Actuarial Insights on Cyber Risk: Challenges and Opportunities for Today's Economy

by Prof. Dr. Thomas Knispel, Prof. Dr. Matthias Scherer, Prof. Dr. Stefan Weber and Dr. Gabriela Zeller

The cyber insurance market is continuously growing in size and scope – but so is the ubiquitous dependence on information systems and thus overall exposure to cyber risks. A persistent cyber insurance gap – i.e., a discrepancy between potential economic impact and losses covered by insurance – remains. This is due to the complex nature of cyber risks, whose associated losses have distinct statistical characteristics, e.g., non-stationarity, heavy-tailedness, and interdependence, resulting in potential accumulation risk. These stylized statistical properties challenge all aspects of actuarial modeling, from the development of statistical models based on sound technical understanding, over the estimation of those models based on adequate data sets, to the design of insurance policies that are appropriate for the highly dynamic cyber domain. Despite these challenges, the cyber insurance market offers a unique opportunity for advanced analysis – statistical, economical, and societal – and the development of innovative products which allow insurers to grow their business portfolio sustainably and in line with customer expectations, for example with products that go beyond financial compensation and include cyber assistance services.

Despite cyber insurance being a growing market for many years, the existing insurance solutions are still only covering a small share of cyber risk exposures. The resulting cyber insurance gap reveals problems and opportunities: Companies exposed to cyber threats are not yet able to insure their risk to the desired extent and at affordable premiums, while from an insurance perspective potential business opportunities have not yet fully materialized.[1] In this article, we discuss key challenges and opportunities in this market. Mitigating the cyber insurance gap would enable more comprehensive coverage for customers and sustainable growth of the cyber insurance market. In particular, coupling cyber insurance with cyber assistance could create new business opportunities for insurance companies and their partners, and additionally improve overall cyber security and resilience of digital ecosystems.

Core challenges

Cyber challenge 1: High complexity

Modern technical systems are highly complex, especially when they are coupled with digital components for monitoring and control. This insight will become even more important in the future, as the importance of digital and AI-based systems will continue to grow. Complexity is further increased by the fact that digital systems are interconnected within large, dynamic graph structures. They also interact with human agents, whose behavior in the context of social systems can have either a corrective or a disruptive impact on the digital processes. A major source of cyber losses is human misconduct, e.g., as a result of social engineering, deliberate internal and external attacks on the integrity of systems, or simply human error. The structures of digital business processes and supply chain dependencies are equally complex.

This complexity makes it difficult to determine the heterogeneous causes of cyber incidents in both an ex-ante and an ex-post analysis. The development of risk-adequate and underwritable insurance contracts therefore represents a major challenge. The complexity of the cyber ecosystem even raises the question of the extent to which cyber constitutes an insurable risk. The limited efficacy of traditional exclusions, the difficulty in defining and substantiating new terms and conditions, overlap with other insurance products, and particularly the necessity to assess and control accumulation risk, all call into question the overall insurability of cyber risks. In summary, there is still room for significant progress in risk / exposure analysis, product innovation, and pricing to define limits of insurability and tackle the existing cyber insurance gap.

Current developments

The "Allianz Risk Barometer 2024" ranks cyber risks as the top global business risk for 2024 (cited by 36% of all respondents), ahead of business disruption (31%), natural catastrophes (26%), changes of legislation and regulation (19%), and macroeconomic developments (19%).

In 2023, gross written premium in the global cyber insurance market already amounted to USD 14 billion and, according to Munich Re's forecasts, will continue to rise to around USD 29 billion by 2027.

Ransomware is on the rise. Cybersecurity Ventures predicts that ransomware will cost its victims approximately USD 265 billion annually by 2031.[2]

37% of the small and medium-sized companies surveyed in a current Gothaer study[3] assume that the risk of falling victim to a cyber attack will "increase" or "increase significantly" in the next 12 months. Nevertheless, a total of 75% of these companies in Germany have not yet taken out a cyber insurance policy. 44% of the companies surveyed without protection assume that they are not a worthwhile target for cyber attacks.

How can these challenges be addressed? In many cases, traditional approaches to loss data analysis are not sufficient in the cyber insurance context. Instead, a deeper analysis of the underlying mechanisms and risk profiles is essential, which requires detailed engagement with technical experts as well as the development of in-house expertise in cyber security within insurance companies. However, this is extremely difficult to achieve, as the global cyber security workforce gap currently stands at 3.4 million employees.[4] At the same time, it will require the collection of process data on a scale that has not been the norm for most insurance products.

The complexity of the cyber insurance domain is broadly comparable to the intricacies of global financial markets. It accordingly requires comparable amounts of data, data analysis, and faster response times than other insurance business lines. The creation of adequate processes, structures, and expertise depends to a large extent on the capabilities of employees and cooperation partners. In the competition for talents with deep technical expertise, insurers will have to devise a successful strategy with respect to the interplay with technology companies, as both competitors and cooperation partners.

Cyber challenge 2: Dynamic evolution

Digital technologies are evolving rapidly, as are cyber threats and problems associated with these technologies.

Evolutionary processes are subject to this development, and criminal cyber attacks are also an arms race between attackers and defenders. This has three implications:

First, the cyber environment is not static; it evolves rapidly over time within the lifetime of a typical insurance contract. This implies that statistically cumulative losses cannot be represented in the same way as for static or even dynamic, but less complex risks such as NatCat, where the underlying scenarios are locally stationary on the time scale of the insurance contracts.[5] Second, in order to diagnose changes in risk processes in a timely manner, data must be collected continuously and faster than insurance companies are accustomed to and current processes allow. In this sense, cyber risk is more similar to financial market risk than insurance risk. Third, data must be acquired with sufficient granularity to identify and respond to heterogeneous patterns and risk exposures.

However, the status quo is that dynamic and changing cyber risk modeling and consistent premium assessment have not yet been implemented.[6] In addition, data is still not available in sufficient quantity and quality, and it remains unclear how and which data exactly needs to be collected.[7] Documenting and processing collective, representative, and dynamic data in a sophisticated way remains a major challenge. Progress can only be made through data pooling and collaboration. The information available is much less comprehensive than in comparable systems such as financial markets.

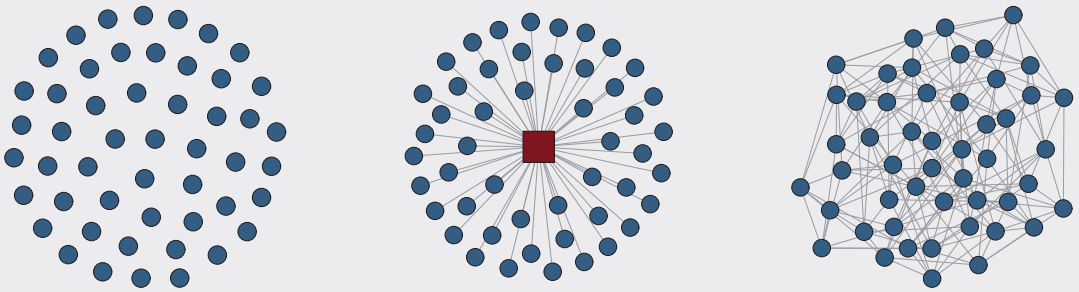
Even if the data challenges were solved, the difficulty of creating an adequate selection of cyber policies would remain. The time scales over which risks and portfolios evolve must be well characterized in order to implement portfolio diversification and risk management. Exposure must be appropriately measured against risk-bearing capacity. At the same time, the risk of a shift in the time scales of evolutionary processes and disruptions must also be taken into account in the concrete specification of policies.

Cyber challenge 3:
Dependence and accumulation of losses

The principle of pooling, or diversification into large collectives of roughly homogeneous and independent risks, is at the heart of the insurance business and the basis of diversification benefits. More specifically, under these assumptions, each collective can be modeled as a producer of independent and identically distributed losses. The structure of the loss-generating mechanism does not change over time. Such a convenient situation is achieved – at least approximatively – by dividing all policyholders into smaller groups that satisfy the necessary homogeneity assumptions. The justification of most classical actuarial modeling paradigms and pricing rules relies on these assumptions, i.e., on the fact that the risks in these subgroups are roughly idiosyncratic.

For cyber risks – and here again the similarity with financial markets becomes apparent – these assumptions generally do not apply. Individuals or organizations are exposed, in addition to idiosyncratic cyber risk like targeted hacker attacks or individual human errors, to both systematic risk and systemic risk: Systematic risk refers to the joint dependence on random background processes, i.e., factors that do not permit full diversification.[8] In financial markets, these might be general market developments or interest rate scenarios. In the area of cyber risk, these include the speed of technological development of cyber security and threats, the timing of failures, and attacks on multiple entities which affect a large number of players. Such inter-

Figure 1. Types of cyber risk



idiosyncratic
(individual risks, e.g., targeted hacker attacks, errors, distortions)

systematic
(common risk factor, e.g., attacks on widely used software or hardware)

systemic
(propagation risks, e.g., viruses, worms, Trojans)

dependencies lead to accumulations of losses, which are also found in natural catastrophes. Unlike NatCat, but analogous to financial markets, the underlying factors for cyber are not stationary, but dynamic and difficult to predict. Systematic data collection and analysis for cyber risks and losses has not yet been sufficiently developed, which is in contrast to the financial markets where a large amount of data is available. As a result, it is very likely that accumulation risk is methodologically underestimated, as illustrated in Zeller and Scherer (2024).

Systemic risks refer to feedback effects caused by local or global interactions. In financial markets, especially in times of crisis, such phenomena play an important role. But they are just as important for cyber risks and losses. In network structures, contagion effects are a real threat, notably through the externalities of behavior, such as decisions to invest in cyber security. Systemic risks also emerge from the interconnectedness of physical-digital systems with other entities, e.g., through supply chains. Appropriate modeling, the right strategies for selecting, collecting, and evaluating relevant data, and the successful design of insurance products are just as important for managing systemic risks as they are for systematic risks.

Various modeling frameworks have been developed for systematic and systemic risk. These include top-down models, e.g., using copulas, and bottom-up models such as factor models, models e.g. based on Cox- or Hawkes processes, or network models.[9] Classical actuarial paradigms will need to be enhanced with models used in financial markets, to adequately tackle the core actuarial tasks of pricing, reserving, and risk management for cyber insurance. In particular, it will be important to benchmark contract durations against time horizons where non-idiosyncratic effects become significant. Irrespective of the modeling approach, however, the fact that data is not yet available in sufficient quantity and quality remains a key challenge that needs to be addressed. Additionally, another important strategy for dealing with accumulation risk is to involve other stakeholders, such as reinsurers, financial markets, or regulators. These can enable data pooling, facilitate risk sharing and alternative risk transfer, and provide appropriate guardrails and backstops.

Cyber challenge 4: Modeling strategic human behavior
Understanding man-made cyber risks requires modeling human behavior. The development of technology is driven by people. Modeling the impact of human error, social engineering, fraud, extortion, and sabotage on systems is especially important. Although these aspects are only a subset of all the mechanisms that cause cyber losses, they can be particularly significant. There may also be disincentives through extortion insurance that increase the scope of cyber extortion. New actuarial approaches are being sought for all these interrelationships. An effective understanding requires an interdisciplinary approach.

Notes

[1] Munich Re's "Global Cyber Risk and Insurance Survey 2022" analyzed why companies do not have cyber insurance in place. Among the respondents (global C-level) without insurance, 29% stated that the price for coverage was too high, 25% did not know that cyber insurance existed, 22% did not understand the product, and 18% perceived the scope of the services/coverage as insufficient.

[2] Cybersecurity Ventures, Global Ransomware Damage Costs To Exceed $265 Billion By 2031, June 4, 2021.

[3] Gothaer Versicherung (2024): KMU-Studie 2024.

[4] Cf. ISC2, Revealing New Opportunities For The Cybersecurity Workforce. For more details regarding the cyber security workforce gap see also, for example, page 16 in Allianz Commercial (2023): "Cyber security trends 2023: The latest threats and risk mitigation best practice – before, during and after a hack".

[5] Climate change is an important issue when adjusting models over time. But climate change takes place on a larger time scale than the duration of contracts. In addition, NatCat scenarios have to be carefully mapped to portfolio losses.

[6] Cf. Section 5 in DAV-Ausschuss Schadenversicherung (2022): "Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen" (Ergebnisbericht).

[7] Cf. Section 4 in DAV-Ausschuss Schadenversicherung (2020): "Daten und Methoden zur Bewertung von Cyberrisiken" (Ergebnisbericht).

[8] Typical drivers of systematic cyber risk include common software and hardware, common cloud systems, common external IT services and cyber security providers, etc.

[9] For a recent survey on modeling and pricing of systematic and systemic cyber risk we refer to Awiszus, Knispel et al. (2023).

[10] The Allianz report on "Cyber security trends 2023" emphasizes that "early detection is key to combating emerging cyber threats" and is crucial to limit the potential loss amount.

[11] DAV-Ausschuss Schadenversicherung (2022): "Use Case der DAV AG Daten und Methoden zur Bewertung von Cyberrisiken" (Ergebnisbericht).

[12] Examples include, e.g., backups, training of employees, and security checks to the existing system.

[13] This includes, e.g., legal advice, help to restore the systems, and IT-forensics.

Game theorists, behavioral economists, psychologists, and computer scientists must all be involved.

The (strategic) interaction of people in the cyber world shows once again that cyber risks have a different dynamic than traditional insurance risks. Models must be capable of representing the time scales involved, and they must also be able to keep pace with the associated dynamic changes in technology and structures. Continuous development and adaptation of the models is necessary to ensure secure pricing and a sustainable cyber insurance business. The complexity of this challenge goes far beyond the requirements of traditional business, such as NatCat. The social dynamics of human actors will be accompanied by a race of AI-methods on the part of threat actors and defenders.

Cyber challenge 5:
Heterogeneous customers and various stakeholders

The significant cyber insurance gap clearly shows that there is still great potential for development. However, product design, risk analysis, and pricing are also complicated by the great heterogeneity of customers. In the corporate segment, the risk exposure, the IT-infrastructure and security, and supply chains are all very individual. A differentiated assessment of the customer's coverage needs and specific risk exposure, especially in case of a complex risk such as cyber, requires a detailed analysis in order to implement tailor-made solutions. Close customer support through cyber assistance services, which can be implemented with partners, is a promising way of dealing with the situation. Cyber assistance expands the insurers' business model, but also offers customers comprehensive risk protection, ranging from improved physical security to financial protection against residual risks. Cyber assistance should be an enabler of better risk data and assessment. Notably, it can also reduce the ambiguity that is a major contributor to the cyber insurance gap.

Cyber risk can be caused by technical processes or human error. But it also involves a strategic level of defenders and attackers who can cause losses.[10] Besides insurers, there are many other players involved: Technology companies, government agencies, regulators of both the insurance business and digital systems and infrastructure. This adds another layer of complexity: the evolution of these players' agendas and regulatory frameworks, in addition to the technical evolution. It is a major challenge to take this into account in product development, risk modeling, portfolio development, and strategic positioning as an insurer. Insurers thus may also play an important role in the further development of cyber security, see Awiszus, Bell et al. (2024), by creating policy conditions and assistance services for customers. So far, however, it must be noted that insurers are not perceived as leading the digitalization agenda, whereas technology companies are. In any case, to expand the cyber insurance business model, insurers need to develop excellent technical and strategic expertise combined with a deep understanding of the regulatory guardrails and to advance their product offerings in this challenging environment.

Opportunities: Business strategies and product design

Classical actuarial approaches

In traditional insurance, collectives are broken down into subgroups with approximately homogeneous insurance claims on the basis of individual characteristics, i.e., suitable covariates. These sub-collectives produce homogeneous and independently distributed losses that are stationary over time. For each subgroup, such a pattern can be modeled, e.g., using a collective risk model, while the decomposition into groups can be achieved using generalized linear models or clustering methods from machine learning. For cyber insurance, an actuarial framework was presented by Zeller and Scherer (2022), which has since been implemented by the Deutsche Aktuarvereinigung Cyber Working Group.[11] Their approach is a preliminary step towards the analysis and pricing of cyber risks. However, firstly, a more comprehensive and reliable implementation requires more exhaustive data than is currently available. Secondly, this modeling approach does not solve another fundamental problem, namely that cyber risks, like financial market risks, are inherently caused by systematic and systemic risks and, as man-made risks, are profoundly influenced by human interaction. Different methodologies and product designs are therefore required, which we will discuss in the next two sections.

Models and products inspired by financial markets

A key characteristic of cyber threats is their evolution over time – as already detailed above. Compared to financial markets, however, the speed of change is generally slower

than in equity markets; the timescales seem more comparable to the fixed income sector, especially credit risks. Credit default swaps are very similar in structure to insurance products, but the financial crisis of 2007/2008, for example, revealed that they are subject to very substantial systematic and systemic risks. A similar conclusion must be drawn for cyber risks. In this respect, cyber models need to be designed accordingly and, in particular, take into account the advances in financial mathematics since 2008, especially in risk analysis and pricing. A high level of transparency and a reduction in the complexity of products are essential to enable broad risk transfer across many market participants. This requires a new dimension of data collection and publication on the one hand, and a new generation of cyber insurance products on the other. Only if this path is taken can a significant expansion of cyber insurance be expected in the long term. Traditional actuarial methods and the associated product range can only support a subset of risks that can be easily assessed in conjunction with risk limits. Such a conservative strategy would perpetuate the cyber insurance gap.

New cyber risk models should focus on the distinct structure of cyber risks. This requires, on the one hand, the identification of relevant covariates in continuous interdisciplinary cooperation with technical experts and, on the other hand, the development of adequate models that reveal risks in a transparent and explainable manner. A great deal of research and development is still required in this area. Structurally, however, methods from the field of financial mathematics can be borrowed. An overview is provided by Awiszus, Knispel et al. (2023). Approaches that are able to capture the dynamic structure of the processes are very promising. For systematic risks, these include Cox processes. In case of systemic risks, a distinction must be made between global and local feedback effects in cyber systems. Global interactions can be described, for example, by Hawkes processes, which, like Cox processes, can also be used to extend collective models, cf. Bessy-Roland et al. (2021) and Hillairet et al. (2023). Local interactions, i.e., the propagation of attributes and contagion in digital networks, are modeled, e.g., by epidemiological models and interacting Markov chains, cf. Fahrenwaldt et al. (2018) and Hillairet et al. (2021). Likewise, an investigation of regulation and strategic interaction in networks - at least in toy models - is necessary to make at the very minimum a qualitative assessment of opportunities and risks, cf. Awiszus, Bell et al. (2023).

Cyber assistance as an enhancement of classical risk transfer

A lack of data means that the dimension of risk is increased by Knightian model uncertainty, which makes the domain

Selected references

Allianz Commercial (2023): “Cyber security trends 2023: The latest threats and risk mitigation best practice – before, during and after a hack”.

Allianz Commercial (2024): “Allianz Risk Barometer: Identifying the major business risks for 2024”.

Awiszus, K., Bell, Y., Lüttringhaus, J., Svindland, G., Voß, A. and S. Weber (2024): “Building resilience in cyber security – An artificial lab approach”. To appear in: Journal of Risk and Insurance, https://doi.org/10.1111/jori.12450

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A. and S. Weber (2023): “Modeling and pricing cyber insurance – Idiosyncratic, systematic, and systemic risks”. In: European Actuarial Journal, 13(1), pp. 1-53.

Bessy-Roland, Y., Boumezoued, A. and C. Hillairet (2021): “Multivariate Hawkes process for cyber insurance”. In: Annals of Actuarial Science 15(1), pp. 14-39.

DAV-Ausschuss Schadenversicherung (2020): “Daten und Methoden zur Bewertung von Cyberrisiken” (Ergebnisbericht).

DAV-Ausschuss Schadenversicherung (2022): “Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen” (Ergebnisbericht).

Dou, W., Tang, W., Wu, X., Qi, L., Xu, X., Zhang, X. and C. Hu. (2020): “An insurance theory based optimal cyber insurance contract against moral hazard”. In: Information Sciences 527, pp. 576–589.

Fahrenwaldt, M.A., Weber, S. and K. Weske (2018): “Pricing of cyber insurance contracts in a network model”. In: ASTIN Bulletin: The Journal of the IAA 48(3), pp. 1175-1218.

Hillairet, C. and O. Lopez (2021): “Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models”. In: Scandinavian Actuarial Journal 8, pp. 671-694.

Hillairet, C., Reveillac, A. and M. Rosenbaum (2023): “An expansion formula for Hawkes processes and application to cyber-insurance derivatives”. In: Stochastic Processes and their Applications 160, pp. 89-119.

Khalili, M., Liu, M. and S. Romanosky (2019): “Embracing and controlling risk dependency in cyber insurance policy underwriting”. In: Journal of Cybersecurity 5(1), pp. 1-16.

Pascu, C., Lourenco, M.B., Scherer, M. and S. Weber (2024): “Cyber insurance - Models and methods and the use of AI”. ENISA Research and Innovation Brief, https://data.europa.eu/doi/10.2824/464473

Zeller, G. and M. Scherer (2022). “A comprehensive model for cyber risk based on marked point processes and its application to insurance”. In: European Actuarial Journal 12(1), pp. 33–85.

Zeller, G. and M. Scherer (2023). “Risk mitigation services in cyber insurance: Optimal contract design and price structure”. In: The Geneva Papers on Risk and Insurance-Issues and Practice 48 (2), pp. 502-547.

Zeller, G. and M. Scherer (2024). “Is accumulation risk in cyber methodically underestimated?” Forthcoming in: European Actuarial Journal.

even harder to approach for insurers rationally exhibiting ambiguity aversion. One possible strategy to mitigate this problem is to work more closely with insurance customers through cyber assistance services. On the one hand, these services can physically reduce cyber risks through better a priori[12] and a posteriori measures[13]. On the other hand, they can decrease Knightian model uncertainty through data collection and a detailed underwriting process, which also enables a valid risk assessment. As players in the digital universe, insurers can help alleviate exposures while providing significantly more coverage for residual risks. Cyber assistance services allow insurers to expand their business model scope while increasing their long-term profitability and reducing risks. Cyber insurance solutions which enhance the classical function of risk transfer by adding risk reduction and better risk assessment through cyber assistance thus have great potential to provide insurers with sustainable growth in the future. The potential design and benefits of such combined insurance products have been theoretically studied e.g. in Dou, Tang, et al. (2020) and Khalili, Liu, et al. (2019).

However, expanding the business model in this direction is not possible without significant investment in expertise and professional skills. Insurers are not typically seen as pioneers of digital development, but rather as players who pick up on and participate in trends. Superior technical expertise is likely to be possible only in partnership with technology companies, with whom these new business models must be developed in a synergistic way. This clearly invokes the question about sharing of costs for service and provision of technological expertise between insurance companies and their customers, a question that has been theoretically investigated in Zeller and Scherer (2023).

Another challenge is to convince customers of the benefits of combining digital security from a physical and monetary perspective. The transfer of internal data for the purpose of risk mitigation and protection must be accepted, and the extent to which this should be done must be analyzed in detail. The legal and regulatory perspective also poses a challenge: For example, what are the legal implications of an insurer‘s involvement in monitoring or (co-)managing the digital security infrastructure, and what level of insurer involvement is desirable and optimal for this business model? Many questions remain to be answered, but it is clear that insurers will only be able to fully tap into the profitable opportunities of the cyber world if cyber assistance is developed as a key building block. This requires a clear business strategy from insurance companies and a massive expansion of technical cyber expertise, but offers a promising path to a clearer view of the insurability of cyber risks, sustainable growth of the cyber insurance market, and a significant contribution to enhanced resilience of cyber ecosystems.

About the authors

→ Prof. Dr. Thomas Knispel
Thomas Knispel is Professor of Mathematics and Statistics at the Berlin School of Economics and Law. Previously he worked in risk management and actuarial consulting. He is a member of the DAV and the DGVFM.

→ Prof. Dr. Matthias Scherer
Matthias Scherer is Professor for Risk and Insurance at Technical University of Munich. He is a member of the board of the DGVFM.

→ Prof. Dr. Stefan Weber
Stefan Weber is Professor of Insurance and Financial Mathematics at the House of Insurance at Leibniz Universität Hannover. He is a member of the board of the DGVFM.

→ Dr. Gabriela Zeller
Gabriela Zeller has previously worked as a scientific researcher at Technical University of Munich, completing her doctoral dissertation on cyber risk and cyber insurance in 2023. She now works in the (re-)insurance industry. She is a member of the DGVFM.