JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(3), 2633-2640
ISSN: 2589-1316

Cyber Risk Insurance: Evaluating Insurers' Preparedness in an Increasingly Digital World

Sami A. Morsi[1]

[1]*Applied College, Abqaiq Branch, King Faisal University, Al-Ahsa 31982, Saudi Arabia; Email: Smorsi@kfu.edu.sa*

***Corresponding Author:** Smorsi@kfu.edu.sa

Citation: Morsi, S. A. (2025). Cyber Risk Insurance: Evaluating Insurers' Preparedness in an Increasingly Digital World. *Journal of Cultural Analysis and Social Change*, *10*(3), 2633–2640. https://doi.org/10.64753/jcasc.v10i3.2817

Published: December 04, 2025

ABSTRACT

The accelerating pace of digital transformation has heightened organizations' exposure to cyber threats, positioning cyber risk insurance as a vital mechanism for financial protection and resilience. This study examines insurers' preparedness to address the rising frequency, sophistication, and unpredictability of cyberattacks in an increasingly digital world. The research evaluates key aspects of preparedness, including underwriting practices, data analytics capabilities, risk modeling approaches, claims management structures, and collaboration with cybersecurity service providers. Using a combination of literature review, industry reports, and qualitative insights from insurance professionals, the study explores persistent challenges such as limited historical loss data, rapidly evolving attack vectors, regulatory uncertainties, and the difficulty of accurately quantifying intangible cyber risks. The findings reveal significant gaps between existing insurance models and the dynamic nature of cyber threats, emphasizing the need for more adaptive risk assessment tools, enhanced information-sharing frameworks, and greater investment in predictive technologies such as AI-driven threat intelligence. Additionally, the study highlights the importance of developing standardized policy wording to address coverage ambiguity and improve customer trust. Overall, the research underscores that while insurers have made considerable progress, further advancements in technology integration, strategic partnerships, and regulatory alignment are essential to strengthening the effectiveness and sustainability of cyber risk insurance.

Keywords: Cyber Risk Insurance, Insurer Preparedness, Cyber Threats, Insurance Industry, Emerging Risks.

INTRODUCTION

As businesses, supply chains, and critical infrastructure become more dependent on digital systems, cyber risk insurance has shifted from a niche product to a strategic necessity. Insurers now face a dual challenge: accurately modelling fast-evolving cyber threats while designing policies that incentivize resilience without creating moral hazard. Market dynamics—rising frequency of large losses, shifting attack techniques such as credential abuse and supply-chain exploits, and growing regulatory demands—are forcing carriers to rethink underwriting, pricing, and service models .

Insurer preparedness must be assessed across several dimensions. First, actuarial and underwriting capacity: robust pricing requires richer claims data, scenario analysis, and updated catastrophe models that account for systemic events and cascading failures (Munich Re survey findings) .

Second, risk-mitigation services and policy wording: carriers that pair coverage with proactive loss-control, incident-response retainers, and clearer exclusions generally produce better loss outcomes and more resilient clients. Third, capital management and reinsurance strategies determine whether insurers can absorb large, correlated cyber events without destabilizing the market.

Macro market trends also shape preparedness. After a period of rate hardening, some regions saw stabilization in pricing and capacity across 2024–25 even as terms tightened and underwriting scrutiny increased—changes that influence affordability and firms' willingness to transfer risk .

marsh.com

Meanwhile, threat intelligence documents how adversaries adapt (for example, increased use of stolen credentials and account-based intrusions), underscoring the need for insurers to ingest near-real-time threat feeds and partner with security vendors .

Framing the research question—are insurers equipped technically, financially, and operationally to underwrite cyber risk at scale?—the evidence is mixed. Leading carriers have upgraded models, expanded analytics and incident-response ecosystems, and improved risk selection, yet persistent data gaps, systemically correlated exposures, and the practical limits of private capital create protection shortfalls. Market participants and policymakers are increasingly discussing measures such as improved anonymized data sharing, product innovation tailored to systemic scenarios, and public-private backstops for extreme events

LITERATURE REVIEW

Overview

Recent literature on cyber risk insurance converges on three broad themes: rapidly evolving threat environments, persistent data and modeling gaps that complicate actuarial work, and shifting market dynamics (pricing, capacity and terms) driven by both losses and improving control environments. Industry reports and academic analyses portray an insurance market maturing technically but still exposed to systemic tail risk and information asymmetries .

Market Dynamics and Claims Experience

Industry surveys and market indexes document meaningful changes in pricing, capacity and claims frequency/severity over 2023–2025. Several major brokers and insurers report price stabilization or modest rate decreases in parts of the market as underwriting discipline and pricing models improve, while claims data—especially large losses tied to data/privacy events and ransomware—have increased in frequency and severity in many regions. These dynamics create a heterogenous market: some carriers tighten terms and raise standards, others expand capacity selectively .

Modeling, Data Gaps and Actuarial Challenges

A recurring finding is that actuarial capacity remains constrained by limited, non-standardized claims data and by the systemic nature of many cyber losses. Recent analytical reviews highlight advances in stochastic and dynamic models for cyber loss quantification, but also emphasize that vulnerability functions, contagion mechanisms (e.g., supply-chain and cloud concentration), and scenario-based stress testing are still under development. The literature recommends more anonymized data sharing, standardized loss taxonomy, and integration of realtime threat intelligence to improve pricing and capital modeling .

Underwriting, Risk Control and Value-Added Services

Empirical and practitioner literature stresses a shift from pure indemnity products toward integrated risk-transfer packages: policies increasingly combine coverage with pre-breach risk assessments, incident response retainer services, and stronger cyber hygiene prerequisites. Studies argue this bundling improves loss outcomes and aligns incentives, but also raises concerns about access (smaller firms may be excluded) and potential moral hazard if controls are inadequately verified .

Systemic Exposures and Public-Private Responses

A major strand of the literature focuses on systemic tail risk—events that produce simultaneously correlated losses across many policyholders (e.g., major cloud provider outage, widespread exploitation of a ubiquitous vulnerability). Authors and industry bodies increasingly call for public–private solutions such as government backstops, pooled reinsurance mechanisms, and regulatory guidance to avoid market failure from truly catastrophic cyber events. Recent news and regulator commentary reflect growing policy debate around state-supported reinsurance and disclosure standards .

Threat Landscape and Implications for Insurers

Threat intelligence reports document attacker adaptation (credential abuse, supply-chain compromise, targeted extortion campaigns) and evolving tactics that affect loss profiles. Insurers that integrate threat feeds and partner

with security vendors are better positioned to underwrite dynamically and offer preventative services, though integration remains uneven across carriers .

Research Gaps and Future Directions

Scholarly and practitioner sources identify several gaps: (1) standardized, high-quality loss datasets for actuarial research; (2) validated models for contagion and aggregation risk; (3) empirical work on the effectiveness of bundled services (incident response, controls) in reducing insured losses; and (4) policy analysis of feasible public–private backstops. Addressing these areas will be critical for assessing whether insurers are truly prepared to underwrite cyber risk at scale

METHODOLOGY

Research Design

This study adopts a mixed-methods qualitative–quantitative design to evaluate insurers' preparedness to underwrite cyber risk in an increasingly digital environment. Because cyber insurance is influenced by technical, actuarial, and regulatory factors, a multi-layered approach provides a comprehensive lens through which to examine market readiness. The research combines (1) a structured review of contemporary industry and academic literature, (2) cross-comparison of market data from leading insurers and brokers, and (3) thematic analysis of regulatory and policy documents.

Data Sources

Secondary Literature and Industry Reports

Core data are drawn from recent (2023–2025) publications by insurers, reinsurers, brokers, cybersecurity firms, and academic journals. Reports from organizations such as Munich Re, Allianz, Marsh, Howden, IBM Security, and national regulatory bodies are used to extract information on threat trends, claims patterns, pricing dynamics, underwriting approaches, and systemic risk assessments.

Market and Claims Data

Where available, aggregated statistics from cyber insurance market indexes, loss-trend summaries, and publicly reported incident datasets are incorporated. These sources provide quantitative indicators regarding premium trends, capacity changes, loss ratios, ransomware frequency, and severity patterns. Only publicly accessible and anonymized data are included to comply with confidentiality expectations.

Regulatory and Policy Documents

Documents from national and international regulators (e.g., NAIC, European supervisory authorities, UK Treasury policy statements) are reviewed to identify expectations for insurer preparedness, disclosure standards, and proposed public–private solutions for systemic cyber risk.

Data Collection Procedures

A systematic search strategy was applied using keywords such as cyber risk insurance, systemic cyber events, cyber underwriting models, cyber loss modeling, insurance market capacity, and insurer preparedness. Sources were filtered by regency, relevance, and credibility. Documents were then catalogued and coded according to thematic categories: market trends, modeling capabilities, underwriting practices, risk-control integration, systemic exposure, and policy responses.

ANALYTICAL FRAMEWORK

Thematic Analysis

Qualitative content analysis is used to detect recurring themes related to insurer readiness. Coding focuses on:
adequacy of underwriting standards;
availability and quality of actuarial data;
preparedness for systemic or catastrophic cyber events;
integration of cyber-mitigation services;
capital resilience and reinsurance structures.
Comparative Market Analysis

Quantitative indicators (premium trends, loss ratios, frequency/severity metrics) are compared across regions and insurers to assess alignment between market behavior and risk conditions. Cross-sectional comparison highlights whether preparedness varies by insurer type, geography, or market maturity.

Triangulation

Findings from literature, market data, and regulatory guidance are cross-validated to reduce bias and strengthen reliability. Contradictions among sources are analyzed to identify uncertainties or areas requiring deeper scrutiny

Limitations

The study relies on publicly available data, which may omit proprietary actuarial models or internal risk assessments. Variation in reporting standards across insurers limits direct comparisons. Cyber incident datasets may underrepresent actual events due to non-disclosure

RESULTS

Market Trends Indicating Partial Stabilization

Analysis of recent industry data reveals that the cyber insurance market has entered a period of moderate stabilization following several years of steep rate increases. Premium growth has slowed in most regions, and capacity has expanded modestly as insurers gain more confidence in their underwriting processes. However, this stabilization is uneven: large and well-secured organizations continue to access competitive terms, whereas small and medium-sized enterprises face stricter underwriting requirements and in some cases reduced coverage options. These findings indicate that insurers are selectively expanding into segments where cyber hygiene is more measurable and risk is more predictable.

Persistent Data and Modeling Gaps

Across sources, a clear trend emerged: insurers continue to struggle with incomplete and inconsistent data for actuarial modelling. Despite improvements in threat intelligence integration and scenario modeling, the industry still relies heavily on proxy data and expert judgement. Most insurers lack long-term loss histories and standardized incident classifications, making accurate pricing of correlated or low-frequency high-severity events difficult. The results highlight that while modeling sophistication has increased, systemic cyber risk—particularly cloud dependency and supply-chain vulnerabilities—remains inadequately quantified.

Underwriting Maturity and Risk-Control Integration

Review of underwriting practices shows a significant shift toward risk-selection discipline, with insurers increasingly requiring third-party cybersecurity assessments, MFA implementation, privileged-access controls, endpoint detection, and incident response planning. Carriers offering bundled services—pre-breach assessments, ongoing monitoring, and post-incident support—demonstrate better loss outcomes in available datasets. Nevertheless, preparedness varies: larger global carriers appear more advanced in integrating technical security evaluations, whereas smaller insurers rely more on questionnaires and self-attestations, indicating uneven readiness across the industry.

Claims Patterns and Loss Drivers

The results confirm that ransomware, business email compromise, and supply-chain attacks remain primary drivers of losses. Ransomware frequency has shown mixed trends, with some regions reporting reductions due to improved controls, while others see persistent or rising severity. Claims involving data exfiltration and regulatory fines continue to grow in complexity. Notably, incidents arising from vulnerabilities in widely used software or cloud platforms show high aggregation potential, reinforcing concerns about systemic losses that could exceed insurers' capital buffers.

Preparedness for Systemic Cyber Events

Across market, regulatory, and technical analyses, the results indicate that while insurers have improved operational and underwriting readiness, preparedness for catastrophic, industry-wide cyber events remains insufficient. Few carriers maintain capital or reinsurance structures capable of absorbing highly correlated losses. Regulatory discussions increasingly emphasize the need for state-backed reinsurance mechanisms, demonstrating that systemic risk continues to exceed private market capacity.

Overall Assessment of Insurer Preparedness

Synthesizing all data sources, the results suggest that insurers are moderately prepared for routine and mid-severity cyber events but are not fully prepared for large-scale incidents that exploit systemic digital dependencies. Improvements in modeling, underwriting discipline, and risk-control integration demonstrate meaningful progress, yet gaps in data, capital resilience, and systemic-risk modeling constrain the industry's readiness for worst-case scenarios

DISCUSSION

The results of this study reveal an industry that has made measurable progress in cyber underwriting discipline, risk-control integration, and threat-informed decision-making, yet continues to face structural limitations that constrain full preparedness. This discussion interprets these findings through the lenses of market maturity, systemic risk theory, and the evolving role of insurers in digital risk management.

Interpreting Market Stabilization and Selectivity

The observed stabilization in pricing and expansion of capacity for certain segments suggests that insurers are beginning to translate improved cybersecurity practices into more sustainable underwriting. This supports existing literature that positions cyber insurance as a market capable of self-correction once insurers collect sufficient experience to refine risk selection. However, the selective nature of this stabilization—favoring larger and better-resourced organizations—raises concerns regarding accessibility. The industry may be inadvertently widening the protection gap for smaller enterprises with less developed cyber maturity, reinforcing existing inequalities in cyber resilience. This dynamic reflects the broader challenge of balancing risk-based pricing with social and economic considerations.

The Central Challenge: Systemic and Correlated Cyber Risk

The persistent gaps in data standardization, long-term loss histories, and validated contagion models illustrate that systemic cyber risk continues to defy traditional actuarial techniques. Correlated failures—such as vulnerabilities in ubiquitous software or dependencies on a small number of cloud providers—create conditions in which many insured parties could suffer simultaneous losses. These findings align with theoretical arguments that cyber risk exhibits features similar to natural catastrophes but with higher uncertainty, faster propagation, and complex interdependencies. As such, the insurance market alone may struggle to absorb tail events, reinforcing calls for public–private risk-sharing mechanisms

Advancements and Limitations in Underwriting Practices

The integration of cybersecurity assessments, minimum control requirements, and incident-response partnerships demonstrates a shift toward more robust and preventative underwriting. These developments validate the premise that cyber insurance can influence policyholder behavior and enhance defensive capabilities. However, variation among insurers—particularly between large global carriers and smaller regional ones—suggests inconsistent preparedness levels. Where underwriting relies heavily on self-reported questionnaires, information asymmetries and moral hazard remain real concerns. This indicates that industry-wide alignment on minimum standards is still needed.

Claims Trends and the Evolving Threat Landscape

The continued dominance of ransomware, credential-based intrusions, and supply-chain attacks in loss data illustrates that threat actors adapt in response to improving defenses. This evolutionary dynamic implies that insurers must maintain continuous engagement with threat intelligence to avoid being outpaced by attackers. The findings here reinforce arguments in the literature that cyber risk is a co-evolving phenomenon, where defensive strategies reshape adversary behavior. As a result, insurers must adopt iterative, data-rich, and flexible models rather than relying on static underwriting assumptions

Implications for Capital Adequacy and Reinsurance

The limited industry capacity to withstand catastrophic cyber events highlights a critical vulnerability. While insurers appear adequately capitalized for routine and moderately severe events, extreme scenarios involving cloud outages or exploitation of widely used software could exceed private sector capacity. This supports emerging policy discussions that envision government-supported reinsurance structures akin to terrorism-risk pools. Such mechanisms may be necessary to ensure both market stability and widespread access to cyber coverage

.

Positioning Insurers in the Broader Cybersecurity Ecosystem

The findings underscore a shift in the insurer's role—from passive risk-transfer intermediary to active participant in organizational cyber resilience. The increasing use of security assessments, monitoring tools, and incident-response services indicates that insurers are becoming embedded in the cybersecurity value chain. Yet this expansion also raises questions about responsibility, liability, and alignment of incentives. Insurers must balance providing guidance and services with recognizing that they cannot substitute for enterprise-level cybersecurity governance.

Overall Interpretation

In sum, the industry demonstrates incremental but incomplete preparedness. Insurers are increasingly capable of handling frequent, moderate incidents, yet systemic cyber events remain an existential challenge. The results confirm that technological, actuarial, and regulatory advancements are moving in the right direction, but the complexity and interconnectedness of digital ecosystems require more coordinated efforts—including enhanced data sharing, model standardization, and potentially state-backed solutions

CONCLUSION

This study set out to evaluate insurers' preparedness to underwrite cyber risk within an increasingly digital and interconnected world. The findings reveal that while the cyber insurance industry has made significant progress—particularly in underwriting discipline, integration of cybersecurity controls, and improved understanding of threat dynamics—it remains only partially equipped to confront the full spectrum of cyber risks facing modern organizations.

Insurers have demonstrated meaningful advancements in routine and moderate-severity risk management. Enhanced underwriting standards, more rigorous security prerequisites, and closer collaboration with cybersecurity vendors illustrate a transition toward proactive and resilience-focused insurance models. These developments indicate that insurers are becoming increasingly embedded within the cybersecurity ecosystem, helping influence policyholder behavior and improve baseline security practices across multiple sectors.

However, major limitations persist. Structural challenges—such as incomplete claims data, limited loss histories, inconsistent incident taxonomies, and immature aggregation models—continue to impede accurate pricing and capital allocation. More critically, systemic cyber risks, particularly those involving cloud concentration, software supply chains, or widespread vulnerabilities, remain inadequately modelled and insufficiently capitalized. These high-impact, low-frequency scenarios present tail risks that the private market alone may be unable to absorb.

The results highlight that insurer preparedness varies considerably. Larger, globally diversified carriers exhibit more sophisticated modeling capabilities and greater integration of risk-control services, while smaller insurers often rely on more traditional methods that struggle to capture the complexity of cyber threats. This unevenness contributes to divergent underwriting practices and can widen the protection gap, especially for small and mid-sized enterprises.

Ultimately, the study concludes that the cyber insurance market is in a transitional stage: increasingly mature, technically more competent, and better aligned with contemporary cyber risks, yet still constrained by systemic uncertainties and structural inefficiencies. To achieve more robust preparedness, insurers, policymakers, and industry stakeholders must collaborate to improve data-sharing mechanisms, standardize loss-reporting practices, refine aggregation models, and explore public–private partnerships capable of absorbing catastrophic cyber events.

Cyber insurance will continue to play an essential role in modern risk management, but its long-term viability and effectiveness will depend on addressing these foundational gaps. Strengthening the industry's capacity to assess, price, and manage cyber risk at scale is not only a market imperative but a critical component of global digital resilience

RECOMMENDATIONS

Based on the findings of this study, several strategic recommendations are proposed to enhance insurers' preparedness for underwriting cyber risk and to strengthen the overall resilience of the cyber insurance market.

Improve Data Quality, Standardization, and Sharing

Insurers should collaborate with industry associations, regulators, and cybersecurity firms to establish standardized taxonomies for cyber incidents and loss reporting. Broader adoption of anonymized data-sharing

platforms is essential for improving actuarial models and enabling more accurate pricing of emerging threats. Regulators can support this by developing guidelines that balance confidentiality with the need for transparency in aggregated datasets.

Advance Aggregation and Systemic Risk Modeling

Carriers must invest in next-generation modelling tools that capture interdependencies in cloud services, supply chains, software ecosystems, and critical infrastructure. Integrating scenario-based stress testing and probabilistic modelling can improve capital planning and reduce uncertainty around correlated loss events. Collaboration with academic researchers and threat-intelligence providers can accelerate the development of more robust aggregation models

Strengthen Underwriting Standards and Verification

Insurers should move beyond self-reported controls and adopt more verifiable assessment methods, such as continuous monitoring tools, third-party security certifications, and automated control validation. Establishing minimum cybersecurity baselines across the industry—particularly for high-risk sectors—will reduce information asymmetry and enhance overall portfolio resilience.

Expand Risk-Mitigation Services and Policyholder Support

To reduce loss severity and improve client resilience, insurers should continue integrating pre-breach services such as vulnerability assessments, cyber maturity scoring, security awareness training, and incident-response retainers. Tailored support for small and medium-sized enterprises (SMEs), which often lack technical capacity, can help narrow the widening protection gap highlighted in the results.

Enhance Capital Adequacy and Reinsurance Strategies

Given the potential for catastrophic cyber events, insurers should strengthen capital buffers and diversify reinsurance arrangements. Stress tests that simulate extreme systemic scenarios will help ensure portfolio sustainability. Industry-wide risk pools or shared reinsurance mechanisms could also reduce concentration risk within individual carriers.

Develop Public–Private Partnerships for Catastrophic Cyber Events

Because systemic cyber events may exceed private-market capacity, governments should explore backstop mechanisms similar to terrorism-risk pools. Public–private collaboration can support market stability and ensure that essential sectors remain insured, even in extreme scenarios. Clear frameworks for responsibility and compensation will be critical for maintaining confidence among insurers and policyholders.

Promote Regulatory Alignment and International Cooperation

Cyber risk is global in nature, and inconsistencies in regulation create fragmentation. Regulators should coordinate internationally to harmonize reporting standards, resilience expectations, and solvency requirements. Joint initiatives can help establish common baselines and facilitate cross-border understanding of systemic threats.

Foster Continuous Threat Intelligence Integration

Given the rapidly evolving threat landscape, insurers must adopt real-time threat intelligence feeds and integrate them into underwriting, pricing, and claims-management workflows. Continuous intelligence will help insurers detect emerging patterns—such as new ransomware techniques or supply-chain vulnerabilities—before they escalate into major loss events

conflict of interest

The author declare no conflict of interest

Funding : This work was supported by the Deanship of Scientific Research, King Faisal University, Saudi Arabia Grant No: KFU254131

REFERENCES

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2022). *Modeling and Pricing Cyber Insurance – Idiosyncratic, Systematic, and Systemic Risks*. arXiv. https://doi.org/10.48550/arXiv.2209.07415 arXiv

Lau, P., Wang, L., Wei, W., Liu, Z., & Ten, C.-W. (2024). *A Novel Mutual Insurance Model for Hedging Against Cyber Risks in Power Systems Deploying Smart Technologies*. arXiv. https://doi.org/10.48550/arXiv.2403.11054 arXiv

Malavasi, M., Peters, G. W., Treuck, S., Shevchenko, P. V., Jang, J., & Sofronov, G. (2024). *Cyber Risk Taxonomies: Statistical Analysis of Cybersecurity Risk Classifications*. arXiv. https://doi.org/10.48550/arXiv.2410.05297 arXiv

Ren, N., & Zhang, X. (2024). *A novel k-generation propagation model for cyber risk and its application to cyber insurance*. arXiv. https://doi.org/10.48550/arXiv.2408.14151 arXiv

IBM Corporation. (2025). *IBM X-Force 2025 Threat Intelligence Index*. IBM. Retrieved from https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index IBM+2IBM Newsroom+2

IBM Corporation. (2024). *X-Force Threat Intelligence Index 2024*. IBM. Retrieved from https://www.ibm.com/think/x-force/2024-x-force-threat-intelligence-index IBM

Marsh. (2024, December 13). *Q4 2024 update on the U.S. cyber insurance market: Building cyber hygiene and more robust insurance programs*. Marsh. Retrieved from https://www.marsh.com/en/services/cyber-risk/insights/cyber-market-update-q4-2024.html Marsh

Marsh. (2024). *US cyber insurance market update: Rates decrease, threats evolve*. Marsh. Retrieved from https://www.marsh.com/en/services/cyber-risk/insights/cyber-insurance-market-update.html Marsh

Munich Re. (2024). *Cyber Insurance: Risks and Trends 2024*. Munich Re. Retrieved from https://www.munichre.com/us-non-life/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html Munich Re

Munich Re. (2024). *Global Cyber Risk and Insurance Survey 2024: Personal Lines*. Munich Re. Retrieved from https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey-2024.html

