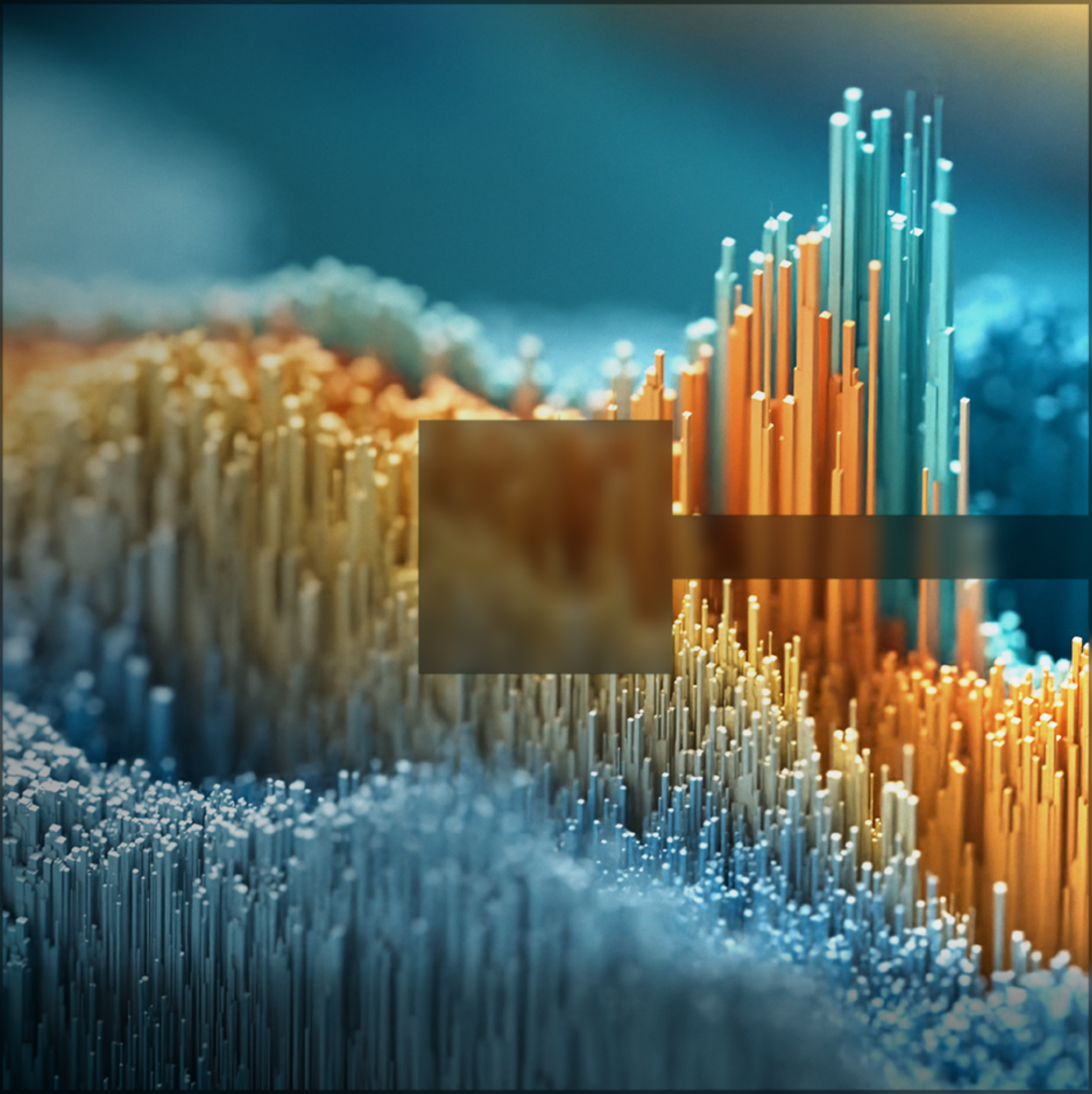


2025 Cyber Predictions

Preparing for the future

CyberCube

Foreword

Yvette Essen
Head of Content, Communications & Creative

As we enter 2025, the cyber (re)insurance market is navigating a dynamic and evolving landscape, one that presents both opportunities and challenges. While market conditions remain competitive, the continued maturation of the cyber (re)insurance sector offers significant potential for growth and innovation.

This year's report highlights key insights from our experts on emerging trends and developments we expect to see in 2025. We anticipate that the frequency of cyber incidents will rise in the near term due to Artificial Intelligence (AI) innovation. As cyber threats become more sophisticated, AI agents are expected to provide leverage for threat actors, enabling them to scale cyber attacks more widely and efficiently. Quantum computing will revolutionize cybersecurity, but at the same time, it will also disrupt cyber insurance.

> *"Quantum computing will revolutionize cybersecurity, but at the same time, it will also disrupt cyber insurance."*

Against this backdrop, a central theme in 2025 will be the shift in cyber underwriting for both single risks and portfolios, which will increasingly rely on science rather than art, driven by advancements in data analytics and risk modeling. At the same time, cross-sector partnerships will play a pivotal role in enhancing the business impact of cyber risk management decisions, creating much-needed efficiencies across industries.

Brokers will also be crucial to unlocking growth in the cyber insurance market, particularly for small and medium-sized businesses that are still underinsured. To better manage growing accumulations of risk, cyber insurers will focus on improving data collection and enhancing their ability to model and mitigate potential exposure. Just as the insurance industry has been instrumental in driving safety improvements against damage caused by natural catastrophes, cyber insurance will meaningfully impact cybersecurity posture.

These are just a few key trends and forecasts shared by CyberCube's team of specialists. We hope you find these perspectives informative and thought-provoking as we look forward to the year ahead.

Cyber underwriting will become more science and less art

Pascal Millaire
Chief Executive Officer

Underwriting complex commercial risks inherently involves a mix of art and science.

In 2025, I expect the balance of underwriting capabilities to tilt more toward science for three reasons.

Firstly, the cyber insurance industry has paid out a critical mass of cyber claims and is more systematically using that claims data to identify the security and exposure signals that are tied to losses. For example, CyberCube data shows a 15x difference in the incident frequency between top and bottom decile accounts and these correlations show up strongly in claims studies we are undertaking with clients, such as **Marsh McClennan.** Taking appropriate action on these signals in the underwriting process will have an even greater impact on loss ratios in 2025.

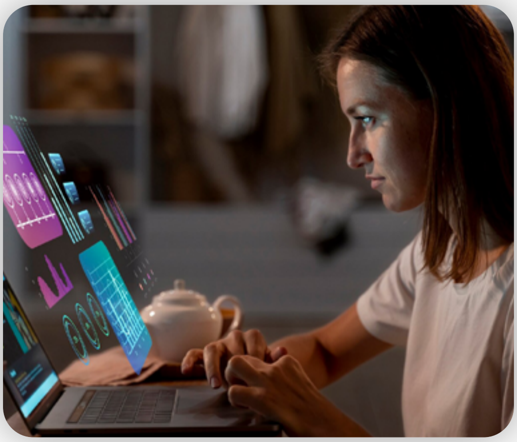
Improve loss ratios with CyberCube's predictive analytics

REPORT

Improve loss ratios with CyberCube's predictive analytics

DOWNLOAD NOW

Secondly, the increasing availability of data through APIs allows for automated screening to augment the human underwriting process with data in a manner that would not otherwise be practical. This will allow underwriters to focus on high-value evaluation factors, supplemented with automated data-driven intelligence on potential risks as carriers continue their technology integration agendas in the new year.



Finally, in 2025, reinsurers will start to have access to more detailed, data-driven analytics to compare the relative risk profiles of prospective cedent portfolios. This will tilt treaty underwriting discussions somewhat away from the softer, qualitative factors that inform a carrier's underwriting process to harder quantitative metrics on underlying risk quality relative to other cedents.

For a risk as complex, dynamic, and multi-faceted as cyber, underwriting will always be a mix of art and science. As underwriters upskill their capabilities, the industry is increasing the state of that art; and as technology providers improve underwriting data, they will be supported with increasingly compelling science.

Artificial Intelligence agents will create leverage for threat actors in scaling widespread cyber attacks

Ashwin Kashyap
Co-founder and Chief Product Officer

The rise of generative artificial intelligence (AI) has already demonstrated its potential to amplify cyber threats.

In the past two years, we witnessed how threat actors leveraged AI to enhance phishing campaigns and financial fraud schemes, marking only the beginning of a new era in cybercrime. Looking ahead, a more advanced and concerning development is emerging: AI agents that operate autonomously to scale cyber attacks with unprecedented speed and efficiency.

CyberCube
Utilizing Artificial Intelligence within CyberCube's products

REPORT

Utilizing Artificial Intelligence within CyberCube's products

DOWNLOAD NOW

> *“AI’s ability to automate and optimize cybercrime activities will allow even smaller, less sophisticated groups to execute highly effective campaigns.”*

These AI agents are capable of executing a wide range of tasks, from reconnaissance and target identification to exploit discovery and malware deployment, without the need for constant human intervention. Trained on data from previous successful and failed campaigns, these agents can adapt and evolve their strategies, dramatically lowering the cost and complexity of launching widespread attacks. This autonomy presents a significant challenge for organizations, enabling threat actors to rapidly scale attacks and target large numbers of businesses and individuals with minimal effort.

While AI has obvious applications in defensive cybersecurity, we believe that in the near term, threat actors will be the primary beneficiaries of these technologies. AI’s ability to automate and optimize cybercrime activities will allow even smaller, less sophisticated groups to execute highly effective campaigns. As a result, organizations will face heightened risks and increased pressure on their security protocols.

This shift in the cyber threat landscape will have profound implications for the cyber insurance market, which relies on models that assess the likelihood of large-scale cyber events. With AI-driven attacks now able to scale rapidly, the probabilities of such events need to be looked at through a fresh lens, which could lead to more stringent coverage terms. We anticipate that the frequency of cyber incidents will rise in the near term due to AI innovation, aligning with our broader outlook for 2024 and beyond.

Cross-sector partnerships will accelerate the business impact of cyber risk management decisions and generate much-needed efficiency

Rebecca Bole
Head of Strategic Engagement

In the current cost-constrained commercial environment, enterprises of all sizes and sectors are increasingly focused on the impact of risk management decisions on their business objectives.

This is especially true in cyber risk management, where risks are increasing at a faster rate than security expenditure. Cyber crime is predicted to increase by 66% between 2024 and 2029, while cybersecurity spend is slated to grow by just 45% in the same period.

Cyber crime is predicted to increase by: **66%** between 2024 and 2029

This dynamic requires a laser focus on the return on investment and time-to-value of risk management actions. That can be met in a couple of ways:

Delivering risk insights, expressed in financial terms, that indicate the most effective risk management decisions to take to minimize loss.

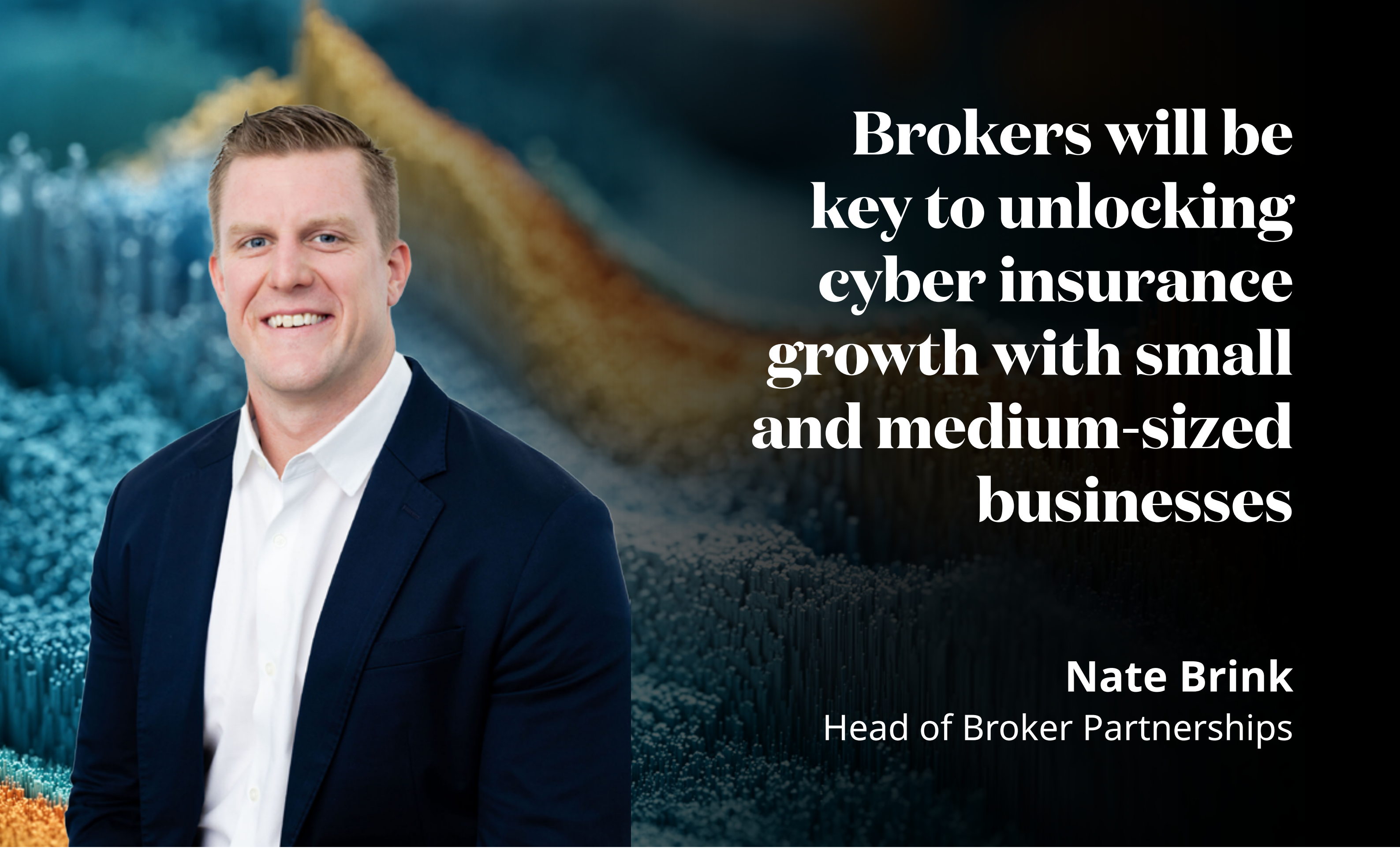
Delivering those insights most efficiently through shared technology infrastructure - thereby getting the information into the right hands and at the right time to manage risk.

But, these objectives cannot be achieved unilaterally. Delivering financially-quantified risk analytics to the organizations that need them requires partnership across the public and private sectors. In 2025, leaders in strategic enterprise risk management, tech infrastructure, and government will seek to develop pathways to obtain timely, data-driven insights.

It is increasingly important to demonstrate the financial ROI of cyber risk management to enterprise leaders. Such partnerships with global leaders in risk management will bring cyber risk quantification into the boardrooms of organizations and assist government policymakers around the world — ensuring the development of strong risk management programs within enterprises and building resilience across society.

Leading technology infrastructure providers to the insurance industry today will also be seeking to expand the actionable insights they deliver to insurance decision-makers directly into their workflows, minimize both friction and E&O issues, and drive profitability and resilience. Partners such as Duck Creek, AdvantageGo, Majesco and Millennial Shift are crucially important to connecting insights to the decision-makers with the least friction.

Through these partnerships, we expect a step change in the usage of cyber analytics by deeply embedding them into the insurance risk transfer process in a more efficient way. There is great power in combining distinct expertise and specializations to create a ground-breaking solution to serve an important need. CyberCube is excited to expand the reach of its cyber risk analytics through a growing distribution ecosystem in 2025.



Brokers will be key to unlocking cyber insurance growth with small and medium-sized businesses

Nate Brink
Head of Broker Partnerships

The small and medium-sized business (SMB) sector represents a significant opportunity for growth in cyber insurance, yet unlocking this potential requires targeted strategies to address persistent challenges. As the cyber risk landscape evolves, 2025 will see a pivotal shift in how insurance brokers and carriers engage with SMBs, emphasizing engagement, education, and innovation.

> *“Sophisticated threat analysis tools and tailored risk assessments will become standard offerings, helping SMBs understand their unique vulnerabilities.”*

In 2025, brokers will increasingly adopt data-driven education campaigns to dispel the myth that SMBs are unlikely targets for cyberattacks. Sophisticated threat analysis tools and tailored risk assessments will become standard offerings, helping SMBs understand their unique vulnerabilities. Real-time demonstrations of coverage applications will become integral to the sales process, establishing greater transparency and trust. By providing SMB clients with proactive insights, including vulnerability assessments and actionable recommendations for mitigating risks brokers will position themselves as trusted advisors, fostering long-term relationships with SMB clients.

With cyber threats evolving rapidly, brokers will need to continue their efforts to stay ahead of emerging risks. Regular cybersecurity training for brokers and ongoing collaboration with insurers will ensure that SMB-focused policies remain relevant. The complexity of cyber insurance policies will also drive a push toward standardization in 2025. Carriers are expected to introduce simplified, modular policy designs tailored to SMB needs, focusing on core coverage areas such as data breach liability, ransomware protection, and business interruption. Partnerships between insurers, cybersecurity firms, and SMB advocacy groups will also play a crucial role in raising awareness. By illustrating the real financial impact of cyber events through case studies and real-world examples, brokers can empower SMBs to recognize the necessity and value of cyber insurance.

As the soft market conditions persist, brokers need to leverage technology platforms to streamline the quoting and binding process for SMBs. Commissions earned on SMB insurance policies remain very small, so brokers must reduce time processing submissions and build relationships of trust by educating SMBs during the sales process. This can be achieved by combining analytics and benchmarking insights within their cyber proposals. Brokers will also need to expand their use of interactive tools and AI-driven platforms to demystify policy terms and efficiently and effectively guide SMBs in selecting coverages that align with their operations and budgets. Demonstrating the cost-benefit ratio of cyber insurance through predictive modeling and financial impact simulations will help SMBs prioritize the right level of investment in coverage.

In 2025, the SMB cyber insurance market is well positioned to thrive as brokers refine their strategies — leveraging engagement, education, and innovation. By addressing key pain points and delivering tangible value, the industry can unlock significant growth in this underserved segment.

> *"In 2025, the SMB cyber insurance market is well positioned to thrive as brokers refine their strategies — leveraging engagement, education, and innovation."*

Cyber insurers will improve data collection to manage accumulations more effectively

Jon Laux

VP of Analytics

Cyber insurance accumulations have grown sharply in recent years. In the absence of evidence to the contrary, responsible risk managers must treat all cyber risk as one peak zone. In 2025, we will see greater discussion about ways to potentially diversify within 'cyber', as well as about the effects of security hygiene on a company's resilience to catastrophic cyberattacks.

These topics of diversification and mitigation have generated a great deal of interest. Prior to the "*CrowdOut*" event in 2024, it was conceivable that airlines could be greatly affected by a faulty software update – but anticipating which airline would be affected in an outsized manner is another matter. We understand that cyber risk arises from a number of sources; what insurers are seeking is a better grasp of explainable variation and a reduction in the perception of pure randomness.

BLOG

The CrowdStrike Outage: How Single Points of Failure Create Widespread Disruption

Sharing preliminary findings from CyberCube

READ NOW

The VUCA framework[1], attributed to the Army War College, considers four different kinds of risk:

Volatility

The pace and nature of change can be rapid and unpredictable.

Uncertainty

Lack of understanding inhibits one's ability to predict future outcomes.

Complexity

Many different, interconnected factors come into play, with the potential to cause chaos and confusion.

Ambiguity

Lack of clarity about a situation or how to interpret the situation.

[1] Sources: Harvard Business Review, Forbes

Cyber risk includes all four of these. But the last of them – ambiguity – has more to do with the data that insurers gather than with the risk itself. No one organization has a full picture of risk. Insurers collect a great deal of information during the underwriting process, but only a small portion of that information tends to be collected in ways that can inform exposure management. Reinsurers, for their part, are worse off being downstream in this information flow.

In 2025, we expect more insurers will follow this wave. A picture is emerging of the common factors influencing a company's exposure to catastrophic cyber risk. This will facilitate increased dialogue between companies and their brokers, insurers and reinsurers, regulators and government agencies. This will be a continually involving process and while not perfect, it will have positive consequences.

The insurance market will see a clearer throughline from risk selection to catastrophe management to capital allocation and back again. Cyber insurance, ever the so-called "nascent" line of business, will take another important step toward maturity.

> *"In 2025, we expect more insurers will follow this wave. A picture is emerging of the common factors influencing a company's exposure to catastrophic cyber risk."*

Quantum computing will revolutionize cybersecurity and disrupt cyber insurance

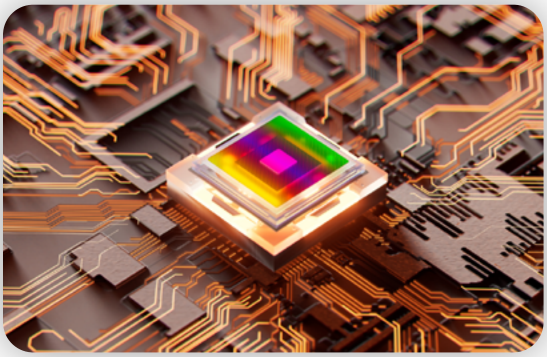
William Altman
Cyber Threat Intelligence Principal

Quantum computing, with its ability to perform complex calculations at unprecedented speeds, is poised to revolutionize cybersecurity and disrupt the cyber insurance industry. While this transformative technology promises advances in areas like optimization and data analysis, it also poses significant risks to the current cybersecurity paradigm, particularly in encryption.

One of the most immediate impacts will be on encryption standards. Current encryption protocols, such as RSA and ECC, rely on the difficulty of factoring large numbers or solving discrete logarithms — problems that classical computers cannot solve efficiently. Quantum computers, leveraging algorithms like Shor's algorithm, could break these encryption schemes, rendering them obsolete. This threatens the foundational security of online communications, financial transactions, and critical infrastructure. In response, the cybersecurity industry is already advancing "quantum-resistant" algorithms under initiatives like the US National Institute of Standards and Technology (NIST) Post-Quantum Cryptography Standardization. However, the widespread adoption of these protocols will take time, leaving a potential gap where quantum-equipped adversaries could exploit vulnerabilities.

From a cyber insurance perspective, the quantum threat adds a new layer of complexity to cyber-portfolio-aggregation risk assessments and underwriting. Quantum computing introduces unpredictability, as breaches enabled by quantum attacks could be significant, targeting encrypted data, intellectual property, or operations of critical systems. Insurers must incorporate the risk of widespread-quantum-enabled attacks into actuarial models, potentially leading to increased premiums or exclusions for quantum-related risks.

Conversely, quantum computing also offers defensive opportunities. For example, quantum key distribution (QKD) provides a method for creating encryption keys that are theoretically unbreakable, as any eavesdropping attempt disrupts the quantum state of the keys. Additionally, quantum algorithms could enhance anomaly detection and threat hunting, enabling real-time identification of sophisticated cyberattacks.



In this evolving landscape, cyber underwriters may need to adapt their risk assessment methodologies to incorporate questions related to quantum-safe practices. This could include inquiries about an organization's readiness for post-quantum cryptography, the use of quantum-resistant algorithms, and investments in emerging technologies like QKD. Underwriters might also assess whether companies are actively updating encryption protocols, conducting quantum risk audits, or collaborating with vendors to future-proof their security measures.

The timeline for widespread quantum adoption remains uncertain, but organizations cannot afford complacency. Governments and industries should invest in transitioning to quantum-resistant cryptography while exploring quantum-enhanced security solutions. Collaboration between policymakers, technology providers, and insurers will be crucial to developing frameworks that address both the risks and opportunities of quantum computing.

"In this evolving landscape, cyber underwriters may need to adapt their risk assessment methodologies to incorporate questions related to quantum-safe practices."

Managing portfolio health will become a competitive advantage

John Anderson
Sr. Principal Product Manager

In 2025, the insurance industry will increasingly prioritize measuring portfolio health as a strategic advantage. This evolution will see a heightened focus on understanding risk quality and uncovering portfolio idiosyncrasies, allowing insurers and reinsurers to refine their risk strategies and improve profitability. The ability to analyze and act on these nuances will distinguish leading organizations from their competitors.

Reinsurers are expected to intensify their scrutiny of cedants, seeking greater transparency and more robust risk metrics. In turn, insurers will leverage these insights to demonstrate how they are strategically managing the composition of their books and strike a balance between growth and profitability.

"In 2025, the insurance industry will increasingly prioritize measuring portfolio health as a strategic advantage."

Insurance companies will also pay closer attention to how their underwriting teams use cyber analytics. A key focus will be ensuring underwriters consistently use the tools and analytics provided to them. This will involve training, better integration of tools into workflows, and fostering a culture where analytics are used in decision-making.

Data quality will remain a cornerstone of these developments, with insurers increasingly demanding higher fidelity in the data they consume. Greater emphasis will be placed on the confidence in the data they use. As data continues to play a critical role in underwriting and portfolio management, insurers will push for improved accuracy and consistency, both internally and across their partner ecosystem.

Cyber insurance will meaningfully impact cybersecurity posture

Richard Ford

VP of Engineering

My prediction is that improved risk quantification will have an increasingly meaningful impact on cybersecurity behaviors across a large segment of the market. Just as the insurance industry has been instrumental in driving safety improvements in the “physical” world, the improvements in risk quantification within cyberspace, coupled with increased adoption of cyber insurance in mid-sized organizations, will drive benefits to security robustness and resilience.

As a technologist who has spent his entire career in some type of Cybersecurity work, I think the unspoken truth is that we all - almost without exception - know how to improve cybersecurity, but for a variety of reasons, we don’t. Put simply, we know better, but we don’t *do* better.

This disconnect often relates to budgets, staffing, and tradeoffs between safety and other business priorities. Essentially, cybersecurity has been positioned as a technical problem more than a business one.

> *“We know better, but we don’t do better.”*

Fortunately, this is changing - and the combination of data-driven risk quantification and cyber insurance is one of the drivers. This isn’t the first time we’ve seen insurance help drive the adoption of best practices. For example, in Florida, it’s long been known that hurricane strapping on roofs can dramatically improve a structure’s resilience to otherwise destructive winds. Despite this knowledge, many homeowners only decided to go forward with this improvement when they realized that their insurance costs would drop dramatically when they did so. Knowledge of the risk wasn’t enough - but making it tangible in terms of policy cost acted as a motivator. In addition, improvements in building codes to make new construction more resilient have been heavily influenced by insurers.

As risk quantification becomes more reliable and defensible, in both broad and targeted ways, we will see cyber insurance play a far more significant role in enabling CISOs to drive improvements in cybersecurity posture that are data-backed, business-driven, and will benefit society as a whole.

For example, we already see companies being required to attest to the adoption of certain security best practices to increase limits on their policies. As models become more sophisticated and accurate, we can expect this trend to increase, making insurance more affordable for the most secure companies while simultaneously driving the adoption of demonstrably beneficial defenses for risk reduction. For CISOs, this could represent a powerful lever to secure buy-in for investments in security measures, positioning them as enablers of financial resilience rather than cost centers — the perfect win-win.

The virtuous cycle of insurance coupled with "cyber building codes" will play an increasingly large role in driving safer systems, and increased insurance penetration in the mid-market will drive down third-party risks, increasing systemic resilience and arming CISOs with the data they need to make ROI-driven decisions.

Policy terms and data capture will evolve to address the more nuanced exposure landscape

Brittany Baker

VP of Solution Consulting

In 2025, (re) insurance policy terms and data capture will evolve to address the more nuanced exposure landscape that was demonstrated by events in 2024.

This will stem from both the demand side, with primary carriers looking for true cat reinsurance coverage, and supply side, with carriers seeing how actual losses varied within events across their portfolio — like CrowdStrike.

We've already seen an increase in demand for more non-proportional coverage. While change has been slow thus far, it will continue to push forward. This will happen in both traditional reinsurance - with some reinsurance carriers playing a unique strategy to their advantage and in the ILS space, with instruments coming to market with more narrow scopes than the 144a structures already in play.

One dimension that was interesting to observe was that of “time” with respect to CrowdStrike. The impact of time was already captured and considered within Business Interruption (BI)/Contingent Business Interruption (CBI) coverages in the form of waiting periods. The global nature of the outage, plus the quicker resolution meant that some regions were more impacted than others due to the local time of day when the outage was initiated. The industry discusses regionality of technology concentrations but the discussion of local time playing such a role in shorter events hadn’t been as discussed as heavily prior to CrowdStrike. Will the wording for waiting periods change in the future?

While we’ve seen previous events in which the interdependency of two different single points of failure technologies caused issues (e.g. wordpress and godaddy), CrowdStrike was the most visible event of this nature. The effect should be that models will increasingly and explicitly take this into account - both on the exposure side as well as the loss side. The other impact will be the continued pressure for better data capture along the insurance value chain. Vendors currently do this heavy lifting to capture, cleanse, and make useful technology dependency data indirectly but the insurance industry is uniquely positioned to capture this directly from their enterprise clients.

Diversification and Mitigation Will be Redefined Through Data-Driven Ecosystems

Cody Stumpo

Head of Product

In 2025, the insurance and reinsurance industries will further entrench data-driven insights as the cornerstone of their risk management strategies. With continued advancements in modeling and analytics, insurers and reinsurers will refine their ability to differentiate performance at a highly granular level. Insurers will increasingly reward insureds with strong risk management practices, using sophisticated tools to evaluate how individual insureds contribute to or mitigate aggregate portfolio risks. This precision will drive a shift toward underwriting strategies that emphasize targeted diversification, ensuring resilience amid escalating global uncertainties.

> *"Insurers and reinsurers will refine their ability to differentiate performance at a highly granular level."*

For reinsurers, the growing importance of exposure management will solidify the role of data in assessing cedant quality. Reinsurers will harness next-generation analytics to identify cedants with superior underwriting discipline, balanced portfolio composition, and proactive loss management. The ability to differentiate cedants based on their aggregate impact on risk models will be critical in shaping long-term partnerships and optimizing capital deployment.

The insurance ecosystem will evolve into a fully integrated, data-centric framework where insights from catastrophe models and portfolio analytics are seamlessly applied to real-world decision-making. This shift will not only enhance diversification and mitigation strategies but also redefine competitive advantage. The trust in and adoption of analytics as actionable tools will empower the industry to navigate an increasingly volatile risk landscape with greater precision and resilience.

CyberCube

CyberCube is the leading provider of software-as-a-service cyber risk analytics to quantify cyber risk in financial terms. Driven by data and informed by insight, we harness the power of artificial intelligence to supplement our multi-disciplinary team. Our clients rely on our solutions to make informed decisions about managing and transferring cyber risks. We unpack complex cyber threats into clear, actionable strategies, translating cyber risk into financial impact on businesses, markets, and society as a whole.

Contributors

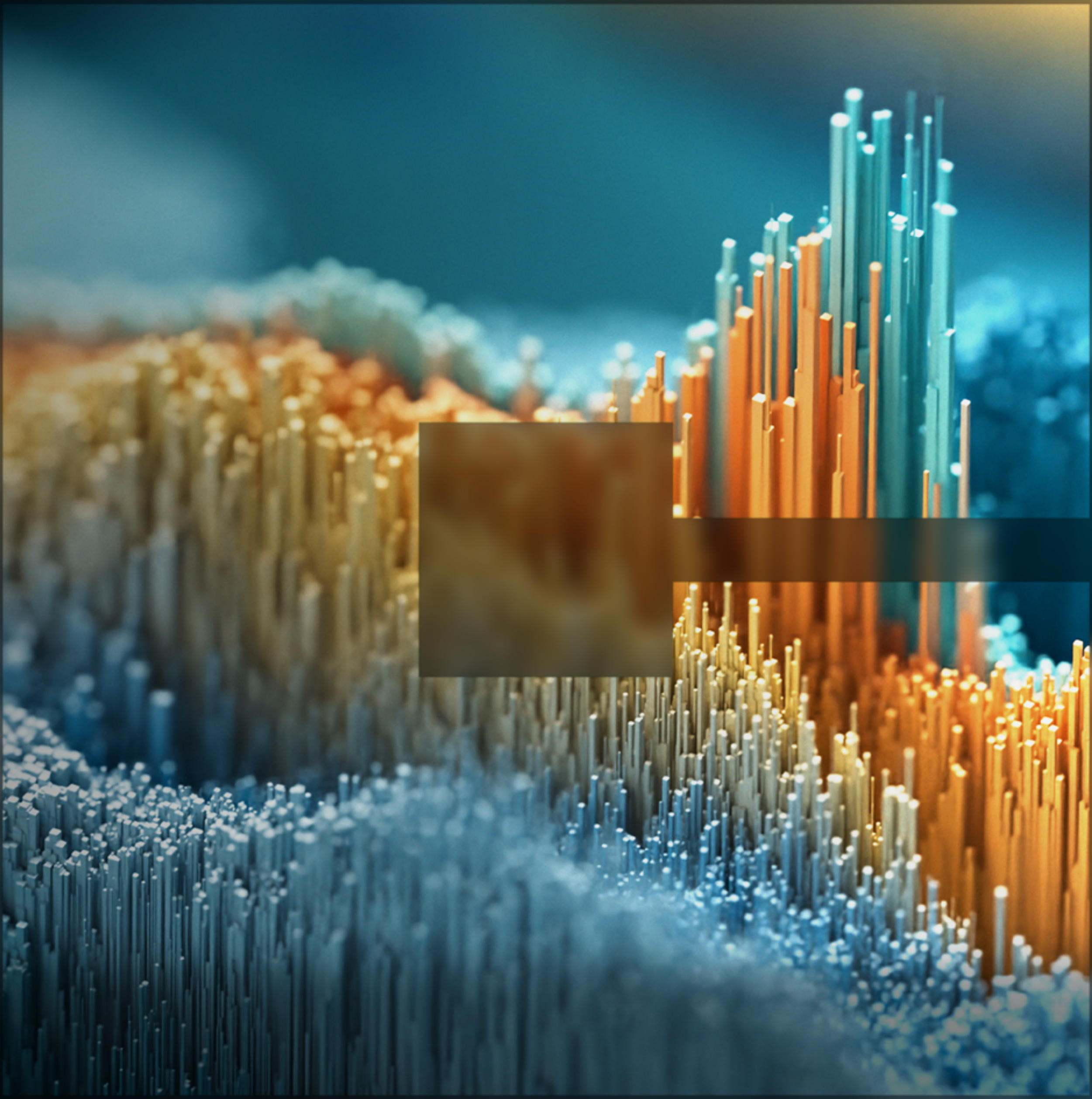
Editorial Manager:

Yvette Essen - Head of Content and Communications

Designer:

Muhammad Ahmad - Graphic Designer

This document is for general information purpose only and is not and shall not under any circumstance be construed as legal or professional advice. It is not intended to address all or any specific area of the topic in this document. Unless otherwise expressly set out to the contrary, the views and opinions expressed in this document are those of CyberCube's and are correct as at the date of publication. Whilst all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of the content of this document, no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. CyberCube and its affiliates shall not be liable for any action or decisions made on the basis of the content of this document and accordingly, you are advised to seek professional and legal advice before you do so. This document and the information contained herein are CyberCube's proprietary and confidential information and may not be reproduced without CyberCube's prior written consent. Nothing here in shall be construed as conferring on you by implication or otherwise any licence or right to use CyberCube's intellectual property. All CyberCube's rights are reserved. CyberCube is on a mission to deliver the world's leading cyber risk analytics. We help cyber insurance market grow profitably using our world leading cyber risk analytics and products. The combined power of our unique data, multi-disciplinary analytics and cloud-based technology helps with insurance placement, underwriting selection and portfolio management and optimization. Our deep bench strength of experts from data science, security, threat intelligence, actuarial science, software engineering, and insurance helps the global insurance industry by selecting the best sources of data and curating it into datasets to identify trustworthy early indicators.



CyberCube