CyberCube

Cyber Predictions Report 2026

Authors

CyberCube

Authors:

Pascal Millaire
CEO, CyberCube

Bob Petrie
President & CEO, Origami Risk and
CyberCube Board Member

Richard Ford
VP of Engineering

Nate Brink
Head of Broker Partnerships

Ross Wirth
VP, Head of Strategic Tech Ecosystem

John Anderson
Sr. Principal Product Manager

Brittany Baker
Head of Solution Consulting & ILS

William Altman
Head of Cyber Threat Intelligence Services

Editorial Content:

Yvette Essen
Head of Communications
& Market Engagement
at CyberCube

Editorial Design:

Felix Paula
Growth Marketing Creative
at CyberCube

CyberCube

Foreword

Yvette Essen
Head of Communications & Market Engagement, CyberCube

As the cyber insurance ecosystem continues to evolve, one truth has become clear: the organizations that thrive are those that anticipate change rather than react to it. Each year, CyberCube's experts analyze emerging trends across technology, threat intelligence, insurance market behaviour, and the broader regulatory environment. The result is a set of predictions for 2026 designed not only to forecast what lies ahead, but to equip the industry with the insight required to navigate it with confidence.

The year ahead will test assumptions, challenge long-held practices, and redefine what "good" looks like in cyber risk management, underwriting, and portfolio strategy. Artificial Intelligence (AI) will continue to dominate boardroom conversations — not simply as an enabler, but as a disruptive force that reveals who has embraced disciplined adoption and who risks falling behind.

At the same time, shifts in regulation, including age-restriction laws, may unintentionally undermine security and privacy for all users. Against this backdrop, insurers and reinsurers are demanding clearer, faster, more actionable insights. Brokers, too, face a pivotal moment. Advisory-driven differentiation will increasingly hinge on digital scale, specialization, and quantification as clients look for partners who can translate complexity into clarity.

Across the industry, value creation will depend on operational excellence. Automation will unlock the next wave of progress in cyber analytics, while actionable data and efficient workflows will be essential to sustaining the bottom line in competitive conditions. These themes underscore a broader market reality: resilience will favor those who prioritize technology-enabled decision-making.

CyberCube remains committed to supporting the industry through this transformational year. By blending advanced analytics, rigorous modeling, and real-world insight, we aim to empower stakeholders to understand, measure, and manage cyber risk with unprecedented clarity.
We hope this report helps you navigate the year ahead with greater foresight — and seize the opportunities it presents.

AI in insurance will expose the disillusioned and reward the disciplined

Pascal Millaire
CEO, CyberCube

Recent surveys paint a striking picture of the P&C industry's relationship with artificial intelligence: executives overwhelmingly believe in its potential, but only a fraction have realized it in practice. In 2026, I predict an increasing rift between the "disillusioned" and the "disciplined" when it comes to AI's impact on insurance.

According to a 2025 Roots survey, 82% of insurance leaders say AI is a top business imperative — yet very few have rolled out AI solutions at scale. The interest is genuine; the results are not… at least, not yet.

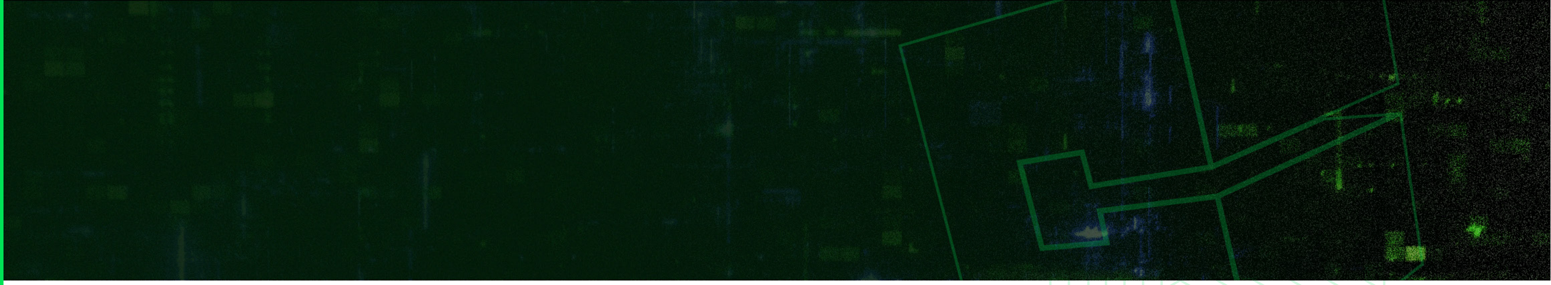
In 2026, I predict we'll see a period of AI disillusionment. The enthusiasm of boardrooms and conferences will meet the reality of legacy systems, data silos, and regulatory caution. Many initiatives will stall before they turn into pilots, let alone scale. But that's not failure. It's part of the technology hype cycle that every transformative innovation must pass through as the initial buzz of AI model expectations meets reality.

2026

An increased rift when it comes to AI's impact on insurance

82%

Insurance leaders say AI is top business imperative



I predict that the winners in 2026 will be the disciplined P&C insurance executives who do two things:

Firstly, they will be willing to experiment across functions and create sandboxes to try new approaches. These experiments need strong guardrails to recognize that most of these approaches will not be ready for prime time, but they lay the groundwork for a world where virtually all functions of insurance are transformed by AI.

Secondly, AI winners will identify real-world pain points that can be solved today. These may not be the end-to-end transformations AI evangelists have promised, but the pain is real and so is the value. For example, CyberCube's increased use of internet-scale data collection, translated into structured data with large language models, will incr easingly provide insurance-specific data augmentation needed by cyber insurers in 2026.

As Roy Amara, the futurist, famously said:

> *" We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."*

That quote captures exactly where the P&C sector stands. Short-term excitement will give way to a few years of realism — and then, over time, reinvention. Some may become disillusioned with AI promises; however, those who are disciplined will have a learning mindset and find early wins.

AI won't transform insurance overnight in 2026, but over the long run, it will transform everything about how insurance understands, prices, and manages risk.

AI will deliver much more radical efficiency gains in the claims handling process

Bob Petrie

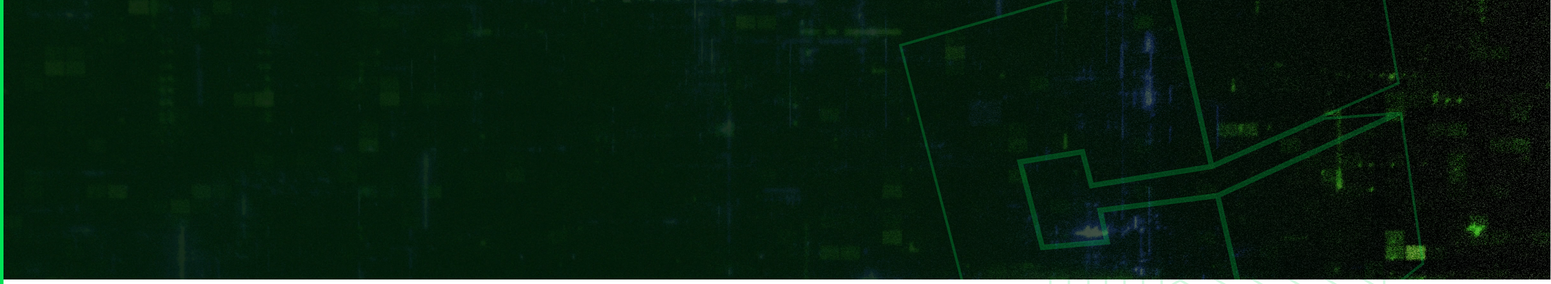
President & CEO, Origami Risk
and CyberCube Board Member

In 2026, AI will deliver radical efficiency gains in claims handling by amplifying human expertise so that smaller teams can handle far more work through configurable, trustworthy automation.

Many of the manual tasks that generate thousands of work hours across the typical claims shop today will be streamlined into AI-enabled workflows. The result: fewer repetitive tasks, fewer errors, and more time for humans to focus on high-value decisions.

Claims can be looked at as a series of workflows. The first workflow is intake. Data has to be entered into a claims system. Along the way, reserves are set, claims are assigned, adjusted, settled, and regulatory compliance is maintained. Verifying coverage, monitoring for fraud, closing claims, and approving payments are all part of that workflow. Humans make almost all those decisions in most claims systems today, particularly in legacy claims systems.

In 2026, you will be able to apply your AI-enabled processes to all of your claims-handling playbooks. You can decide to what extent you configure AI-driven decision-making, and you can test and validate the outputs to assess where AI performs with more accuracy and less bias than a human.



The result will be that a lot of the decisions and the work in the claims-handling process can be automated where it brings value, with humans focusing on the parts of the workflow that cannot be efficiently or safely automated using AI.

> *"AI will reduce repetitive manual tasks and deliver relevant insights, while humans will make all the critical decisions in a claim."*

How far and how fast this change takes effect will depend on different claims-handling shops' risk tolerance and focus on efficiency. 2026 will transform the way claims shops operate, leading to better claims management and freeing up time for more high-value tasks.

Overall, this means faster claims processes, fewer human errors, and a significant reduction in the number of touches a human needs to make in processing a claim... resulting in greater accuracy, lower response times, and lower costs.

2026 will be the year when you start seeing this happen. You will already have seen a lot of research and development, but from 2026 you will see those tools deployed at scale.

Age restriction laws will erode security and privacy for all

Richard Ford
VP of Engineering, CyberCube

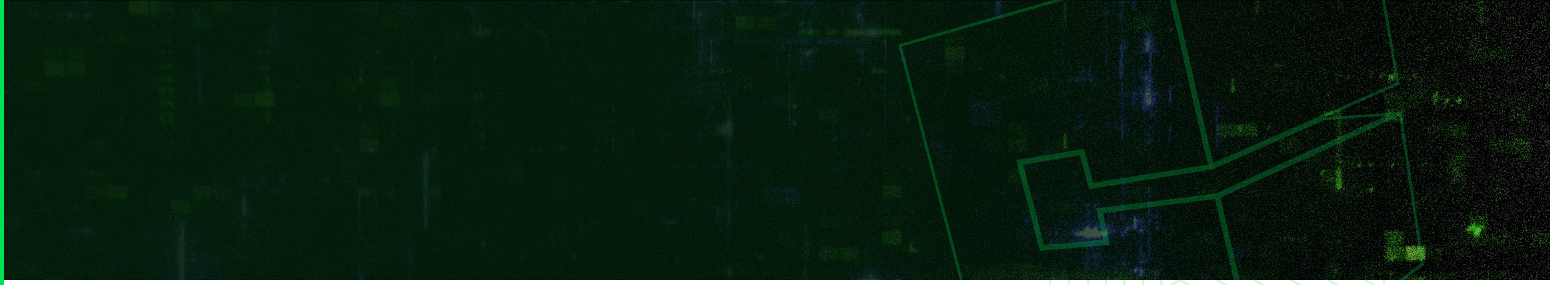
In 2026, I expect a sharp rise in identity-based coercion and insider compromise if individuals continue to lose online anonymity due to Age Restriction Legislation and VPN bans/limits. Attritional cyber losses are likely to grow, particularly through attacks exploiting insecure public WiFi, credential theft, and extortion.

For many years, encryption has provided a solid foundation for security and privacy across the Western world. However, these technologies are coming into conflict with online safety legislation — most notably, though not exclusively, the UK's Online Safety Act (OSA).

In the US, age verification laws (such as Utah SB152, Texas HB1181), as well as the potential security risks raised by limitations on personal VPNs (such as Wisconsin AB 105/SB 130), create additional opportunities for cyber criminals.

While the United States is unlikely to place a federal-level ban on VPN usage due to the First and Fourth Amendments, it is entirely possible that some states will enact legislation that effectively makes personal VPN usage untenable within a particular jurisdiction.

> *"While child safety is a legitimate concern, legislators are potentially sleepwalking into a security disaster."*



The problem is structural: identity verification creates a new, high-value data set for attackers. Moreover, this data set would be the perfect foundation for extortion or coercion: Once identity data is leaked, attackers gain leverage over individuals who can be blackmailed into granting access to sensitive corporate systems. This would drive major corporate breaches and widespread compromise - a perfect attack vector for nation-states and Advanced Persistent Threat (APT) actors.

The inevitable consequence of this legislative path is not a true ban, but rather "regulatory capture". Policymakers, driven by the desire to close these loopholes, will mandate that commercial VPN providers adopt Know Your Customer (KYC) checks and relinquish their "no-logs" policies. This regulatory burden will erode the commercial privacy model, forcing legitimate, privacy-focused VPN services to abandon the market altogether.

The irony is that this self-inflicted harm jeopardizes secure operational continuity. VPNs are critical infrastructure for banks, corporate remote workforces, and financial institutions.

By pushing legitimate services out, lawmakers risk greater economic damage and compromise to sensitive government and corporate networks.

Brokers must become the integrated data hub, the "One-Stop-Shop" for their retail agent partners

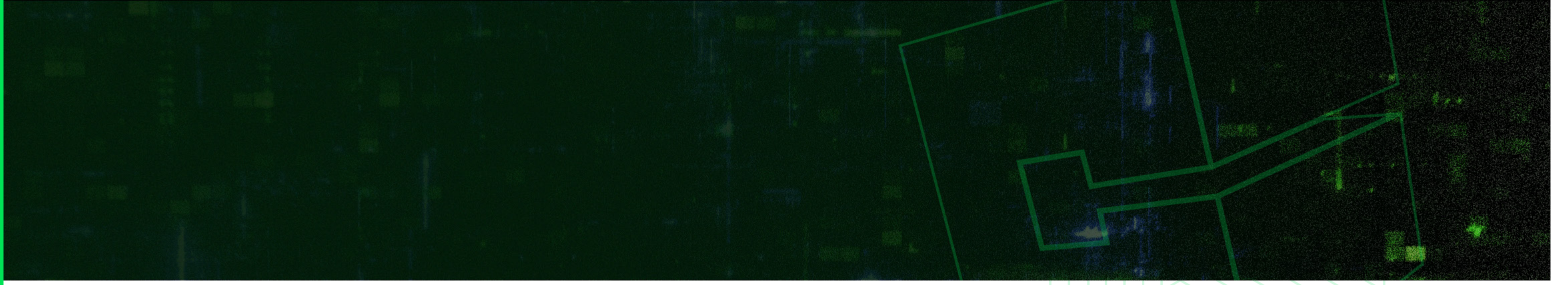
Nate Brink
Head of Broker Partnerships, CyberCube

The cyber insurance market, saturated by capacity and defined by softening rates, demands brokers change their value proposition. The key to sustaining client relationships and winning new business is moving the conversation from a transactional focus on premium to a consultative focus on risk financing.

To thrive in today’s soft cyber market, brokers must evolve into sophisticated advisors that combine technology, specialization, and data-driven insight.

The high-volume Small and Medium Business (SMB) sector cannot be served profitably through manual processes. While digital quote-to-bind platforms are assumed, true efficiency means optimizing the entire distribution chain.

> *“Brokers will need to provide advisory-driven differentiation through digital scale, specialization, and quantification.”*



By providing benchmarking and analytics alongside quotes, producers can efficiently educate clients on their risk posture compared to peers, turning a fast transaction into a consultative opportunity.

At the same time, the modern threat landscape is too granular for generalist advice. Successful brokers must achieve deep domain knowledge by specializing in high-exposure verticals, such as Manufacturing or Healthcare. Focusing on a sector like Manufacturing, for instance, allows brokers to address the unique convergence of IT and Operational Technology (OT) risks, moving the discussion beyond data breaches to cover potential physical damage and production downtime.

Finally, to gain a seat at the C-suite table, brokers must avoid technical jargon and speak the language of financial impact and balance sheet protection. This requires leveraging analytics partners to quantify risk. Instead of focusing on the limit amount, brokers should model potential loss scenarios to demonstrate how a recommended limit transfers a specific percentage of the client's total financial exposure to a cyber event.

This data-driven approach also allows brokers to justify client investment in security controls by proving remediation leads to better underwriting terms.

The broker's new value proposition in 2026 will become "We don't just transfer risk; we help you understand, mitigate, and finance it."

Automation will unlock the next wave of value in cyber analytics

Ross Wirth
VP, Head of Strategic Tech Ecosystem, CyberCube

In 2026, demand will accelerate for automation and frictionless access to analytics within the systems insurance and risk professionals already use. As soft market conditions in the cyber (re)insurance market persist, efficiency and optimization will define success. The focus will shift from more data to better-delivered data: insights presented at the exact point of decision, within underwriting, broking, and risk-management workflows.

Across the insurance value chain, technology platforms will evolve from passive systems of record into intelligent systems of insight. APIs, embedded analytics, and workflow automation will increasingly eliminate the manual steps that slow underwriting, placement, and capital allocation. The platforms that succeed will be those that disappear into the background, surfacing only the insight required to make the next best decision.

For analytics providers, this represents the maturation of the market and client needs. Rather than discrete models or standalone tools, clients will demand unified, interoperable platforms that connect seamlessly with their core environments. The power of the platform for cyber analytics will allow (re)insurers, brokers, and capital providers to draw from a single source of intelligence — enabling consistent risk views across systems, teams, and geographies.

Underlying this transformation is the orchestration of immense data ecosystems: the capture, curation, and synchronization of diverse cyber signals and loss data into advanced modeling pipelines, and the delivery of those insights back into operational systems at scale. Managing this end-to-end intelligence flow — from input data to model outputs to in-workflow guidance — will become a defining competency for the industry's leaders.

Through deep collaboration with technology ecosystem partners, the industry will finally unlock the scale needed to operationalize cyber risk analytics everywhere decisions are made.

> *"The next frontier for cyber analytics lies in orchestrating data, models, and insights into a unified, intelligent platform."*

This evolution will optimize how cyber risk is quantified, managed, and communicated — turning data into guidance, and guidance into action.

Actionable data and efficient workflows will help sustain the bottom line

John Anderson
Sr. Principal Product Manager, CyberCube

In 2026, actionable portfolio health data and more efficient processes will be a focus for (re)insurers to sustain them through these market conditions. The (re)insurance industry will double down on the actionability of insights for portfolio and underwriting decision-making.

The current pricing and market conditions pose a challenge for profitable top-line growth for both insurers and reinsurers alike.

> *"Companies that are investing in actionable data and processes that support underwriting discipline will be best positioned for bottom-line growth, and longer-term success."*

This greater emphasis on actionable data will both help improve underwriting decision-making and, in turn, lead to more resilient insureds. Managing this at the portfolio level will help identify adverse risk selection and reinforce uniform underwriting rigor across teams.

Insurers, especially, will seek to improve efficiency to better serve their customers. This means enabling workflows that help them better serve and capture profitable market share, without necessarily adding headcount.

For many insurers, there has been a push to expand their positions in untapped markets, especially in parts of Europe. In order to effectively capitalize on this opportunity, insurance carriers will need to have well-defined playbooks, supported by light-weight and well-oiled processes and actionable data to help improve the cyber posture of the insureds in this market and in their book.

AI, as others will note, will be one such tool to aid the light-weight efficiency needed, without hurting the bottom line. Advances in agentic AI solutions have shown early signs of promise, with other lines of insurance capitalizing on the opportunity.

Cyber, which has historically been a tip of the spear in terms of innovation in insurance, remains well-positioned to be an early adopter of agents and generative AI that can automate underwriting and claims workflows, and streamline information gathering.

Innovation will continue across the cyber insurance industry

Brittany Baker
Head of Solution Consulting & ILS, CyberCube

Cyber insurance has always attracted people who were attracted to new markets, thrive in uncertainty and who are comfortable forging new paths. In a soft rate environment, most insurance lines fall back on muscle memory. Pricing pressure is real as is the increased claims rate driven by ransomware events.

So is the competitive pressure to differentiate on something other than rate cuts and the drive to expand the market footprint. That is why we started to see genuine product and capital innovation surface in 2025, the kind that comes from necessity rather than marketing, and it is likely only the beginning of what will emerge in 2026.

2025 examples of innovation have included:

- Aon's Surge Stop Loss cyber reinsurance product, launched to provide coverage for abnormal loss surges during a specified time period without the need to agree on event definitions
- Beazley's new Bermuda-based ILS fund focused on cyber-ILS strategy to help grow the market
- CyberCube's Exposure Manager, a first of its kind solution that provides security hygiene data in the hands of reinsurers and portfolio managers.

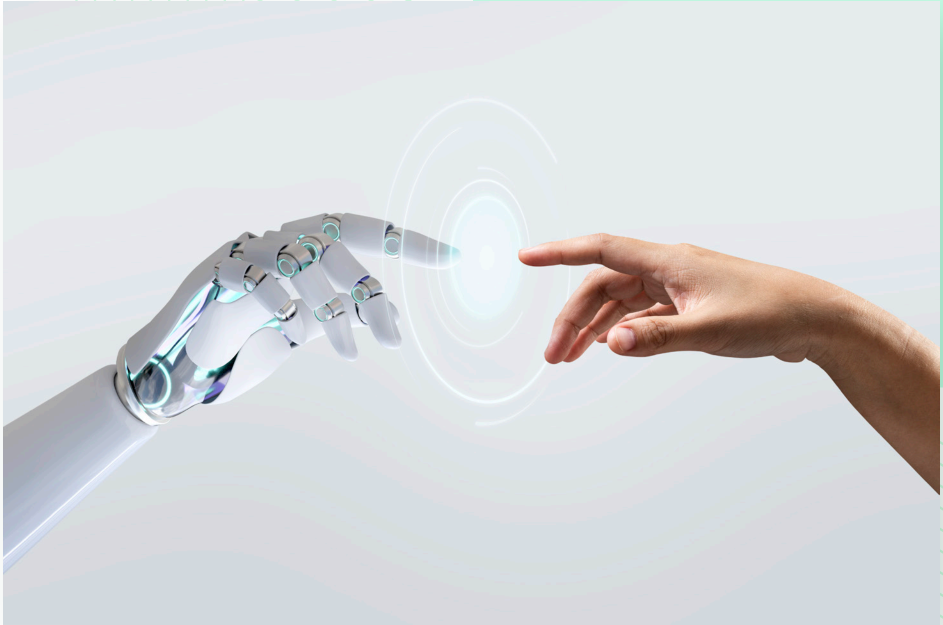
We need to see more creativity as the market pursues growth in new territories with focus on countries such as India, Japan, and South Korea, and in smaller sized insureds. Products need to align with demand, and education is still imperative. The industry has done this in many ways already – we can do it again.

One area where innovation will be especially important is the expanding commercial use of AI. The market has already begun responding by creating new products. This will continue to evolve as we observe how AI reshapes the threat landscape and as real incidents materialize. In the near term, I expect more impact on the attritional types of losses rather than on systemic events, alongside growing evidence of how defensive AI capabilities are enabling security teams to react faster and more effectively.

As we look ahead to 2026, one theme is clear:

> *“ The industry’s ability to adapt, experiment, and innovate will define its success.”*

Cyber risk is dynamic, but so is the ingenuity of the cyber insurance ecosystem. By embracing emerging technologies, designing products that meet the needs of a broader set of buyers, and continuing to invest in data-driven insights, the market can turn uncertainty into opportunity. The organizations that lean into this moment — not away from it — will shape the next chapter of cyber insurance.



2026 is the year quantum risk gains real traction in cyber insurance thinking

William Altman
Head of Cyber Threat Intelligence Services, CyberCube

In 2026, quantum computing may begin to gain more serious consideration within the cyber insurance industry as scientific and commercial signals become clearer and more credible.

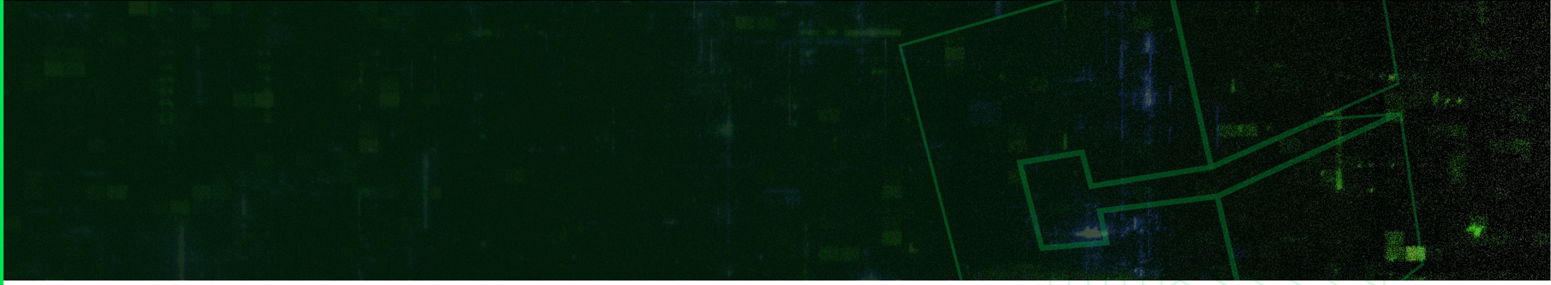
No dramatic leap is expected, but steady progress in several areas could shift quantum from a long-term abstraction to an exposure that underwriters and portfolio managers start to examine with more structure.

Throughout 2026, leading hardware providers may demonstrate incremental but important advances: higher logical qubit fidelity, early evidence of scalable error mitigation, and more transparent roadmaps detailing how and when cryptographically relevant systems might emerge. None of these developments will threaten encryption on their own, but their combined effect could reduce uncertainty. As confidence grows in the pace and direction of progress,

> *“Insurers may need to begin forming views on how quantum timelines intersect with multi-year policy and portfolio horizons.”*

One area that could draw new attention is the feasibility of “harvest now, decrypt later” activity. Even if quantum computers remain years away from breaking modern cryptography, adversaries with long planning cycles may already be collecting encrypted datasets.

Insurers may begin to consider whether certain classes of data have long enough value duration that future decryption could matter. This conversation may be especially relevant for healthcare, life sciences, financial services, and government contractors.



For underwriters, 2026 could introduce early-stage discussions about quantum-readiness indicators. Questions may arise around whether an organization has mapped its cryptographic dependencies, whether it has a post-quantum transition strategy, and whether it is monitoring relevant NIST standards. These would serve as directional signals rather than rating factors, helping underwriters understand which insureds are preparing for longer-term security transitions.

Portfolio managers may also begin to test quantum-related stress scenarios. These may explore how long-tail confidentiality losses might emerge if historic encrypted data becomes exposed, or how quantum-inspired optimization techniques could accelerate threat-actor workflows even without breaking encryption. Such scenarios would not drive capital decisions in 2026, but they could support early accumulation analysis and risk education.

Overall, quantum computing is unlikely to create measurable insured losses in 2026. However, the year could mark an important shift in mindset as technical progress becomes harder to ignore. Insurers may begin building frameworks, asking structured questions, and preparing for a future in which quantum risk becomes a defined part of cyber exposure management.

CyberCube

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 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 their 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.