sure[secure] your security operations center × securance

securemag

CYBER INSURANCE AND RISK ASSESSMENT

Operational security reality between underwriting, insurability, and claims experience

Cyber risks as an assessment and market problem

In recent years, cyber risks have become one of the dominant issues in the insurance market. Cyber incidents such as ransomware attacks, data breaches and IT outages is the top global risk for 2025, marking its fourth consecutive year at the top. Ten years ago, cyber risk ranked only #8 globally with just 12% of responses, compared with 38% in 2025.[1] For insurers, this development is reflected in rising claim volumes, volatile claims histories, and an increasing need for differentiated risk selection. For several years now, companies have been confronted with an overall increase in premium levels, more restrictive contract terms, and greater demands on the representability of their cyber risks. Even though there has been a moderate easing of prices in individual market segments and periods, access to insurance coverage remains increasingly dependent on perceived risk maturity.

The assessment of cyber risks faces a structural challenge. Digital infrastructures are highly individual, attack vectors change dynamically, and operational security performance can only be standardized to a limited extent. Nevertheless, the market relies on procedures that enable comparability, scaling, and economic viability. The resulting tension shapes today‘s risk assessment in cyber insurance.

1. Allianz SE, Allianz Risk Barometer 2025, Allianz Commercial, 2025, https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Cyber insurance and underwriting: Scaling up as a structural necessity

Cyber insurance is no longer a niche product, but part of regular risk transfer. At the same time, it remains a relatively young insurance field whose models are still in the consolidation phase. Unlike established lines of business, there is a lack of long-term, stable claims data, while technological developments are continuously changing the risk profile.

According to Munich Re's Cyber Insurance: Risks and Trends 2025, the global cyber insurance market will grow to around USD 16.3 billion by 2025; at the same time, factors such as increasing attack sophistication, supply chain risks, and heterogeneous risk exposures are making underwriting more complex and challenging.[2] These market and risk developments illustrate why scalable yet realistic valuation approaches are necessary.

Insurers are therefore faced with the task of assessing risks in such a way that they are both economically calculable and sufficiently realistic. For companies, this means that insurability is increasingly linked to the ability to describe and classify risks in a comprehensible manner. Risk assessment thus becomes the interface between technical reality and actuarial abstraction.

In practice, standardized risk dialogues form the backbone of underwriting in cyber insurance. They serve as the primary tool for recording technical and organizational security measures and determine whether a risk is underwritten, under what conditions, and with what restrictions.

For underwriters, these dialogues enable structured comparability between very different organizations. For companies, they act as a translation mechanism that converts their own security organization into a format suitable for insurance. The significance of these dialogues extends beyond the initial conclusion of the contract and regularly influences renewals, premium adjustments, and contract modifications.

2. Munich RE, Cyber Insurance: Risks and Trends 2025, https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html

Binary risk dialogues and the loss of operational context

The structure of most risk dialogues is deliberately kept simple. Yes/no queries enable clear classifications, automated scoring models, and consistent risk classes. This simplification is not a methodological shortcoming, but a prerequisite for scaling in underwriting.

At the same time, this logic creates systemic limitations. Security measures are classified as present or absent without reflecting their scope, quality, or operational integration. For companies, this means that complex security architectures are reduced to a few decision-making characteristics that only allow limited conclusions to be drawn about actual resilience.

This abstraction is inherent to insurance-based risk management. Analyses by the OECD (Organisation for Economic Co-operation and Development) point out that insurance models necessarily rely on simplified representations of complex risk realities in order to remain comparable and economically viable. While such abstraction enables insurability and scalability, it also implies that certain qualitative aspects of risk cannot be fully captured through standardized assessment mechanisms.[3]

The loss of context is particularly evident in individual security-critical measures. The query regarding the use of multi-factor authentication is a prime example of this.[4] While the formal answer appears clear, it remains unclear for which systems, user groups, and access scenarios this measure actually applies.

In practice, hybrid states often exist: MFA is partially implemented, except for legacy systems or certain operational roles. These distinctions can hardly be reflected in binary queries. The risk assessment is therefore based on an abstract picture of the security situation, which provides only limited visibility of both risks and existing levels of maturity.

3. OECD, Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, 2022 https://www.oecd.org/finance/insurance/cyber-risk-insurance.html

4. ENISA, Guidelines on Multi-Factor Authentication, European Union Agency for Cybersecurity, 2022 https://www.enisa.europa.eu/publications/multi-factor-authentication

Self-disclosure, loss history, and operational effectiveness

For years, insurers and supervisory authorities have been pointing out that successful cyber-attacks often take place in environments that have implemented formal security measures.[5] The decisive factor here is not the existence of individual controls, but their resilience in operational use.

This creates structural uncertainty for risk assessment. Self-disclosures reflect the intended state, while damage experiences reveal operational weaknesses that were not previously visible. This discrepancy has a direct impact on loss ratios and premium models.

Operational effectiveness encompasses aspects such as detection capability, response speed, and decision-making ability under time pressure.[6] These factors are crucial for the actual loss experience but are difficult to measure in a standardized way.

This poses a methodological problem for underwriters. Collecting such information is time-consuming, requires interpretation, and is only scalable to a limited extent. For companies, this means that a high level of operational security does not automatically translate into a more differentiated risk rating.

5. Federal Office for Information Security, The State of IT Security in Germany 2023, BSI, 2023 https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lageberichte/lageberichte_node.html

6. ENISA, ENISA Threat Landscape 2023, European Union Agency for Cybersecurity, 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

The role of security expertise in risk classification

In this context, security expertise acts as a connecting element between formal queries and operational reality. This perspective aligns with Gartner's assessment that meaningful cyber risk quantification requires contextual interpretation beyond control checklists.[7] It enables security measures to be classified in their technical, organizational, and operational context.

This expertise can be anchored at different levels: within the organization, at specialized service providers, or on the part of the insurer. However, its integration has so far been selective, for example in the case of complex risks or high sums insured. Comprehensive standardization is still pending.

7. Gartner, Market Guide for Cyber Risk Quantification, Gartner Research, 2023

Operational signals as a supplement to formal risk assessment

In addition to formal information, there is a wealth of operational information available that allows conclusions to be drawn about the effectiveness of security measures. This includes findings from security operations, documented incident response procedures, external attack surface analyses, and the results of technical audits.[8]

These signals often already exist but have so far only been integrated into risk assessment on a selective basis. Their structured integration opens the possibility of classifying risks in a more differentiated manner without replacing formal risk dialogues.

8. IBM Security, Cost of a Data Breach Report 2023, IBM, 2023 https://www.ibm.com/security/data-breach

DO YOU ASSESS OR ASSUME CYBER RISKS?

A classification based on evidence for underwriting and firms

Cyber risks are predominantly assessed in underwriting through structured risk dialogues. This approach is established, scalable, and forms the basis for comparable risk classifications. At the same time, market analyses and scientific studies show that standardized questionnaires only reflect part of the actual risk reality. A significant portion of risk assessment is therefore inevitably based on assumptions and proxy indicators.

The European Cybersecurity Agency points out that there is currently no uniform, cross-market language for assessing cyber risks. In practice, this means that identical questionnaire responses can conceal very different operational security levels. Risk dialogues thus provide a necessary but not sufficient basis for a robust risk assessment.[9]

From a risk management perspective, this gap can be described precisely. Frameworks such as the NIST (National Institute of Standards and Technology) Cybersecurity Framework and the Risk Management Framework define risk assessment not as a one-time survey of controls, but as a continuous process of identification, evaluation, review, and monitoring. Applied to cyber insurance, this means that a purely declarative recording of security measures structurally lags an evidence-based assessment.[10]

International regulatory and market analyses confirm this perspective. The International Association of Insurance Supervisors explicitly describes cyber underwriting as a data- and evidence-dependent process in which uncertainties arise where operational effectiveness cannot be verified. In these cases, underwriters inevitably resort to assumptions to maintain their decision-making ability.[11]

Against this backdrop, the question is not one of either/or. In practice, a robust risk classification emerges where assumptions are systematically reduced. This is achieved by combining formal risk dialogues with supplementary evidence that makes the operation, coverage, and responsiveness of security measures visible. Such an approach does not follow a new methodology but rather applies established principles of evidence-based risk assessment to the insurance context.

A practical model can be described as multidimensional risk triangulation. The risk dialogue continues to form the scalable entry point. This is supplemented by operational evidence and technical signals that classify and clarify formal information. External perspectives on attack surfaces and exposure complete the picture without acting as isolated predictors of damage.[12]

This shifts the nature of risk assessment. It is no longer based exclusively on assumptions about implemented measures, but increasingly on the verifiable effectiveness of these measures in operational use. For underwriters, this means a reduction in structural uncertainty. For companies, it creates transparency about which aspects of their security organization are actually relevant to risk.

9. ENISA, Recommendations on Cyber Insurance – Commonality of risk assessment language in cyber insurance, European Union Agency for Cybersecurity, 2017 https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-3-2%201%20Recommendations%20on%20Cyber%20Insurance.pdf

10. NIST, Cybersecurity Framework (CSF 2.0) – Overview, National Institute of Standards and Technology, continuously maintained https://www.nist.gov/cyberframework & https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

11. IAIS, Cyber Risk Underwriting – Identified Challenges and Supervisory Considerations for Sustainable Market Development, International Association of Insurance Supervisors, 2020 https://www.iais.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf

12. Gallagher Re, Looking from the Outside-In: Outside-In Data, Gallagher Re, n.d. https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/gallagher-re-cyberiq-outside-in-data.pdf

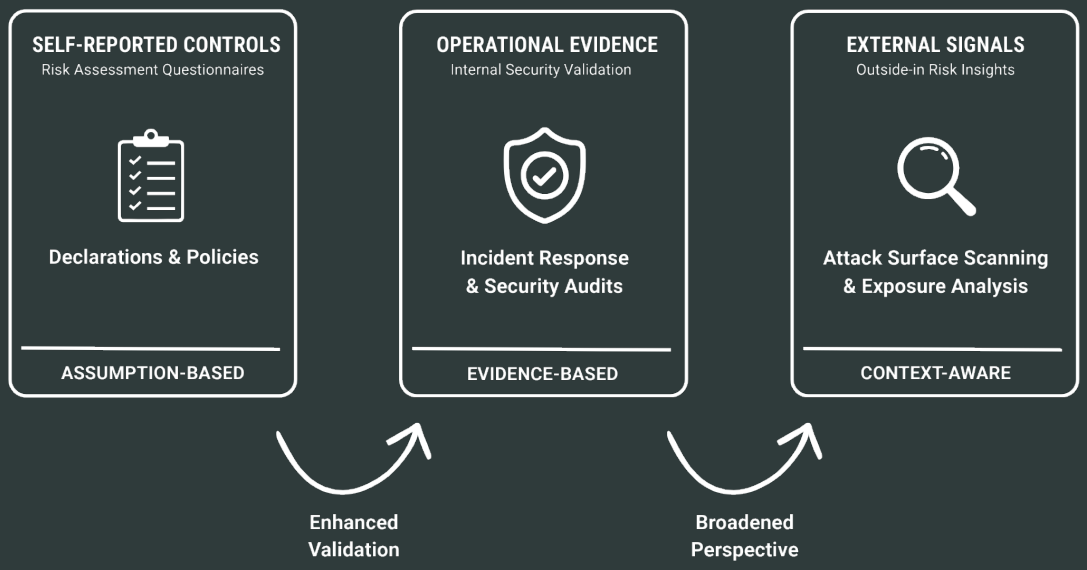
From assumption to assessment - a combined assessment approach

In practice, it has been shown that reliable cyber risk assessments are not based on a single instrument. Rather, meaningful insights are gained by combining several perspectives:

- **Risk dialogues** provide a scalable record of formal security measures and governance structures.
- **Operational evidence** from security operations and incident response shows whether these measures are effective in everyday life.
- **Outside-in signals** supplement the view with external exposure and attack surfaces, without serving as isolated risk forecasts.
- **Audit and assessment results** place technical controls in the overall context of the security architecture.

This approach follows established principles of evidence-based risk management and reduces assumptions where damage relevance and uncertainty are particularly high.

Evidence-Based Cyber Risk Evaluation



Implications for insurers, underwriters, and companies

For underwriters, this development offers the opportunity to differentiate risks in a more granular way. At the same time, the complexity of the assessment increases, as qualitative information must be interpreted and made comparable. The challenge is to integrate additional signals in a way that does not undermine scalability and consistency.

In the long term, there are signs of a shift from purely formal to more evidence-based assessment models, especially in segments with high exposure to damage.

For companies, the visibility of their own security organization is becoming more important. Insurability is determined less by individual measures than by the traceability of their implementation and operation. The way in which security performance is documented and communicated is therefore becoming increasingly important.

Conclusion and classification

Risk assessment in cyber insurance is undergoing change. Standardized queries remain a key tool, but they have their limits when it comes to reflecting operational reality. Supplementary signals and security expertise enable a more realistic classification without fundamentally questioning existing models.

Cyber insurance is increasingly becoming a reflection of organizational resilience. This creates a common frame of reference for insurers, underwriters, and companies, linking security reality, insurability, and economic viability.

Podcast

In an episode of Counder Conversation, Michel Weiss, Founding Partner & CEO, speaks with Andreas Papadaniil, CEO of suresecure and founder of securance, about the evolving reality of cyber risk. The discussion illustrates how ransomware, CEO fraud, and AI-driven attacks have become material insurable risks, and why cyber insurance increasingly depends on operational effectiveness, response capability, and verifiable resilience rather than declared controls alone.

YouTube

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Phone: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.eu

securance GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Phone: +49 (0) 2156 97 49 110

E-Mail: kontakt@securance.de
Web: www.securance.de