models for Cyber Insurance*, Chapman and Hall/CRC, December 19, 2020.

16 Panda, S. et al. *Cyber-Insurance: Past, Present and Future*, Encyclopedia of Cryptography, Security and Privacy, Springer Nature, 2021.

17 Bolot, J. and Lelarge, M. Cyber Insurance as an Incentive for Internet Security, *Managing Information Risk and the Economics of Security*, Springer, 2009, pp. 269-290; Shetty, N. et al. "Competitive cyber-insurance and internet security," in Moore, T., Pym, D. and Ioannidis, C. (eds.) *Economics of Information Security and Privacy*, Springer, 2010; Woods, D., and Simpson, A. "Policy measures and cyber insurance: A framework," *Journal of Cyber Policy* (2:2), 2017, pp. 209-226; Kesan, J.P., and Hayes, C.M. "Strengthening cybersecurity with cyber insurance markets and better risk assessment," *Minnesota Law Review* (102), 2017, pp. 191-276.

18 Camillo, M. "Cyber risk and the changing role of insurance," *Journal of Cyber Policy* (2:1), 2017, pp. 53-63.

19 Hatzivasilis, G. et al. *Cyber Insurance of Information Systems*, Conference Paper, March 5, 2021; Böhme, R. and Schwartz, G. *Modeling Cyber-Insurance: Towards a Unifying Framework*, Workshop on the Economics of Information Security, May 21, 2010.

20 Hayel, Y. and Zhu, Q. *Attack-Aware Cyber Insurance for Risk Sharing in Computer Networks*, Decision and Game Theory for Security: 6th International Conference, 2015, pp. 22-34.

21 Wolff, J. *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware*, Computer Fraud, Data Breaches, and Cyberattacks, MIT Press, 2022.

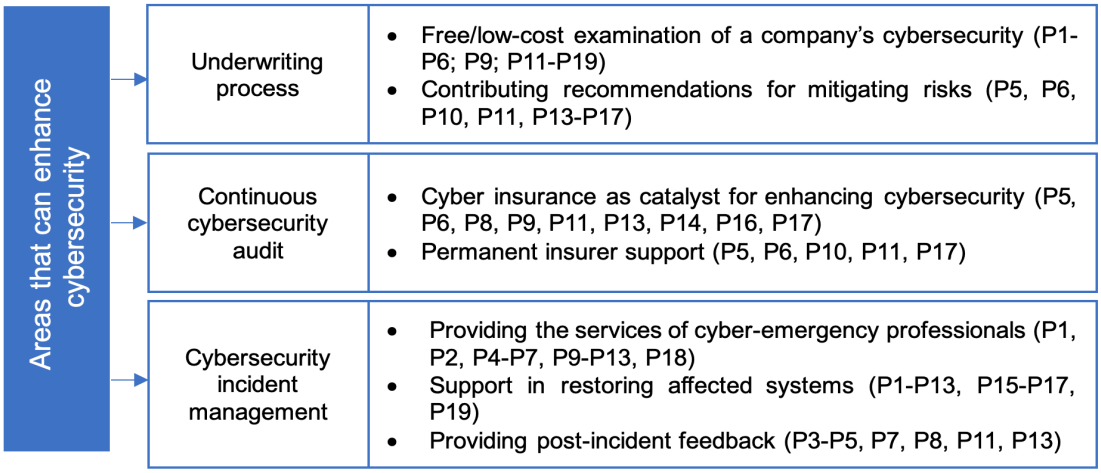
22 Aziz, B. *A Systematic Literature Review of Cyber Insurance Challenges*, International Conference on Information Technology Systems and Innovation, 2020, pp. 357-363.

23 Ibid.

24 Panda, S. et al. "Cyber-insurance: Past, present and future," in S. Jajodia et al. (eds.) *Encyclopedia of Cryptography, Security and Privacy, Springer*, 2021, pp. 1-4.

25 *Cyber Insurance: Risks and Trends 2024*, Munich Re, April 4, 2024, available at https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html?utm_source=chatgpt.com.

Figure 1: Three Areas Where Cyber Insurance Can Enhance a Company's Cybersecurity



of the insurance product and ending with the analysis of the organization's cybersecurity after a cyberattack has occurred. We used multiple sources of evidence, including interview transcripts and archival documents (including insurers' and intermediaries' websites and documents provided by interviewees).[26]

However, the main source of data came from interviews, which were led over two rounds (see Appendix). The first round comprised 11 interviews conducted between October and November 2023, lasting 28 to 60 minutes each. Interviewees were experts in the field of insurance and came from the insurance intermediaries' market—including brokers, underwriters, chief operating officers, directors, insurance company owners and professors.

The second round of interviews took place in September 2024 and comprised six interviews, which each lasted 23 to 36 minutes. Interviewees consisted of company representatives who were involved in the purchase of cyber insurance.

How Does Cyber Insurance Enhance Companies' Cybersecurity?

Our interviews revealed that cyber insurance helps companies transfer some of the financial risk associated with cyber incidents to insurance providers. Less obviously, the interviews also revealed three primary ways that cyber insurance positively impacts a company's cybersecurity (Figure 1).

Demystifying the Cyber Insurance Underwriting Process

Companies seeking cyber insurance must first prove their cybersecurity practices meet stringent standards. An IT data-security officer explained that qualifying for such a policy requires organizations to adopt "very strict cybersecurity requirements" (P17). This requirement ensures that companies evaluate and strengthen their cybersecurity risk profile. A CEO told us: "The very process of preparing to obtain this insurance requires a more comprehensive look at one's security systems" (P18).

The underwriting process begins with a detailed questionnaire from the insurer, designed to collect information on the company's cybersecurity practices, IT infrastructure, data management, incident-response capabilities, regulatory compliance and history of cyber incidents. An associate professor described this stage as a "conscience check" (P2), encouraging companies to confront neglected areas in their security systems. As they answer the insurer's

26 Yin, R. K. *Case Study Research: Design and Methods*, Sage Publications, 2014.

probing questions, organizations may find it necessary to admit that "the area of cybersecurity is neglected" (P2) or that their current measures are insufficient.

After completing the questionnaire, the company submits the necessary documentation to the insurer, including cybersecurity policies, audit reports and IT security assessments. The insurer then reviews this information to evaluate the company's cybersecurity-risk profile and its exposure to potential cyberthreats.

As part of the underwriting process, the insurer often conducts additional tests to better assess the company's cybersecurity position. The associate professor noted: "What is already happening now is that insurers are doing vulnerability testing on a particular customer in terms of whether the insurer wants to accept that customer in the portfolio after all" (P2). This testing involves a range of real-time cybersecurity assessments, including vulnerability scans, penetration testing and checks to ensure that corporate websites and/or customer networks are properly secured against potential threats. A senior underwriter explained, "We're doing a real-time cyber incident and looking at whether, for example, the corporate website or the customer's network is sufficiently secured" (P6).

Based on the information provided, the cyber insurance underwriter evaluates the company's cyber-risk profile. Depending on the assessment, the underwriter can make one of two decisions: accept the company for insurance coverage or provide recommendations for necessary changes to improve cybersecurity. These recommendations guide the company in enhancing its security measures before insurance coverage is granted; these recommendations are, moreover, often provided at no additional charge, offering businesses a roadmap for strengthening their security. For example, a director of financial insurance and reinsurance said:

> *"If, at the moment of underwriting the policy, the policyholder is not yet in the perfect condition that the insurer would like, the policyholder gets an instruction that 'we accept you for insurance coverage, but within six months correct this and that,' and afterwards the insurer checks whether the policyholder has fulfilled its obligations"* (P5).

After this review period, the insurer will revisit the company's cybersecurity measures to ensure the company has addressed its requests. *"This cooperation is very important,"* the aforementioned director emphasized. The senior underwriter added: "If, for example, the customer's networks are not properly secured, they are vulnerable to incidents. Therefore, if a customer takes care of it, they can come back to us and then we will talk again about offering insurance" (P6). In this way, the underwriting process not only helps insurers assess risk, but also encourages businesses to take a proactive approach to cybersecurity.

Unfortunately, after implementing the requests of the insurer, companies sometimes withdraw from applying for cyber insurance due to the misconception that they are now safe and do not need cyber insurance. At other times, companies withdraw their application for insurance because they notice how much effort the underwriting process requires and elect not to apply.

However, by promoting cyber-risk awareness and management, the cyber insurance underwriting process is the first step in encouraging companies to adopt a more proactive approach to cybersecurity. The second important role of cyber insurance in this area is insurers' requirement that companies' continuously strengthen their cybersecurity.

How Cybersecurity Audits Drive Continuous Improvement

Cyber insurance policies require organizations to continuously improve their cybersecurity practices. These policies usually address various aspects of cybersecurity, such as data protection, access control, employee training and cyber-incident response. Employee training, which aims to raise awareness and equip staff with the knowledge needed to follow cybersecurity best practices, is one of the most common requirements of insurers. This training typically includes topics like phishing awareness, password hygiene, social engineering and incident reporting.

If companies lack the resources to implement such initiatives on their own, insurers often step in to provide support. This may include offering employee training or access to specialized services, such as cybersecurity experts, forensic investigators and/or legal counsel. The senior underwriter observed that cooperation with an insurer often involves "building employee awareness … [consisting of] training related to cybersecurity" (P6).

This support might extend beyond training to include discounts or partnerships with cybersecurity providers, enabling organizations to enhance their defenses by installing additional software or accessing expert guidance. The underwriter said:

> *"If a given policyholder signs a contract with an insurance company, then they can expect that within the scope of the insurance, or thanks to insurer negotiated discounts with a cybersecurity specialist, they will be able to increase the level of security. For example, by installing additional software"* (P6).

Another critical role that insurers play involves sharing insights about cybersecurity risks. For instance, insurers may alert organizations to vulnerabilities in commonly used systems, helping companies mitigate potential threats. As a director of cyber practice pointed out, "If we don't share information regarding vulnerabilities and risks, then we will fight alone, and it will simply be a one-man war, and that, in my opinion, will be unwinnable" (P13). This collaboration fosters a more informed, better prepared, cybersecurity community.

Overall, cyber insurance can serve as a catalyst for continuous improvement in cybersecurity by providing organizations with incentives, resources, expertise and insights to enhance their security posture over time. An owner of a consulting company said: "I believe that insurers in general should play the role of those who try to help not only after, but also before, and the whole process of before and after [entering an insurance contract]" (P10). This support ensures that organizations are better equipped to prevent incidents, while also having the support needed to respond effectively when incidents do occur.

Importantly, many businesses view cyber insurance providers' requirements as an opportunity to improve their security practices. As another senior underwriter observed, "Entrepreneurs, noticing the requirements of insurers, are working on and improving their security every year and are becoming more aware of cybersecurity" (P11). This continuous improvement, driven by the integration of cyber insurance into broader risk-management strategies, can positively impact companies' cybersecurity.

How Cyber Insurance Elevates Incident Response and Business Continuity

Cybersecurity incident management refers to the process of identifying, responding to and resolving cybersecurity incidents within an organization. It involves a series of steps designed to minimize damage and restore operations, while learning from each event to improve future resilience. Our interviewees highlighted three stages in managing cyber incidents: accessing the services of cyber-emergency professionals, restoring affected systems and conducting post-incident analysis.

Without cyber insurance, many organizations would struggle to access the cyber-emergency professional services required to handle a significant cyberattack. As a cyber practice leader noted, "It may turn out that a company employs two IT specialists, who are able to take care of all typical problems on a daily basis, but such staff are overwhelmed if malware attacks them and encrypts all their computers" (P8).

In such situations, having immediate access to external expertise is essential. The cyber practice leader added: "The sooner the damage is addressed and mitigation of the consequences is undertaken, the lower the damage will be for the insurer and the lower the costs the insurer will have to pay out" (P8). Insurance companies often provide cyber-incident management services, coordinating efforts with third-party professionals such as cybersecurity firms, forensic experts, legal counsel and PR agencies to ensure a comprehensive response.

The immediate detection and identification of an incident is one of the most crucial aspects

of managing a cyberattack. Early identification is vital because, as a cyber practice leader pointed out, "seconds matter" (P9). As a result, cyber insurers often offer a 24-hour hotline that connects organizations with cyber-emergency professionals who can assess a situation quickly. As the senior underwriter explained:

> *"In the event of an incident, this service will give the customer access to a 24/7 hotline. An expert will first check what exactly happened at the customer's site, what kind of attack or data leak we are dealing with, and then determine a plan of further action to get out of the crisis situation as soon as possible"* (P12).

The next step in managing a cyberattack is to contain the damage. Once the incident is contained, efforts are made to eradicate the root cause of the incident and remove any malware or unauthorized access from the affected systems. After the incident has been resolved, the organization can focus on restoring affected systems and data to normal operations. With the above actions, the company can maintain business continuity, which is achievable through the provision of an additional service in a cyber insurance policy, "cyber incident management."

In the last step of incident management, the insurance company will usually conduct a post-incident analysis to identify areas for improvement. From an organization's perspective, this could involve updating cybersecurity measures, revising incident-response plans and/or providing additional training to staff.

Many of our interviewees emphasized that cyber insurance should be an integral part of a company's cybersecurity framework. Cyber insurance ensures business continuity by minimizing downtime and disruptions; it also provides opportunities for learning and improvement, allowing organizations to strengthen their overall security posture. A chief operating officer explained: "Insurance is one element of building cybersecurity. I am committed to such a 'ten point' classification, where insurance is about 10% of this resilience" (P4). The associate professor added, "Cyber insurance should be viewed as part of enterprise risk management. Meaning it should be seen as an integral, but non-exclusive, part of the process" (P1). Therefore, by offering proactive guidance and post-incident analysis, cyber insurance should "be understood as part of a holistic remedy to cyberthreats" (P4), strengthening long-term resilience and integrating seamlessly into a company's overall risk-management framework.

Recommendations

Focus on the Long-Term Benefits, Not the Short-Term Costs, of the Underwriting Process: Interviewees viewed the complicated cyber insurance policies and the underwriting process for cyber insurance as effort-intensive. A senior broker said: "The underwriting process is quite difficult, complex … [and requires] a large number of answers and information to underwriters' questions … people in the IT area often perceive this as a threat" (P3).

Because IT employees may view insurers' requirements and standards as not worth the effort, an interviewee recommended that the decision-making process regarding the acquisition of cyber insurance should not be simply "transferred to IT specialists" (P3). Additionally, many organizations, particularly small businesses, may hesitate to purchase cyber insurance due to the associated costs and other perceived burdens that will be placed on their IT teams. But if the decision to buy cyber insurance—and responsibility for cybersecurity—involves both IT and non-IT employees, such concerns can be partly mitigated.

In some cases, cyber insurance is also required by a client or investor. Companies should therefore weigh all the long-term benefits of cyber insurance against the short-term costs (premiums, deductibles and compliance). Executives, in particular, should take the time to understand the scope and benefits of cyber insurance, including its coverage options, costs and potential value in mitigating cyber risks. Firms, likewise, should embrace the underwriting process as an opportunity to strengthen their overall cybersecurity framework.

Be Transparent About Cyber Hygiene During the Underwriting Process: Our research shows that the underwriting process for cyber insurance requires companies to demonstrate solid cybersecurity practices, including rigorous data management, timely incident response

and acknowledging any prior cyber incidents. Insurers also conduct vulnerability tests, offering recommendations to improve cybersecurity before coverage is granted. However, some firms find the process too complex and opt out—while others cut corners to get approval faster.

Companies should be transparent during the underwriting process and provide accurate information about their security posture to get appropriate feedback and risk assessments. Companies that are not transparent ultimately hurt themselves by passing up an opportunity for improvement.

Insurers' recommendations should thus be taken seriously and implemented promptly—to both help secure coverage and reduce a company's cyber risks. A senior underwriter told us that insurers' feedback to companies can be very valuable and that "entrepreneurs, in response to the requirements of some insurers, are steadily enhancing their cybersecurity measures year by year" (P11).

An Insurer's Regular Audit is an Opportunity to Strengthen Cybersecurity: Our interviewees noted the fact that cyber insurance policies often require companies to regularly improve their cybersecurity practices through audits, employee training and updated cybersecurity measures. Many insurers provide support for these initiatives, offering resources such as expert consultations and discounts for security tools. Companies should take advantage of insurer-provided resources, including access to cybersecurity experts and training, to stay ahead of constantly changing cyberthreats. Regular cybersecurity audits also help ensure that cybersecurity is an ongoing process, allowing companies to build resilience and adapt to the ever-changing threat landscape.

Treat Cyber Incident Management as the Last "Brick" of the Security System: Interviewees agreed that cyber insurance plays a pivotal role in helping companies manage cybersecurity. Insurers coordinate cyber incident responses by engaging third-party experts, restoring affected systems and conducting post-incident analysis to prevent future attacks. Quick detection and responses are, as noted, crucial for minimizing damage and maintaining business continuity.

While cyber insurance provides valuable support in managing cyber incidents, it should not be seen as a substitute for a strong cybersecurity foundation. Companies should first invest in robust security measures of their own—such as firewalls, intrusion-detection systems, regular security audits and employee training—to reduce the likelihood of attacks. Cyber insurance then serves as a safety net, offering financial protection and expert assistance when preventive measures fail. As a chief operating officer noted, cyber insurance should be "part of a holistic remedy to cyberthreats" (P4).

Concluding Comments

This article sheds light on the pivotal role of cyber insurance in strengthening organizational cybersecurity. Our findings underscore the multifaceted impact of cyber insurance on companies' risk-management strategies. The findings also highlight cyber insurance's potential to mitigate financial losses, while fostering a more proactive approach to cybersecurity.

Interviewees, for example, revealed that cyber insurance supports cyber-risk management not only by paying out claims in the event of a cyber incident; but also by providing incentives to strengthen cybersecurity defense systems and by responding immediately to investigate an incident—and then contain it.

Companies, we also learned, can benefit from going through the underwriting process for an application for cyber insurance, as potential vulnerabilities are discovered and corrective measures are taken. For these reasons, the cybersecurity benefits of cyber insurance extend far beyond its obvious function as insurance.

Appendix 1: Methodology

Interview questions, developed by the authors, are presented in Appendix 2. The questions revolve around factors affecting the development of the cyber insurance market, including barriers and opportunities related to buying cyber insurance, and the perception of cyber insurance among executives.

In this article, qualitative data from 19 interviews was used: 17 interviews were personally conducted and recorded by the authors, while recordings from two online

interviews were used as secondary data sources. From October to November 2023, 11 interviews, lasting 28 to 60 minutes each, were conducted. In September 2024, six interviews, lasting 23 to 36 minutes each, were conducted.

The first group of interviewees were experts in the field of insurance and operated in the insurance intermediaries' market, including brokers, underwriters, chief operating officers, directors, insurance company owners and professors. To validate our results, we turned to the second group of interviewees, which was comprised of company representatives who were involved in the purchase of cyber insurance.

We chose interviewees based in Poland because of the significant interest of potential policyholders in the country in new and innovative solutions and products. Poland has a young financial market that has been developing since 1989, when Poland established independent commercial banking, tax and legal systems to support a market economy.[27]

By focusing on the perspectives of interviewees from Poland who were also experienced in cooperating with multinational companies, we were able to provide recommendations for both businesses around the world and shed light on the challenges faced by companies in Central and Eastern Europe (CEE). As a result, our article enhances the understanding of insurers from the U.S. and Western Europe (the primary providers of cyber insurance products in CEE) of the cyber insurance market in CEE.

All interviews were conducted remotely, then recorded, transcribed and translated into English. Transcripts and translations from Polish into English were checked for accuracy. The interview sessions are summarized in chronological order in Appendix 3, showing interviewee code, job title, industry and the duration of the session.

Interview analysis was conducted with the use of the computerized coding software, MAXQDA. Open, axial and selective coding processes were applied to fit interviewee responses into codes and categories.[28] These processes were used to identify the driving forces behind the purchase of cyber insurance, as well as to identify practices that might enhance organizations' cybersecurity.

Here, we adopted open coding by creating initial codes to identify the main characteristics of the studied material. For example, the initial codes presented detailed information about the role of insurance, such as "permanent insurer support" and "free examination of company's cybersecurity." Next, we applied axial coding to identify relationships between the codes and, then, to combine the codes into sub-categories. For instance, initial codes were combined into the sub-category "underwriting process." In the final stage, we used selective coding to build a meta-category and develop a story, the "role of cyber insurance in fortifying organizational cybersecurity."

Appendix 2: Semi-Structured Interview Questions

1. The European cyber insurance market, compared to the U.S., is just developing. In your opinion, for what reasons have the American cyber insurance market overtaken European markets?
2. What factors determine the development of cyber insurance?
3. 3. What support does the cyber insurance market need to grow?
4. How do you see the future of the European and, especially, the Polish cyber insurance market?
5. Do you think that Polish insurance companies can compete with foreign companies in the context of selling cyber insurance?
6. Do you see any additional barriers related to the development of the cyber insurance market in Poland?
7. Do you think that potential new regulations (e.g., mandatory cyber insurance, mandatory cybersecurity systems) could either slow down or fuel the development of the cyber insurance market in Poland?
8. During a cyber incident, do you think that insurance companies should get involved in the settlement of the damages that have occurred? Should the scope of the service end with the damage valuation and payment of compensation?

27 Ugolini, P. *National Bank of Poland: The Road to Indirect Instruments*, International Monetary Fund, 1996.

28 Strauss, A., and Corbin, J. *Basics of Qualitative Research: Procedures and Techniques for Developing Grounded Theory*, Sage, 1998.

9. Why do businesses decide—or not decide—to purchase cyber insurance? Why do you think customers (businesses) opt out of purchasing cyber insurance?
10. What are your observations regarding the perception of cyber insurance among Polish businesses? In your opinion, is such insurance treated as a cyber-risk mitigation tool—or is it, say, seen as insurance that is necessary when participating in public tenders?

a. In your opinion, what needs to happen to cyber insurance offered in the Polish cyber insurance market to present a greater benefit (value) for the customer?

11. In your opinion, can cyber insurance cause "moral hazard" by causing companies to take more risks around cybersecurity than they otherwise would?
12. Would you like to add anything?

Appendix 3: Interview Sessions

Code	Job title	Profile of interviewee	Industry	Duration
First round of interviews				
P1	Associate Professor	Researcher and expert in regulations for European insurance market at University A	Higher education	39 min., 21 sec.
P2	Associate Professor	Researcher and expert in both insurance market and insurance-product development at University B	Higher education	61 min., 25 sec.
P3	Senior Broker	Responsible for financial and professional lines, provider of risk-management services	Insurance intermediary	33 min., 41 sec.
P4	Chief Operating Officer	Responsible for risk-management information security, personal data security, cybersecurity, business continuity and crisis situations	Consulting	42 min., 14 sec.
P5	Director of Financial Insurance and Reinsurance	Experienced as a senior financial lines underwriter and insurance broker	Insurance	60 min., 58 sec.
P6	Senior Financial Lines Underwriter	Responsible for the underwriting process carried out for financial lines insurance	Insurance intermediary	41 min., 50 sec.
P7	Co-Owner/ Co-Founder of Insurance Company	Leads company X's expansion of its cyber insurance offerings	Insurance	28 min., 16 sec.
P8	Cyber Practice Leader	Leader in insurance company Y	Insurance	25 min., 04 sec.
P9	Cyber Practice Leader	Leader in insurance company Z	Insurance	27 min., 56 sec.
P10	Owner of Consulting Company	Responsible for assistance and claims settlement	Consulting	29 min., 0 sec.
P11	Cyber Senior Underwriter	Responsible for the underwriting process carried out for cyber insurance	Insurance intermediary	60 min., 05 sec.

Code	Job title	Profile of interviewee	Industry	Duration
External interviews—secondary data				
P12	Senior Underwriter	Responsible for the underwriting process carried out for cyber insurance	Insurance intermediary	10 min., 38 sec.
P13	Cyber Practice Director	Responsible for professional services industry, including technology consulting	Consulting	24 min., 32 sec.
Second round of interviews				
P14	Risk Manager	Experienced in purchasing cyber insurance	Financial institution	22 min., 39 sec.
P15	Senior Specialist, IT and Cybersecurity Department	Responsible for company's cybersecurity services, involved in insurance underwriting process and experienced in cyber insurance purchasing	Broadcasting	30 min., 41 sec.
P16	Cybersecurity Lead	Experienced in cybersecurity audit and insurance purchasing	Consulting	25 min., 53 sec.
P17	IT Data Security Officer	Experienced in cyber insurance purchasing	Pharmaceutical industry	35 min., 16 sec.
P18	Chief Executive Officer	Experienced in cybersecurity audit and insurance underwriting	IT security	26 min., 5 sec.
P19	Management Consultant	Experienced in cybersecurity and cyber insurance purchasing	Consulting	22 min., 54 sec.

About the Authors

Wojciech Strzelczyk

Wojciech Strzelczyk (wstrzelczyk@kozminski.edu.pl) is Head of the Finance and Accounting Program at Kozminski University and Assistant Professor in the Department of Accounting and Corporate Governance at the same university. He was Chief Regulatory Officer at the Polish Financial Supervision Authority in the Regulation Development Department. His research interests include performance management and measurement using modern technology tools, IS/IT use in public sector organizations, IS/IT productivity, and cybersecurity. He has published in *Accounting*, *Auditing and Accountability Journal*, *Public Performance & Management Review*, *Information Systems Management*, *Information Technology for Development*, and in the proceedings of EAA and AMCIS, among others.

Karolina Pulawska

Karolina Puławska (kpulawska@wz.uw.edu.pl) is Chief Regulatory Officer at the Polish Financial Supervision Authority in Regulation Development Department and Assistant Professor at University of Warsaw. In December 2019, she has defended Ph.D. thesis entitled "The consequences of bank levy introduction in Europe". In the past, she worked at Kozminski University as an assistant professor, at the National Bank of Poland, in the Ministry of Finance, and Consulting Companies. Currently, her professional and research activities are mainly related to insurance market.