Executive Welcome

Welcome to Aon's 2025 Global Cyber Risk Report, a study that follows a year of noteworthy systemic cyber events. This report stands alone in its ability to help businesses make better cyber risk decisions thanks to the unique way we have drawn together data and interpretation across critical cyber security controls, cyber events and the cyber insurance market — globally and by region.

Read more

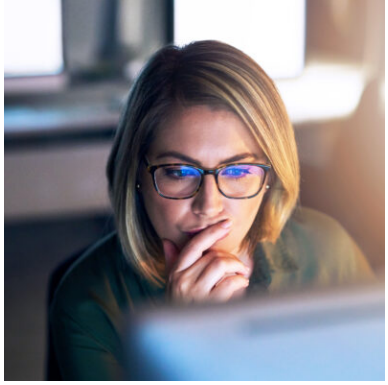
01

Ransomware Payouts Decline Despite Growing Cyber Claims Frequency

Learn more

In 2024, cyber incidents were more frequent while ransomware remained a focal point. Understanding the evolving market dynamics and cyber risk landscape has never been more essential.

02



Cyber Risk Insurance Market Remains Buyer-Friendly

Learn more

Ample capacity and competition drove cyber risk insurance premiums lower in 2024. Learn how insurance is steering cyber risk preparedness and how to better manage large-scale systemic risks.

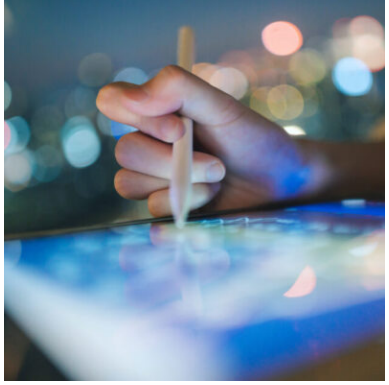
03

Raising a Red Flag: Cyber Risk Controls and Insurability

Learn more

As cyber risks dynamically change and threat actors shift their tactics, critical security — or red flag — controls can change. Find out how your organization compares in terms of cyber risk resilience.

04



Finance and Insurance Industries: Managing Risk in a Rapidly Evolving Environment

Learn more

Finance and insurance companies have more work to do to manage, mitigate and transfer cyber risks in a rapidly evolving risk environment.

05

Third-Party Risks Can Create Cyber Challenges for Healthcare

Learn more

The healthcare sector is contending with a range of risks specific to its sector — including its heavy reliance on third-party service providers, a growing technology footprint and tight budgets — that can increase the severity and complexity of cyber risks.

06

Cyber Risk in an Increasingly Digitalized Manufacturing Sector

Learn more

A combination of legacy systems, rapid digitalization and significant third-party vulnerabilities, makes cyber risk a growing concern — and a growing challenge — for the manufacturing sector.

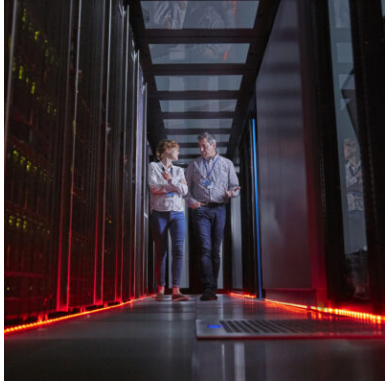
07

Asia-Pacific's Commitment to Cyber Security Pays Off

Learn more

Asia-Pacific's cyber maturity continues to improve — in the face of considerable threat. Risk Leaders, therefore, should focus on geopolitical drivers of risk, a shifting regulatory environment, the impact of artificial intelligence and opportunities to help enhance risk capital protection.

08



Riding the Wave: EMEA Approaches Cyber Maturity

Learn more

With great volatility comes great cyber risk. Explore how a mix of security controls, cyber risk insurance and regulatory compliance can help your organization manage, mitigate and transfer cyber risk.

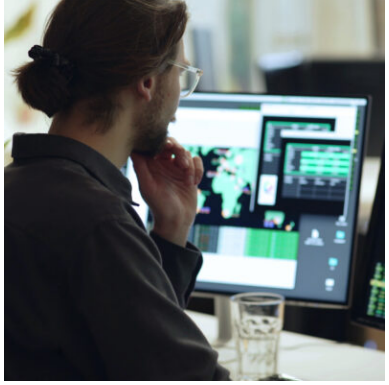
09

Cyber Risk is a Corporate Risk — Latin America Responds

Learn more

The Latin American region is maturing and the cyber insurance market is opening. Learn how businesses scored across critical cyber risks and assess your readiness to secure a cyber insurance policy in 2025.

10

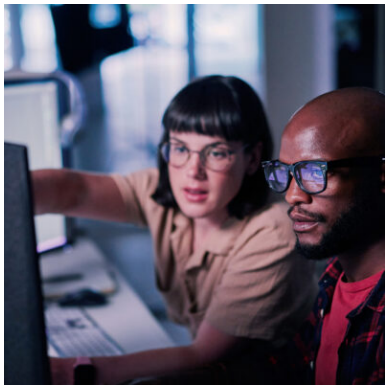


North America - Cyber Risk Maturity Grows Amid Systemic Cyber Events

Learn more

Cyber risk insurance premiums declined as organizations invested in controls to manage large-scale systemic risk. It’s time to make the right decisions to ensure stability in a volatile cyber risk environment.

11

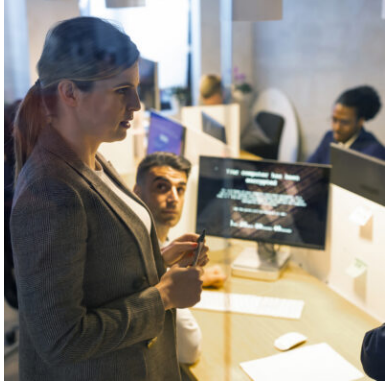


The Five Drivers That Can Help Mitigate Growing Reputation Risks

Learn more

Reputation risks related to cyber events are growing, but companies can help safeguard shareholder value by understanding and mitigating them.

12



A Highlight Year For Systemic Risk – And Single Point Of Failure Events

Learn more

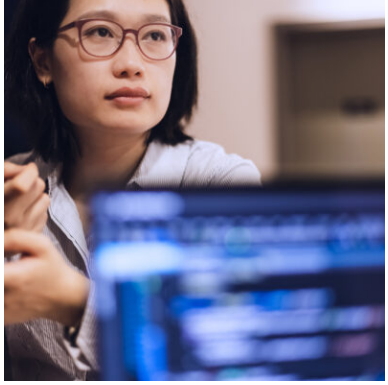
Dealing with third parties involves real and unavoidable cyber risks. Capture insight into potential single points of failure and help protect your balance sheet against systemic risk.

13

Tackling Ransomware: Helping Insurers and Their Clients Keep Pace with Change

Learn more

An in-depth study reveals the benefits for both insurers and commercial buyers from implementing strong cyber controls in ransomware claims



Behind the Data: Better Decisions Facilitated Through Aon's Cyber Broking Process

Learn more

Aon's 2025 Cyber Risk Report leverages proprietary data from the Cyber Quotient Evaluation (CyQu), a patented global cyber e-submission platform, that helps streamline the insurance intake process and strengthens clients' cyber risk management programs by delivering insights into exposures and insurability factors.

Ransomware Payouts Decline Despite Growing Cyber Claims Frequency

Key takeaways

The frequency of reported cyber incidents grew — up 22% on the previous year.

Ransomware claims frequency increased while the average ransom payment amount for Aon broking clients declined by 77%.

Midsized organizations filed more cyber claims than any other group, over half of all incidents.

The past year's cyber attacks and technology outages illustrated the compounding risk from growing technology interdependencies. Major systemic-type events shook the scene in 2024, particularly evident in attacks against information technology (IT) service providers. A notable February attack on a healthcare payments technology provider resulted from the failure to implement multi-factor authorization, an industry standard and mandatory for baseline cyber-readiness. The ransomware breach affected the private data of approximately 190 million individuals. It led to a backlog of unpaid claims that left doctors' offices and hospitals with severe cashflow problems and threatened patients' access to care.[1] The direct financial impact on the company was likewise extreme, tallying $3.09 billion pre-tax.[2]

More like this

Podcast

On Aon Podcast: How has CrowdStrike Changed the Cyber Market?

Article

In July, the Crowdstrike outage served as a timely warning of the high risks associated with digital interconnectedness. The outage caused more than 8.5 million systems to crash, disrupting operations worldwide and impacting commercial flights, hospitals, and financial services.[3] One airline industry victim reported a $500 million revenue and $170 million expense impact.[4] Wrapping up the year, a ransomware attack on a U.S. supply chain management provider was felt around the world. This hosting environment disruption affected major organizations, including retailers and software and IT service providers.

Cyber Claims Rise. Payouts Decline

As cyber attacks persisted, the frequency of cyber claims grew across 2024, ranging from ransomware and business interruption to class action litigation and regulatory investigations — resulting in an increasingly complex incident response. In the U.S., for example, Aon Cyber and Errors and Omissions (E&O) claims data revealed 1,228 reported incidents across broking clients in 2024, reflecting an increase of 22 percent year over year. Cyber events or litigation represented most claims, with 776 reported matters in the U.S. — up a third on the previous year — and 320 reported matters in EMEA.

Aon U.S. E&O-Cyber Broking Reported Incident - Year

Raising a Red Flag: Cyber Risk Controls and Insurability

Report

Global Risk Management Survey

776

Reported cyber-incidents or litigation represented the most claims, an increase of 31% year over year.

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation
- Insurance Claim Management

Incident reports by year

Aon U.S. E&O-Cyber Broking Reported Incident - Quarter

Incident reports by quarter

Aon U.S. E&O-Cyber Broking Reported Incident

Cyber - Incident or Litigation

E&O - Professional Liability

E&O - Tech E&O

E&O - Media Liability

Other/ Unidentified

This increase was driven by a rise in cyber incidents, more organizations acquiring cyber insurance and a heightened regulatory focus on publicly disclosing material events. Aon analysts observed underinsurance and a lack of basic cyber readiness plans exposed mid-market organizations to significant risk.[5] Midsized organizations with $100 million to $2 billion annual revenue filed more claims than any other group, representing 52 percent of all matters.

Aon U.S. E&O-Cyber Broking Reported Incidents: 2024

Midsize ($100m -$2B)

Enterprise ($2B - $5B)

Global ($5B+)

SME ($0 - $100m)

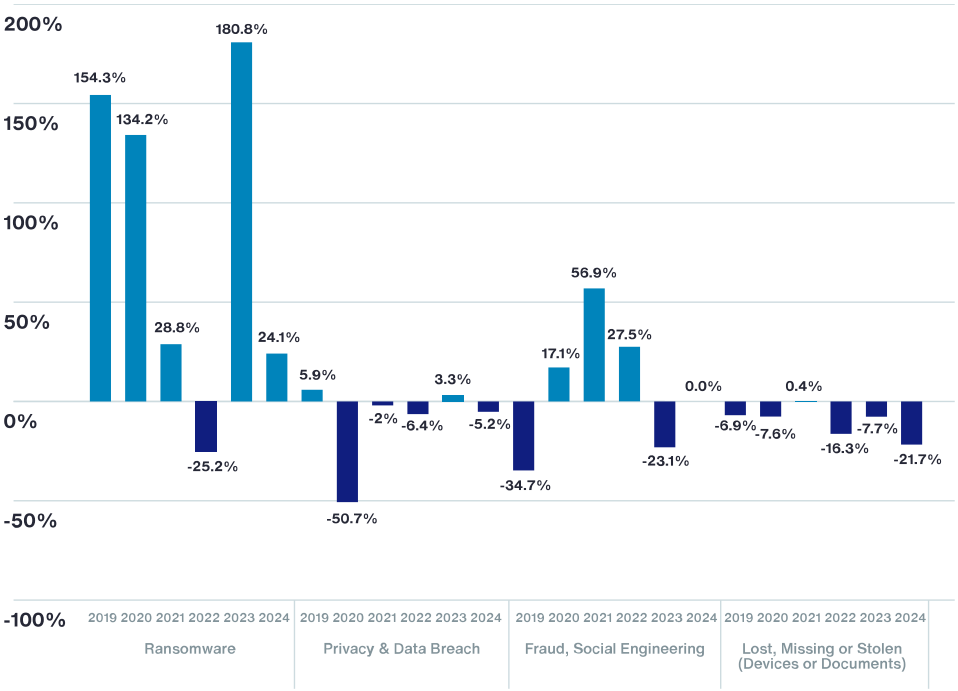
Response plans enable organizations to reduce the cost of a breach by an average of almost $500,000, providing reassurance about the effectiveness of these strategies.

Though the frequency of claims grew, claim ratio experience from a leading cyber insurer remained mostly static and even improved in 2024, decreasing by nearly 3 percent compared to 2023.[6] Despite pressure on premium rates, it was observed that Aon clients who invested in cyber preparedness were better able to respond to attacks with the technology controls and continuity plans to restore systems or regain access to data. IBM research found that having an incident response team and formal incident response plans enables organizations to reduce the cost of a breach by an average of almost $500,000, providing reassurance about the effectiveness of these strategies. [7]

Ransomware Persists

Ransomware incidents persisted in 2024, increasing 24 percent versus 2023. Fraud and social engineering remained flat while claims frequency for privacy and data breaches and lost, missing, or stolen data decreased.

Cyber Frequency Trend | Global Data*



Source: *Risk Based Security, analysis by Aon.

* Global dataset with a strong U.S. emphasis

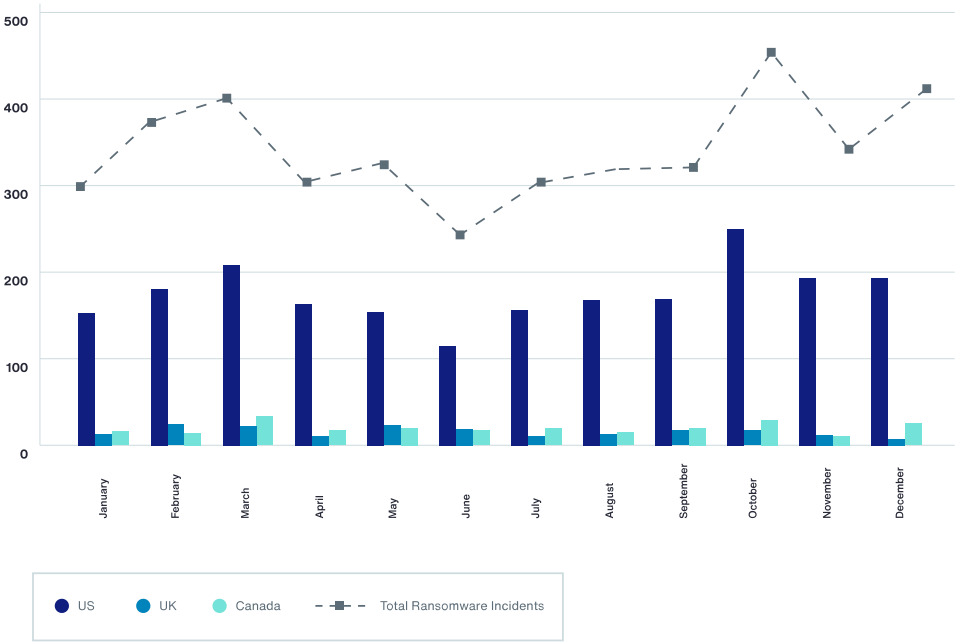
Despite the increased frequency of incidents, ransomware payment severity for Aon broking clients declined, likely supported by stronger cyber security controls.[8] The average reported payment amounts also dropped by 77 percent, helping to maintain a soft market.

This Aon client data aligns with Coveware's 2024 quarterly report[9] which shows that despite increased ransomware activity,

fewer companies are paying. The percentage of companies paying ransom dropped to an all-time low of 25 percent, marking a significant milestone in the fight against ransomware. While the average ransomware payment trended up in 2024, cresting at $553,959 in the fourth quarter of 2024, or an increase of 16 percent over the prior quarter. Meanwhile, median payments, which are typically a more reliable indicator of where the market is heading, are declining. The median ransom payment was $110,890 in fourth quarter 2024, a decline of 45 percent from the previous three months.[10] Global organizations such as the Ransomware Task Force, continue to identify ransomware threat actors and protect organizations. While successful, recent law enforcement actions to dismantle ransomware threat actor groups destabilized the space, giving rise to dozens of splinter groups.

Observed Ransomware Breach Trends | YE 2024

Top Targets by Country



Ransomware payment bans are back on the table as governments contemplate minimizing payments and compelling cybercriminals to cease attacking their countries' organizations.[11]

According to Aon's data, E&O Cyber Broking reported incidents trended up in 2024 with 1,228 events or an increase of 22 percent. As for observed ransomware breaches (ORBs), or instances of organizations named and/or having their data published on ransomware leak sites due to not paying, the U.S. dominated the charts with more than 50 percent of incidents. Consumer and industrial products, professional services and consulting and manufacturing were the top three targeted sectors, with the real estate industry running close behind, claiming 13 percent of total victims.

Ransomware Victims by Sector

Access claims trended up and down across the year. Access claims arise when threat actors, known as initial access brokers, breach organizations' networks and sell this unauthorized access to other threat actors, leading to ransomware attacks and malicious activities. Targeting Remote Desktop Protocol (RDP) tools was the method of attack for half of all access claims.

Top 10 Technology Types Targeted

Technology Type	Percentage Impact
RDP Tools	51.1%
Not Listed	21.5%
Corporate Remote Access Portals	14.0%
Corporate Application	3.9%
Remote Access Services	3.5%
Unspecified Technologies	1.1%
Other	1.0%
RMM Tools	0.8%
Email Platforms	0.7%

Technology Type	Percentage Impact
Goverment Application	0.6%

Based on Aon’s proprietary data, threat actors continue to favor remote access and other administrator tools over malware. Identifying non-standard applications remains a key challenge for victims, and threat actors use ORBs more frequently to keep attacks hidden. With perimeter devices such as firewalls and VPNs as the most common entry point for attackers, IT teams must be vigilant about patching, MFA, and cert-based authentication.

The Return on Security Investment

Entering 2025, we expect to see more organizations better able to manage their cyber risk. Insureds continue to use data modeling to help make better decisions and inform cyber purchasing decisions to determine the appropriate limit levels. Aon saw 21 percent of clients purchase additional limits in 2024 and we anticipate further increases in demand for cyber insurance and technology E&O insurance. Competitive market conditions in excess layers coupled with rate decreases across the tower in both the primary and excess layers helped to drive this increase in additional limits. However, organizations are constantly evaluating cyber risk. Risk analysis allows organizations to make better-informed decisions around their insurance risk transfer program, whether through higher limits, different program structures, or alternative risk transfer solutions.

References

[1] Chairman Brett Guthrie. What We Learned: Change Healthcare Cyber Attack. U.S. Department of Energy and Commerce. May 3, 2024. https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack

[2] United Health Group Incorporated. Form 8-K. January 16, 2025. https://www.sec.gov/ix?doc=/Archives/edgar/data/731766/000073176625000022/unh-20250116.htm

[3] Raphael Yahalom. What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk. Harvard Business Review. January 10, 2025.

[4] Delta Airlines Inc. Form 8-K. August 8, 2024. https://www.sec.gov/ix?doc=/Archives/edgar/data/0000027904/000168316824005369/delta_8k.htm

[5] Aon. A Middle Market Roadmap for Cyber Resilience. October 2, 2024. https://www.aon.com/en/insights/articles/a-middle-market-roadmap-for-cyber-resilience?collection=3ab7b09b-e783-4c99-b960-0be73fb4fa49&parentUrl=/en/insights/collections/cyber-resilience#aon-collection-detail-item-%7B0B90E4C1-2E4F-4BCC-BEC6-66BD640DB9D2%7D

[6] Beazley plc results for year end 31 December 2024. Beazley PLC. March 4, 2025. https://beazley2023tf.q4web.com/news/news-details/2025/Beazley-plc-results-for-year-end-31-December-2024/default.aspx

[7] IBM. Cost of a Data Breach Report. July 2024. https://www.ibm.com/reports/data-breach

[8] Aon 2025 Cyber Risk Report. Aon's existing and new client's Red flags decreased year-over-year across all industries. This supports Aon's broking's value proposition demonstrating a 5% improvement in critical security controls that may impact insurability.

[9] Will Law Enforcement success against ransomware continue in 2025? Quarterly Report. Coveware. February 4, 2025. https://www.coveware.com/blog/2025/1/31/q4-report

[10] Coveware. Law Enforcement Doxxing Raises Risk Profile for Threat Actors. November 1, 2024. https://www.coveware.com/blog/2024/11/1/law-enforcement-doxxing-raises-risk-profile-for-threat-actors

[11] Coveware. New Ransomware Reporting Requirements Kick in As Victims Increasingly Avoid Paying. Quarterly Report. January 26, 2024. https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying 9 https://www.coveware.com/blog/2025/1/31/q4-report

[12] Risk Based Security, analysis by Aon.

that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Cyber Risk Insurance Market Remains Buyer-Friendly

Key takeaways

After ten straight quarters of pricing decreases, cyber insurance pricing is still decreasing, ending with a 7% decline in Q1

2025. Broader coverage and increased limits are now available in most markets for risks with responsive cyber security controls.

Despite increased claims frequency, the average payment dropped by 77%. Insurers demonstrated remarkable resilience and loss ratios remained stable, serving as a testament to the stability of the market.

Systemic and third-party risks remain under-managed and deserve focus in 2025. Organizations are encouraged to model the total cyber risk exposure of large-scale systemic events.

Significant, systemic events dominated 2024 with Aon's Cyber Solutions U.S. data revealing 1,228 reported incidents across Aon's Cyber Solutions clients — an increase of 22 percent. Cyber incidents or litigation represented most claims, with 776 reported incidents — up 31 percent.

Aon U.S. E&O-Cyber Broking Reported Incident - Year

More like this

Article

Buyer-Friendly Cyber Risk Insurance Market Persists

Article

Ransomware Payouts Decline Despite Growing Cyber Claims Frequency

Article

Global Risk Management Survey

7%

cyber insurance pricing decline in Q1 2025, after ten straight quarters of pricing decreases.

Incident reports by year

Aon U.S. E&O-Cyber Broking Reported Incident - Quarter

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation
- Carrier-Aligned Security Assessment

Incident reports by quarter

Aon U.S. E&O-Cyber Broking Reported Incident

Cyber - Incident or Litigation

E&O - Professional Liability

E&O - Tech E&O

E&O - Media Liability

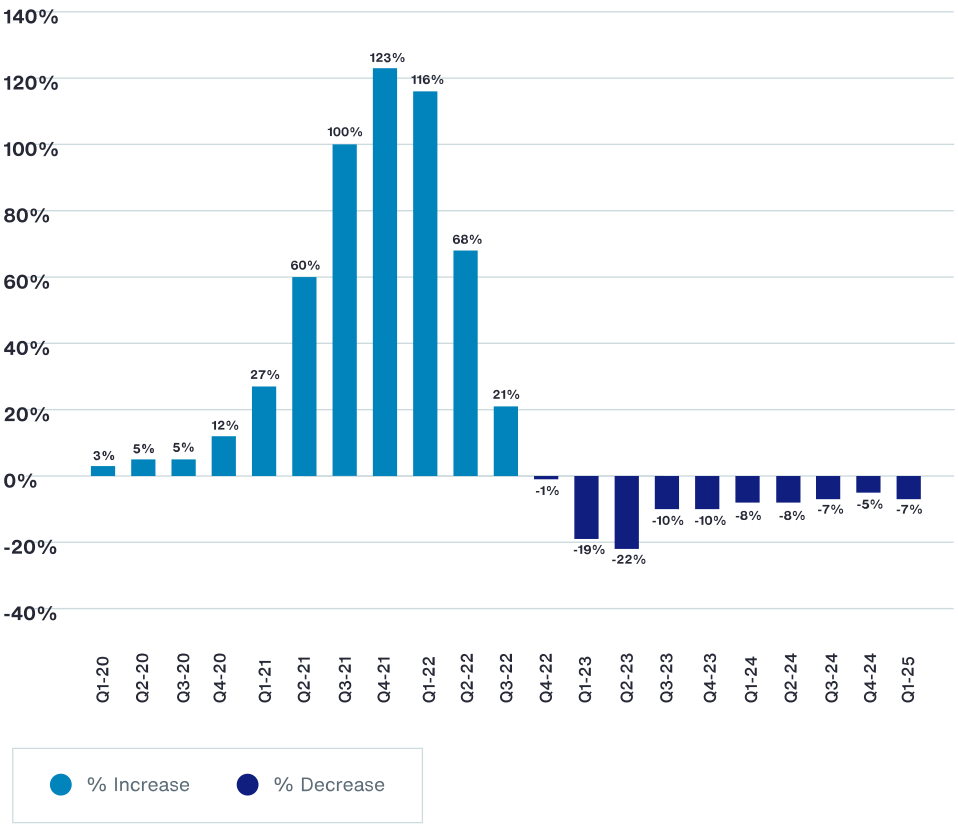
Other/ Unidentified

Despite increased claims frequency in 2024, insurer loss ratios were not materially impacted, and buyers' market conditions continued through 2024 for cyber amid a well-capitalized and competitive environment. Favorable conditions are expected to continue in 2025, supporting growth in emerging cyber markets; however, the juxtaposition of loss trends and a softening market could mean future market volatility. Risk differentiation remains key to favorable renewal outcomes over the long term."[1]

On average, buyers achieved a 7 percent premium decrease in Q1 2025, primarily driven by ample capacity, the introduction of new capacity and incumbent insurers being aggressive with renewal terms to maintain their incumbent renewals.

2020–2025 Cyber Premium Changes by Quarter

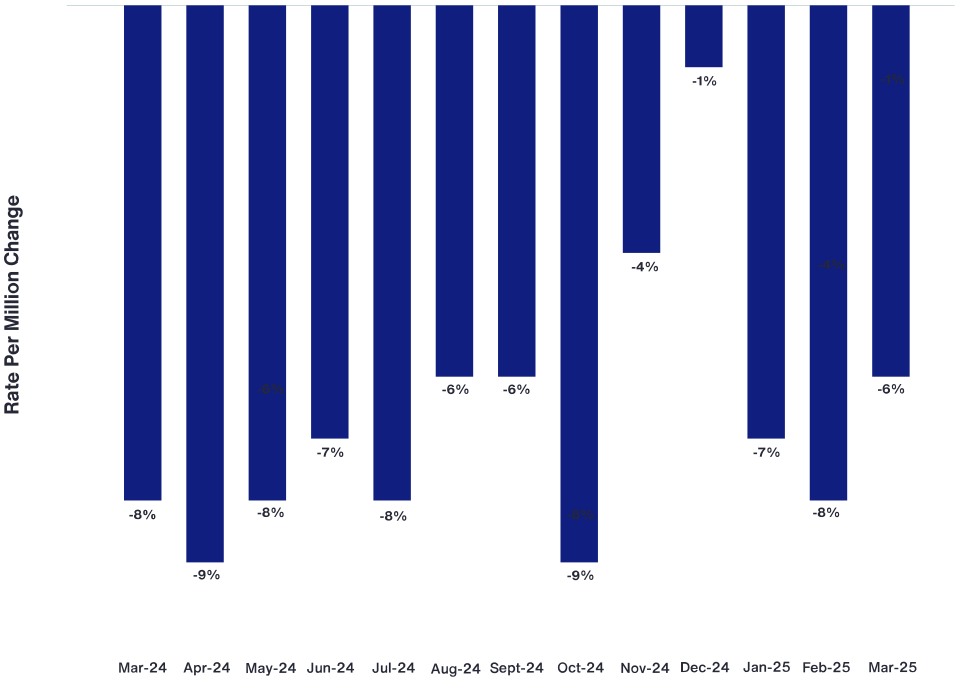
Average Year–over–Year Change (Same Clients)



Premium changes continued to decrease quarter over quarter while ransomware claims frequency was up.

Cyber Monthly Pricing All Layers

Average Year–over–Year Change (Same Clients)



ACT Data

Despite this difference in activity, it's still unclear how many of these ransomware incidents are claims with insurance recoveries, versus falling within the self-insured retention (SIR).[2]

The cyber retail and reinsurance markets demonstrated solid margins, supporting the view that the global cyber insurance industry is stable despite growing competition and the increasing sophistication, severity and frequency of cyber incidents.[3] Stronger competition has also resulted in lower self-insured retentions, premiums, an easing of required sub-limits and coverage enhancements for policyholders.[4]

In 2025, we expect pricing to continue to moderate, with more favorable conditions across an increasingly wider range of risks and geographies. Ample capacity and aggressive competition continue to drive a buyers' market for cyber despite an increase in

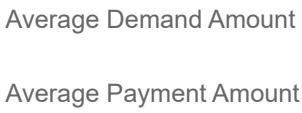
ransomware activity in prior years. In most markets, moderate rate reductions, broader coverage and increased limits are available for risks with responsive cyber security controls.

Looking to the reinsurance market in 2025, supply of capital from traditional sources remains abundant relative to current demand, with alternative capacity, such as insurance-linked securities and catastrophe bonds increasing in availability through innovative risk transfer structures. This supply-demand imbalance led to a favorable January renewal cycle for buyers of cyber reinsurance. The suite of reinsurance products and structures will continue to evolve and expand as cyber insurers seek new, more effective, ways to optimize their net position according to their risk appetite. This is a strong indicator that buyer-friendly market conditions, which include slightly lower premiums, broader coverage and more flexible terms, can be expected into the first half of 2025 for cyber insurance purchasers.

Cyber Insurance Steers Risk Mitigation

Cyber-attacks pose a growing balance sheet threat, with three-quarters of completed attacks leading to financial losses.[5] Adoption of cyber insurance is widespread and is a board-level consideration. It is reported that 90 percent of organizations with 500 to 1,000 employees have some form of cyber coverage, 50 percent have a standalone policy while 40 percent have cyber as part of a wider business insurance policy[6], and 25 percent of Aon clients purchased additional limits in 2024. Stricter underwriting by insurers demands that organizations invest in cyber preparedness to help secure a policy. This investment in readiness can benefit both insurers and insureds. Aon clients that invested in cyber preparedness in 2024 were better positioned to respond to attacks with technology controls and continuity plans in place to restore systems or regain access to data. Despite increased claims frequency across 2024, the average payment dropped by 77 percent. This paradox — rising claims but declining payments — helped to maintain the soft market.

Ransomware Severity (in $)



Key Observations:

In 2024, the average payment amount declined 77%, and the number of ransomware incidents remained flat, compared to the same period in 2023. Despite frequency increasing year over-year, the severity has declined supported by stronger cyber security controls, so we've remained in a soft market.

Despite a decrease in severity, the increase in frequency necessitates guidance around reporting and navigating notices.

Large-scale systemic events took center stage in 2024, as evidenced by the CrowdStrike outage that disrupted operations worldwide and impacted commercial flights, hospitals, and financial

services. Technology interconnectedness is growing, coupled with increased regulatory scrutiny on how organizations manage their systemic risks. In this uncertain operating environment, organizations should model their total cyber risk exposure through the financial quantification of relevant cyber scenarios and insurers need this high level of modeling to write or renew policies. Although the ransomware breach of a major healthcare payments technology provider in 2024 did not impact the cyber insurance industry directly, it caused associated and downstream losses for organizations that depended on that vendor. Aon is on the frontline in this trend, using more sophisticated models and tools that enable data-driven scenario analysis with its Cyber Risk Analyzer.[7]

It is expected that insurers will employ more robust modeling to help protect their portfolios against loss and close knowledge gaps around systemic and third-party risk. By leveraging quantitative modeling and underwriting, they can help improve decision-making to safeguard shareholder equity and help protect customers, employees and the public. This increased focus on advanced risk-selection technologies and claims management, including incident response (IR) and even specialized ransomware response teams, is also helping to make the cyber insurance industry more sustainable and propelling its development.[8]

Actions for Organizations

Use Decision Analytics. Cyber events can affect all areas of an organization, and regulatory bodies as well as shareholders are expecting a tighter focus on this risk. Aon's Cyber Risk Analyzer provides brokers and clients access to loss forecasting, exposure assessment and total cost of risk (TCOR), driving stakeholder alignment across the C-suite and enabling businesses to optimize their cyber-insurance programs relative to their unhedged loss potential.

Strengthen Cyber Security Posture. Systemic and third-party risks remain undermanaged and deserve focus in 2025. A privacy data breach, unauthorized access or disclosure of personal information, or loss of personal information can also have serious consequences. While a well-known topic, multi-factor authentication is still an underwriting requirement, as is a tested IR plan.

Be Strategic In-Market. Given the buyer-friendly market conditions, we advocate for insurers to offer expanded coverage to meet evolving risks. Organizations require broader coverage that addresses business and dependent business interruption, supply chain vulnerability, regulatory exposure inclusive of wrongful data collection events, and coverage for AI creation or usage-related events.

References

[1] Q4 2024: Global Market Insurance Overview. Aon. February 3, 2025. https://www.aon.com/en/insights/articles/global-insurance-market-overview-q4-2024

[2] Not limited to Aon E&O Cyber Broking clients.

[3] Cyber Insurance Market Outlook 2025: Cycle Management Will Be Key To Sustaining Profits. Manuel Adam and Koshimo Emura. S&P Global. November 27, 2024.

[4] Cyber Insurance Market Outlook 2025. Manuel Adam and Koshimo Emura.

[5] Addressing the insurance protection gap in the age of AI. David Molony. The Insurer. January 28, 2025.

[6] Cyber Insurance and Cyber Defenses 2024: Lessons from IT and Cybersecurity Leaders. Sophos. White Paper. June 2024. Cyber Insurance and Cyber Defenses 2024: Lessons from IT and Cybersecurity Leaders – Sophos News

[7] Turn to Cyber Risk Analyzer for Better Decisions…Every Day: https://assets.aon.com/-/media/files/aon/capabilities/cyber-resilience/aon245160-rims-placemat-cyber-risk-analyzer-v8.pdf

[8] Cyber Insurance Market Outlook 2025: Manuel Adam and Koshimo Emura. S&P Global. https://www.spglobal.com/ratings/en/research/articles/241127-cyber-insurance-market-outlook-2025-cycle-management-will-be-key-to-sustaining-profits-13323968

[9] ACT Data

the advice of legal counsel or a cyber insurance professional and should not be relied upon for any such purpose. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Raising a Red Flag: Cyber Risk Controls and Insurability

Key takeaways

Aon clients who invested in security controls reported a significant 9% improvement in

critical — or ‘red flag’ — controls. This may impact insurability.

Cyber insurance carriers moved towards a more holistic view of cyber risk resilience.

Prioritization of controls and red flags continued to change in 2024, with privacy-oriented, third-party and supply chain controls emerging as new areas of interest for insurance.

Security measures and frameworks continue to be mission-critical in the battle against cyber threats, and organizations across sectors continued to invest in and improve their critical controls over the course of 2024.

At the same time, insurance carriers have become more sophisticated in risk underwriting, requesting less information than before. Where insurers might have looked at a weak control a few years ago and taken a firm position, this was no longer the case. As opposed to the long-established approach, if you have control “X,” then the result “Y” ensues, carriers became more focused on the overall cyber maturity profile and proved more receptive to accepting an organization’s narrative around specific controls. This approach rang true with larger, more mature organizations, as many insurers accepted updates on security road maps and confirmation that controls were in place without scrutinizing

More like this

Article

Buyer-Friendly Cyber Risk Insurance Market Persists

Article

Ransomware Payouts Decline Despite Growing Cyber Claims Frequency

evidence that controls were tested and effective. This new climate that emerged in 2024 was driven in part by intense global cyber insurance market competition and is expected to continue into 2025.

Despite the changing requirements for cyber insurance, global data indicates that organizations continue to invest in cyber security. Aon client organizations who invested in cyber security control improvement demonstrated robust preparedness against cyber, reporting a 9 percent improvement in critical — or “red flag” — controls that may impact insurability.

Renewal Clients Red Flags by Industry

Report

Global Risk Management Survey

9%

improvement of critical red flag controls year over year, demonstrating investment and implementation of critical security technology continues to advance.

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation
- Carrier-Aligned Security Assessment

2023

2024

* ‘Other Industries’ category represents responses from clients in the following industries: Financial Sponsors, Food, Agribusiness, & Beverage, Hospitality, Travel & Leisure, Insurance, Life Science, Natural Resources, Sports & Entertainment.

Notable improvements were reported by the financial (21 percent), professional and business services (12 percent) and industrial and manufacturing sectors (11 percent). Clients also stated improvement in operational technology (OT) red flags, with a seven percent increase. Notably, OT environment segmentation, multi-factor authentication (MFA) for employee remote access to OT and endpoint detection and response in the OT environment improved.

All Clients Operational Technology (OT) Red Flags

2023

2024

This shows how organizations think across the whole enterprise, fortifying defenses against external access and exploitation and increasing the ability to detect cyber events rapidly.

Privacy-Oriented Controls. A Growing Priority

Despite overall cyber security improvements, significant breaches persisted across 2024, exploiting vulnerabilities such as weak MFA controls and third-party diligence. As risks dynamically change and threat actors shift their tactics, controls remain a moving target. The prioritization of different security controls continues to evolve, making organizations often uncertain about where to focus security investment. A data analysis of security controls to risk can help illuminate potential exposure to loss.

Privacy-oriented controls emerged as a focus for insurance carriers in 2024. This shift is in response to the increasing legal scrutiny of

how insured entities handle personal information. This scrutiny was particularly noticeable in the U.S., where data breaches have led to multi-plaintiff or class action lawsuits.[1] These lawsuits piled up in 2024 in response to numerous healthcare breaches alleging violation of patient privacy rights, including sharing data with third parties.[2] As new technologies such as AI emerge, class action lawsuits are evolving. Companies are also facing a new cyber threat based on “pixels,” code embedded in webpages or mobile apps from third-party providers to collect information about a user’s interaction.[3]

Regulatory shifts also play a significant role in shaping the focus on privacy. More states across the U.S. are working to pass laws and regulations that emulate both the California Consumer Privacy Act (CCPA) — which protects consumers’ data privacy and security, including from cyber attacks, fraud and mistakes — and the European Union’s Digital Operational Resilience Act, which requires financial institutions to incorporate data protection and privacy risks into their overall Information and Communication Technology risk assessments.[4]

Recommended Actions

- Work with your cyber insurance broker to review controls and claim sources. Control improvement helps to reduce claim frequency and severity and helps build cyber risk resilience.
- Conduct a data-driven analysis of your organization’s cyber risk posture to inform decision-making about security investments. Understand controls from both a risk and an insurability perspective.
- Develop an action plan to address critical risks that could increase your organization’s likelihood of being attacked. Importantly, build resilience in privacy and third-party cyber security.

References

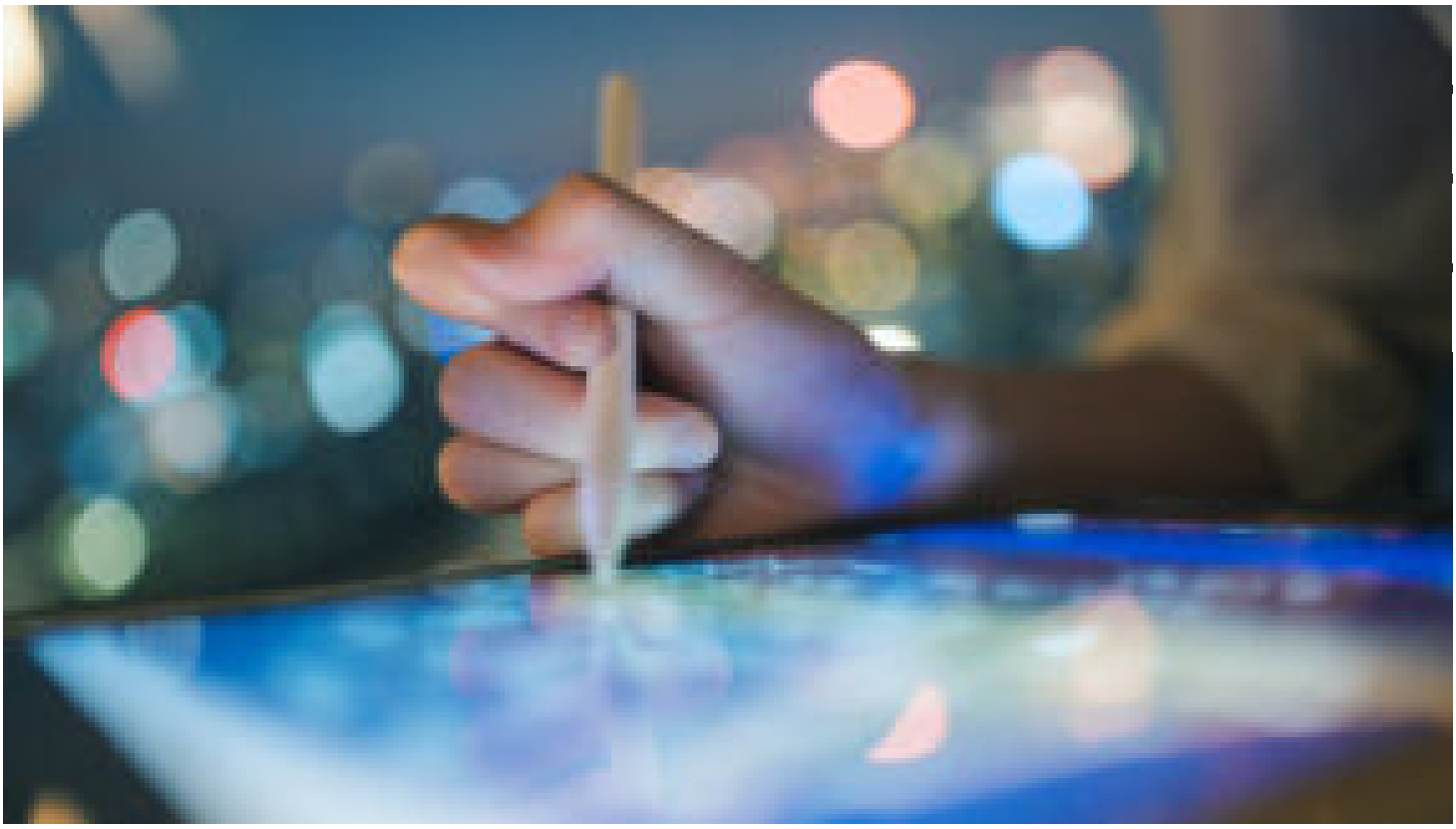
[1] Emerging Legal Issues in Data Breach Class Actions. American Bar Association. Business Law Report. Joseph Yenouskas and Levi Swank. July 17, 2018.

[2] Class Action Lawsuits Pile Up After Healthcare Data Breach. The HIPAA E-Tool. February 11, 2025. https://thehipaaetool.com/class-action-lawsuits-pile-up-after-healthcare-data-breach/

[3] Pixels and Privacy. A New Wave of Class Action Litigation. LAW.COM. Ian M. Ross and Sidley Austin. March 15, 2024.

[4] Digital Operational Resiliency Act. European Insurance and Occupational Pensions Authority.

Finance and Insurance Industries: Managing Risk in a Rapidly Evolving Environment



Key takeaways

Clients reported an improvement in overall cyber risk score in 2024, with the average industry score indicating risks are now “managed.”

Third-party risks are responsible for a significant and growing proportion of data breaches.

Basic IT controls remain an issue for some middle-market companies and small and medium-sized enterprises, with 15% –25% lacking multifactor authentication across a range of key systems.

Financial institutions continue to be the backbone of the global economy. A cyber attack that compromises the operations of a financial institution can have a major effect on the ability to access finance and payment systems, with direct impacts for markets, businesses across sectors and the general public. As a result, issues related to cyber security are highly regulated. Reflecting the importance of this issue, the International Monetary Fund made the growing threat of cyber attacks, and the knock-on potential impact

More like this

Article

Third-Party Risks Can Create Cyber Challenges for

for macroeconomic stability, a major theme of its April 2024 Global Financial Stability Report.[1]

The sector faces an increasingly complex risk landscape — as can be seen in the recent high-profile attacks targeting both companies and government agencies. In April 2025, the U.S. Department of the Treasury's Office of the Comptroller of the Currency, whose role is to regulate and supervise U.S. and foreign banks, announced that the emails of executives and other employees of the agency had been hacked, blaming long-standing vulnerabilities for the breach.[2]

The finance and insurance industries are well aware of the extent of these risks. Industry leaders ranked the threat of a cyber attack or data breach as the top risk in Aon's most recent Global Risk Management Survey.[3] As a result, these industries are constantly seeking to understand the changing shape of the threat environment and get ahead of it. There are signs that these efforts are starting to pay off — at least for enterprise and global clients. On average, the global risk score for finance and insurance organizations is higher than for other sectors, though scores do vary significantly according to the size of the organization and other factors.

But companies still have a lot of work to do in building their cyber resilience. Vulnerabilities still exist across the sector, particularly around third-party and application security. In addition, and of particular concern, many small and medium-sized enterprises (SMEs) and mid-market companies still lack basic controls, such as multifactor authentication, for key systems.

The cyber-insurance market has matured a great deal over the past few years. Previously, financial institutions were thought to represent a vertical that was "high risk," or difficult to place, but now they are among the organizations that present the most attractive risks for the cyber market. The amount of regulatory scrutiny that these companies face on a daily basis means that they are among the most well-managed businesses from a cyber perspective.

In addition, the banks and insurance companies of today increasingly view themselves as financial technology businesses

Healthcare

Article

Cyber Risk in an Increasingly Digitalized Manufacturing Sector

Report

Global Risk Management Survey

29%

Middle-market and SME clients that still report a lack of multifactor authentication on backups

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation

rather than “just” financial institutions and believe that digital transformation has forced the market to step up and expand the scope of cyber-insurance offerings available to those businesses. The supply of willing risk transfer capital has continued to expand, which means that financial institutions of all sizes can now enter the market confident that they will be provided with cyber risk-transfer programs that meet their needs.

Insurance Claim Management

Cyber Attacks Can Still Cause Significant Damage in the Finance and Insurance Sector

In addition to the broad geopolitical, macroeconomic and technological factors that have complicated the operating environment and increased cyber risks across industries, the finance and insurance industry has several features that render cyber attacks particularly problematic. First, the industry is highly interconnected, and the shared use of a number of platforms and services can significantly increase the magnitude of any cyber attack.

Second, many of today’s banks and other financial institutions are the result of decades of mergers and acquisitions, which means that cyber-related infrastructure can be a tapestry of different systems with different levels of sophistication. In addition, rapid growth in fintech and broader digital assets — which may not be governed by the same regulations as the industry at large — continues to exponentially expand the potential attack footprint and introduces even more third-party vulnerability to larger financial institutions. Third-party attacks are a growing issue, with a recent report indicating that these attacks are responsible for most data breaches reported by the top 150 insurance companies.[4]

Last, a cyber attack that compromises service availability — even for a very short period — can have very serious implications for finance and insurance customers in a way that is not necessarily true for other industries. The relationship between a bank and its customer is based on reputation and the customer’s trust in their ability to access and move money, among other factors. Losses or issues with access — even if relatively minor — can damage that

relationship to the extent that the customer may decide to take their business elsewhere, possibly leading to a run on the bank.

Aon Clients Report: Finance and Insurance Industry and Cyber Risk

The proportion of finance and insurance companies' information technology budgets that is spent on security has risen globally over the last few years. Companies reported that 9 percent of their IT budget was dedicated to security in 2024, compared to 8 percent in 2022. And this increased investment is beginning to pay off. Aggregated data results from Aon's Cyber Quotient (CyQu) show that clients reported overall risk score improvement from 2.92 in 2022 to 2.96 in 2024 across all finance and insurance companies, indicating that risks are, on average, "managed." These scores indicate that the finance and insurance industry is further along on managing risk than many other industries, including both healthcare (2.82) and manufacturing (2.53).

The risk score varies according to the size of the organization, with large companies notably more advanced than smaller companies. Reported risk scores improved between 2022 and 2024 for small and midsize entities (2.8, up from 2.7) and global companies (3.3, up from 3.0), while remaining consistent for enterprise and mid-market entities at 3.2 and 3.0, respectively.[5]

When looking at risk score by cyber domain, companies generally score best on endpoint and network security. Unsurprisingly, given the known issues around third-party vulnerabilities discussed above, they score least well — on average — for application security and third-party security, creating potential opportunities for threat actors. Risks around backups and business resilience also continue to be an issue, which is particularly problematic given the ongoing issues with ransomware attacks.

Cyber Domains | 2024 Financial Institutions and Insurance

Overall Risk Score 2.96

Highest Scoring

3.21 Endpoint Security	Logging & Monitoring	3.35
	Endpoint Protection	3.31
	Secure Config.	3.18
3.15 Network Security	Pen Testing	3.57
	Enviroment	3.12
	Capacity	3.07
3.12 Data Security	User Awareness Training	3.47
	Governance	3.25
	Data Protection	3.06

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Lowest Scoring

2.49	Software Mgmt.	2.30

Application Security	Training	2.50
	Secure Dev.	2.65
2.62 Third Party	Due Diligence	2.49
	3rd Party Contracts	2.54
	3rd Party Inventory	3.27
2.91 Business Resilience	Backup	2.71
	Incident Response	2.94
	BCM/DR	3.03

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Looking to the U.S. in particular, Aon's CyQu red flag controls data shows that, year-over-year, our renewal clients' red flags dropped by 15 percent, a substantially faster rate of improvement than the industry average of 9 percent. Almost 70 percent of middle-market and small and medium-sized enterprises now have an incident response plan for ransomware, and the same is true for over 80 percent of our global and enterprise clients — a substantial improvement over prior years.

There is, however, still plenty of room for improvement, particularly for middle-market and SME companies. The data indicates that over 25 percent of these companies do not have multifactor

authentication (MFA) for backups, and 15 to 20 percent also lack MFA on corporate emails and domain admin emails. More than 40 percent do not have backups stored at a secondary data center. Controls such as these are fundamental to effective cyber-risk management, and their absence could render these companies effectively uninsurable, despite the market being broadly favorable for finance and insurance companies. Companies lacking these basic controls should move to fill these gaps as soon as possible.

Global and enterprise clients perform better on these fundamental controls, although — again — there is more they can do to effectively manage risks. Almost half of these companies, for example, do not yet scan 100 percent of the enterprise for cyber vulnerabilities.

Top 10 Critical Red Flags | 2024 Financial Institutions and Insurance - Global & Enterprise

2024

Globally, fewer than 5 percent of ransomware attacks appear to have targeted financial services companies,[6] a significantly lower percentage than for many other industries. This comparatively small number of attacks is likely explained by the industry's greater degree of sophistication in managing cyber risk.

Key Observations | 2024 Financial Institutions and Insurance - Ransomware Victims by Sector (Threat Intel)

Consumer & Industrial Products

Professional Services & Consulting

Manufacturing

Real Estate

Life Sciences & Healthcare

Public

Technology, Media & Telecom

Energy, Resources & Agriculture

Nonprofit

Financial Services

Others

Now What? Action for Finance and Insurance Organizations

While finance and insurance companies are generally further along on managing risk than those in other industries may be, there is still room for improvement. In addition, companies continue to vary considerably on their progress. Those looking to decrease risk exposure — as well as improve the terms of their cyber-insurance policies — should consider action across these five areas among others they may deem appropriate for their individual organization.

Invest in Cyber Resilience: Many companies are considering pulling back from major investments as a result of economic uncertainty, but they could face challenges if they defer investments related to managing cyber risk. Instead, companies need to continue to build — and keep investing in — cyber resilience. Customer and regulatory demands are becoming ever more stringent, and successful organizations will need to continue to meet or exceed those standards. At the same time, threat actors are always searching for new ways into an organization. Companies will need to identify and manage weaknesses. Unpatched vulnerabilities, for example, are an easy way for diligent attackers to access a company's systems, with these risks increasing as AI continues to become more sophisticated. Email and phishing once provided the primary entry point, but as many organizations deploy MFA, attackers have pivoted to compromising business emails and other strategies.

Map and Manage Third-Party Risks: In a breach, it is important to understand who is responsible for

response and recovery. Companies should ensure they have a full and up-to-date understanding of third-party vulnerabilities and undertake regular scenario planning related to third-party cyber events. Organizations will also need to ensure that they have a risk transfer program to help mitigate the effects of a cyber event by protecting the balance sheet and alleviating issues arising from income loss.

Optimize Cyber Insurance: Cyber insurance should be considered an integral part of the organization's approach to managing cyber risk. Instead of thinking about cyber risk as a technology issue or merely an insurance issue, companies should approach these risks from an enterprise point of view. Cyber-insurance solutions should be adapting to reflect the shift that financial institutions are making to become joined-up technology-driven businesses. With that in mind, companies may find that they have more than one option to transfer and manage cyber risk. It may make sense to transfer a portion to the cyber-insurance market, but companies should also consider alternative risk retention or self-insurance financing strategies, in addition to continued upgrading of processes and controls.

Prepare for Ransomware Attacks: Ransomware attacks can wreak havoc on operations, causing significant financial and reputational damage, and both insurers and regulators are increasing their scrutiny in this area. Companies should act now to put the best tools, processes and other resources in place to build better resilience to these attacks. They should also test those defenses regularly, including developing the ability to

help remediate damage effectively and quickly. Ensuring quick access to clean backups will also be vital.

Track Ongoing Regulatory Developments: Complying with the EU's Digital Operational Resilience Act (DORA) remains a major focus across Europe.[7] For many companies, this legislation means going beyond check-box compliance and conducting regular assessments across technical defenses, control maturity, financial impact and insurability. However, simply complying with existing legislation is not sufficient. Given regulatory uncertainty in the U.S. and variations in the extent of DORA implementation across European countries,[8] companies will also need to keep a close eye on both regulatory developments and the impact that these may have on their business.

References

[1] Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks, International Monetary Fund, April 2024, https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024.

[2] "US regulator OCC says its executives' emails were hacked," Reuters, April 8, 2025, https://www.reuters.com/technology/cybersecurity/us-regulator-occ-notifies-congress-major-security-breach-2025-04-08/.

[3] Ninth Edition: Global Risk Management Survey, Aon, 2023/2024, https://www.aon.com/en/insights/reports/global-risk-management-survey.

[4] Joe Toppe, “Most top insurer data breaches result from third-party attacks,” PropertyCasualty360, February 7, 2025, https://www.propertycasualty360.com/2025/02/07/most-top-insurer-data-breaches-results-from-third-party-attacks/.

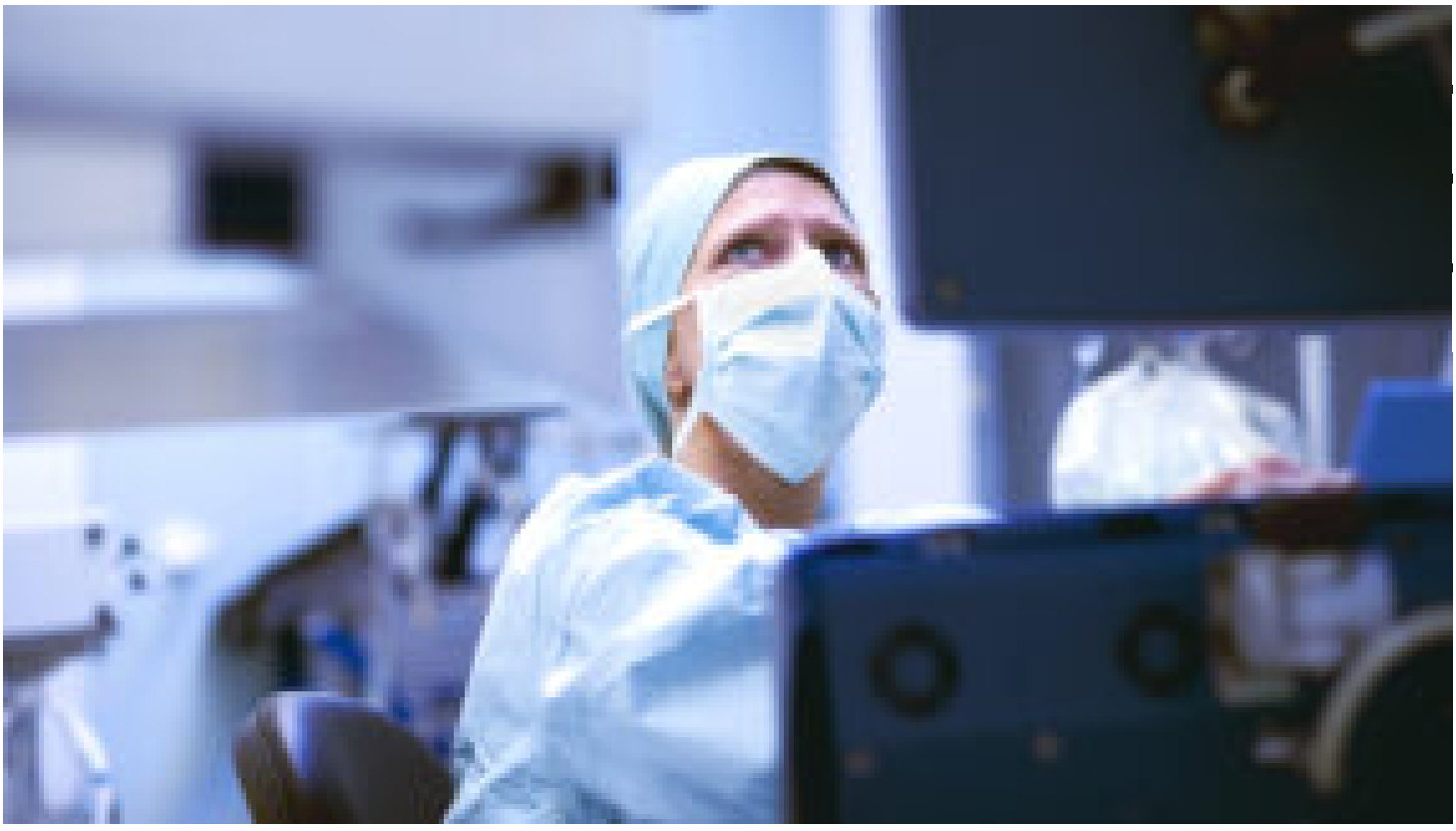
[5] CyQu Enterprise Edition response data analysis for 2024, Aon.

[6] According to both Aon Intelligence team analysis of information posted on ransomware leak sites on the dark web and Aon Access Claims data.

[7] “Digital Operational Resilience Act (DORA),” European Insurance and Occupational Pensions Authority, accessed May 30, 2025, https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[8] Javvad Malik, “Exploring the Implications of DORA,” Information Security Buzz, April 8, 2025, https://informationsecuritybuzz.com/exploring-the-implications-of-dora/.

Third-Party Risks Can Create Cyber Challenges for Healthcare



Key takeaways

Healthcare organizations spend an average of 7% of their IT budgets on cyber security — lower than many other industries.

A significant proportion of healthcare organizations still lack basic resilience-related cyber controls.

AI is opening many new fronts for potential cyber risks which will require updated insurance products, as well as training and human intervention.

The impact of cyber attacks in the healthcare industry can be catastrophic. Healthcare organizations hold a wealth of very sensitive information, and the theft of client and patient data and intellectual property can have serious financial, reputational and regulatory consequences. On top of that, cyber security breaches in medical-device and medtech organizations can threaten the health — and even the lives — of patients.

The healthcare sector also faces its own unique set of challenges when it comes to managing cyber risks. First, many organizations — including hospitals and clinics — continue to suffer from a

More like this

Article

Finance and Insurance Industries: Managing Risk in a Rapidly Evolving Environment

shortage of IT talent.[1] Second, budgets are often tight, making it difficult to secure the funding needed to manage cyber risk. Our data suggest that healthcare organizations spend a median of 7 percent of their IT budget on security, which is lower than manufacturing organizations (8 percent) and finance and insurance organizations (9 percent).[2]

Meanwhile, healthcare organizations have embraced a broad variety of digital innovations, from incorporating hybrid cloud technology to deploying wearable devices and telehealth applications enabled by AI — all of which can increase the number of entry points for threat actors. In 2024 alone, for example, the FDA approved 107 new medical devices, bringing the total number of approved devices to 1,016 — up from just six in 2015.[3] The more internet connectivity an organization creates, the larger the cyber-attack surface can become. AI powered methods also open many new fronts of potential cyber risk,[4] of which privacy and security represent only one. Insurance products are being updated to help transfer these risks, but training and human intervention will also be very important in any effective holistic risk management strategy.

In addition, these new technologies — as well as the outsourcing of a number of functions, including IT management — require healthcare organizations to work with a broad range of smaller companies, many of which may have a lower level of cyber sophistication and security. These third- and fourth-party risks have increased significantly in recent years and are a major concern for many organizations. The recent uptick in mergers and acquisitions activity in the healthcare sector in recent years has also led to the introduction of similar risks related to mismatched cyber controls.

Healthcare organizations are often a top target for cyber attackers and it's perhaps not surprising that healthcare organizations ranked a cyber attack or data breach as their number one risk in AON's 2023 Global Risk Management Survey.[5] As the American Hospital Association (AHA) reports, both the rate and severity of cyber attacks on hospitals have risen dramatically over recent years, with 259 million Americans' healthcare records having been stolen in full or in part by the end of 2024.[6]

Article

Cyber Risk in an Increasingly Digitalized Manufacturing Sector

Report

Global Risk Management Survey

58%

of mid-market and SME clients in Healthcare reported they had not performed a tabletop exercise during the preceding 12 months.

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation

Insurance Claim Management

As a result, healthcare organizations must be laser-focused on managing cyber risks. Patients, insurers and regulators are putting pressure on the industry to meet cyber-resilience standards — including through legislation such as the Health Insurance Portability and Accountability Act and the Health Information Technology for Economics and Clinical Health Act — and the penalties imposed for noncompliance or data breaches can be significant.[7]

To stay ahead of cyber risks and legislation, healthcare organizations need to look at their cyber risk holistically and understand the full range of risk transfer strategies and mitigation measures. While the breadth of coverage available to healthcare organizations through cyber insurance has increased in a competitive insurance market, there is also increased scrutiny on key aspects of cyber maturity — including cyber resilience. Companies that lack key cyber-security controls may struggle to secure insurance and may achieve less favorable outcomes in the insurance market.

Aon Clients Report: The Healthcare Industry and Cyber Risk

Aon's Cyber Quotient Evaluation (CyQu) data show that overall risk scores for healthcare organizations improved marginally from 2.76 out of 4 in 2023 to 2.82 in 2024. These scores mean that on average, healthcare organizations perform slightly better than manufacturing organizations (2.53), which tend to be less highly regulated, but not as well as finance and insurance organizations (2.96). As is generally the case across sectors, global and enterprise companies score higher (3.06 and 3.02, respectively) than mid-market organizations (2.85) and small and midsize enterprises (SMEs) (2.66).[8]

Looking at risk score by cyber domain, healthcare organizations score highest for endpoint security, network security and data security, on average. These areas are of particular importance for the industry and have been a major focus of cyber security

investments. Perhaps unsurprisingly, given the issues highlighted above, they score lowest for business resilience and third-party cyber due diligence. But these areas are attracting increased scrutiny across the healthcare sector and from insurers, and we expect to see a growing focus on managing these risks in the coming years. Scores are also low for application security, though these risks may have less relevance for companies in the healthcare sector because many do not develop their own software applications.

Cyber Domains | 2024 Healthcare Providers & Services Industry

Overall Risk Score 2.82

Highest Scoring

3.07 Endpoint Security	Endpoint Protection	3.22
	Logging & Monitoring	3.20
	Secure Config.	3.05
3.03 Network Security	Pen Testing	3.28
	Enviroment	3.01
	Wireless	2.94
2.98 Data Security	User Awareness Training	3.37
	Governance	3.01
	Data Protection	2.96

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Lowest Scoring

2.40 Application Security	Software Mgmt.	2.37
	Training	2.42
	Secure Dev.	2.49
2.44 Third Party	Due Diligence	2.25
	3rd Party Contracts	2.56
	3rd Party Inventory	3.00
2.66 Business Resilience	BCM/DR	2.57
	Backup	2.71
	Incident Response	2.72

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Looking to the U.S., Aon's Ransomware Supplemental Applications red flag controls data show that year over year, our renewal clients' red flags decreased by 14 percent, significantly higher than the cross-industry average of 9 percent.

However, there is still significant room for improvement, particularly regarding resilience-related controls and for mid-market organizations and SMEs. A significant proportion of these smaller organizations still lack several relatively basic controls; for example, 58 percent reported they did not have an annual tabletop exercise, and 30 to 50 percent reported lacking backups stored in a secondary data center, an incident response plan for ransomware, or MFA for backups. Addressing these issues as well as the lack of several other resilience-related controls would be relatively straightforward and should be a priority for healthcare organizations.

Addressing a lack of vulnerability scans across 100 percent of the enterprise will be much more challenging for organizations of all sizes given the rapid churn in providers and ongoing M&A activity across the sector.

Top 10 Critical Red Flags | 2024 Healthcare Providers & Services

Global & Enterprise

2024

Middle Market & SME

2024

Given the size and prominence of the sector, it is perhaps unsurprising that a significant portion of ransomware attacks appear to have targeted healthcare organizations.[9] Underreporting of attacks will likely be particularly prevalent in this sector.

Key Observations | 2024 Healthcare Providers & Services Industry

Ransomware Victims by Sector (Threat Intel)

Consumer & Industrial Products

Professional Services & Consulting

Manufacturing

Real Estate

Life Sciences & Healthcare

Public

Technology, Media & Telecom

Energy, Resources & Agriculture

Nonprofit

Financial Services

Others

Target Victims by Sector (Q4’24 Access Claims)

Unknown

Consumer & Industrial Products

Professional Services & Consulting

Public

Technology, Media & Telecom

Real Estate

Manufacturing

Life Science & Healthcare

Non Profit

Energy, Resources & Agriculture

Others

Financial Services

Now What? Actions for Healthcare Organizations

Understand Your Exposures

Healthcare organizations need to develop a detailed and regularly updated understanding of their control maturity and cyber vulnerabilities and of the potential impacts of those vulnerabilities. The full range of potential losses should be quantified to better inform budget decisions. This detailed understanding of cyber risk can then be used to help choose the highest-priority risk mitigation measures to assess available risk-transfer solutions.

Healthcare organizations have sometimes been slow to integrate cyber risks related to new technologies. They will, however, need to face technology-related issues head-on, especially given the rapid adoption of AI across the sector. One of the first steps to an effective risk management strategy will be gaining a full understanding of current technology-related risk exposure and its likely evolution.

Manage Third-Party Risks

Understanding and managing cyber risks related to third parties, vendors and potential M&A transactions is becoming more important across the healthcare sector. While many healthcare organizations were early adopters of vendor and business partnership due-diligence agreements, most organizations lacked the resources to verify that all their vendors were complying.

Given the volume of third parties that many healthcare organizations work with, they will need to scrutinize their vendors in terms of cyber risk. Those seen as critical — for example, those with access to electronic health records — should face additional due diligence checks.

Healthcare organizations will also need to ensure they are resilient to cyber events affecting their suppliers, including by considering how they can disconnect from their vendors and ensure business continuity.

Take a Holistic Approach to Building Cyber Resilience

While access management remains an issue and cannot be ignored, healthcare organizations will also need to increase their focus on building their cyber resilience. An early step should be ensuring all basic controls — including using MFA for backups, storing backups in a secondary data center and holding tabletop exercises at least once a year — are in place, especially given that many of these controls are relatively easy to implement.

Aligning incident response and business continuity planning should also be a priority. Organizations should conduct diagnostic reviews of existing plans and run business impact analyses. They should also break down silos as much as possible to get a 360-degree view of risk and to ensure that goals, processes and procedures are aligned. Leveraging the strength of existing enterprise emergency operations centers can also help build cyber resilience.

The Network and Information Security (NIS2) Directive,[10] an EU-wide piece of legislation that applies to healthcare, life sciences and pharmaceutical organizations, came into force in 2024. Some of the biggest changes under NIS2 are the specified management liabilities and administration fines for noncompliance. The legislation calls for direct action in some key cyber-security areas and outlines new controls that must be implemented, along with new guidance on how significant incidents should be reported. However, the extent to which NIS2 is implemented varies by

country within the EU, just as data breach laws can vary by state in the U.S.

Organizations will need to understand shifts in and impacts of legislation. Over recent years, for example, a number of plaintiffs' law firms in the U.S. have been taking advantage of some of the regulations targeted at healthcare companies to initiate a number of class actions. As a result, many hospitals have spent a considerable amount of money defending themselves against online tracking/pixel lawsuits.[11] Healthcare organizations should ensure they are well prepared for regulatory shifts, including by implementing appropriate governance structures.

References

[1] "Cyber Security Talent Gap: Use These Solutions to Help Rectify Ongoing Issue," Aon, January 2023.

[2] CyQu Enterprise Edition response data analysis for 2024.

[3] Artificial Intelligence Index Report 2025, AI Index Steering Committee, Stanford University Human-Centered Artificial Intelligence, April 2025.

[4] "The Role of Risk Management in the Age of Generative Artificial Intelligence," Aon, January 7, 2025.

[5] "Top Risks Facing Healthcare Organizations," Aon, November 28, 2023.

[6] John Riggi, "3 Must-know Cyber and Risk Realities: What's Ahead for Health Care in 2025," American Hospital Association, April 3, 2025.

[7] "Implications of Noncompliance with HIPAA: What to Expect as a Healthcare Organization," Compliancy Group, April 19, 2023.

[8] CyQu Enterprise Edition response data analysis for 2024.

[9] According to both Aon Intelligence team analysis of information posted on ransomware leak sites on the dark web and Aon Access Claims data.

[10] "NIS2 Directive: securing network and information systems," European Commission, updated July 1, 2025.

[11] Melissa Bilancini, Alexander Vitruk, Aleksandra Vold and Lynn Sessions, "DSIR Deeper Dive: Tracking the Crackdown on Tracking/Pixel Technologies: Web Litigation and Regulatory Landscape – Part 1," Baker & Hostetler, November 6, 2024.

Insurance products and services are offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida, and their licensed affiliates.

The information contained herein and the statements expressed are of a general nature, not intended to address the circumstances of any particular individual or entity and provided for informational purposes only. The information does not replace the advice of legal counsel or a cyber insurance professional and should not be relied upon for any such purpose. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Cyber Risk in an Increasingly Digitalized Manufacturing Sector

Key takeaways

In spite of a challenging risk environment, the overall cyber-risk profile of manufacturers remained flat between 2022 and 2024.

Aon's red flag controls data indicating that companies of all sizes lack several key resilience-related cyber controls.

Manufacturers need to understand and manage current and developing risks, segment IT and OT environments and invest in response and recovery.

The manufacturing sector is a leading driver of growth around the world— employing more than 150 million people and adding some $13 trillion a year to the global economy[1]. It's little wonder then that any cyber attack on the sector has wide-ranging and damaging implications.

Manufacturers not only have to tackle the information technology (IT) risks that apply across many sectors, they also have to secure their operational technology (OT)— the cornerstone of most manufacturing businesses that is also becoming increasingly digitalized. The Industrial Internet of Things (IIOT), the continued

More like this

Article

Finance and Insurance Industries: Managing Risk in a Rapidly Evolving Environment

migration of key systems and data to the cloud, and the incorporation of new technologies continue to open up whole new areas of cyber risk. At the same time, the OT environments of most companies still have many legacy systems. These systems may lack the same protections as their newer counterparts and therefore significantly increase a manufacturer's overall cyber vulnerability.

Managing these risks can be particularly challenging, especially when it comes to third-party cyber risks. Many manufacturing companies in the sector are relatively small or rely on a large network of smaller or more diverse businesses within their supply chain, which may not have the same level of cyber sophistication as larger organizations. Merger and acquisition business transactions can also introduce risk. In our experience, some of the biggest cyber events in the manufacturing industry result from limited or poor integration of acquired companies into the whole.

Manufacturing organizations are generally well aware of these risks and vulnerabilities. In our latest Global Risk Management Survey, manufacturers ranked both cyber attack or data breach and business interruption — which, when it occurs, is often the result of a cyber attack — as top-five industry risks.[1] These risks are no longer hypothetical; a large global steel producer was forced to temporarily suspend production at multiple locations after a cyber security incident.

Economic and political uncertainty further complicates the management of cyber risks, with inflation continuing to be a major challenge. Meanwhile, geopolitical upheaval is also having an impact on both supply chains and overall investment decisions. This may help to explain why the median percentage of the IT budget reportedly spent on security by companies in the manufacturing sector has stalled — or even fallen slightly — since 2022; companies reported that 8 percent of their IT budget was dedicated to security in 2024, compared to 8.5 percent in 2022.

Aon Clients Report: The Manufacturing Industry and Cyber Risk

Article

Third-Party Risks Can Create Cyber Challenges for Healthcare

Report

Global Risk Management Survey

69%

of middle-market and SME manufacturing clients reported that they had not performed a tabletop exercise over the preceding 12 months.

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation

Aon's Cyber Quotient Evaluation (CyQu) data shows that overall risk scores in the sector remained fairly flat, with the average shifting from 2.5 in 2023 to 2.53 in 2024. For global manufacturing companies, scores improved marginally from 2.73 to 2.82, but there was little movement among smaller companies, which currently report an average score of 2.32. This stagnation may be particularly problematic for these small and medium-sized enterprises, especially as prominent manufacturers are increasingly imposing additional cyber maturity requirements from their supply chains. These companies reported a median spend of 7 percent of their IT budget on cyber security, which is below the industry average and may not be sufficient to secure the resilience and risk coverage needed for key risks.

Looking at risk score by cyber domain, manufacturing companies score best, on average, for end-point security, remote work and network security, all of which are important for the industry. Perhaps unsurprisingly, given the issues highlighted above, they score least well — and significantly lower than the finance and insurance industry or the healthcare industry — for business resilience and third party. In addition, digital access to production, often held by trusted suppliers for maintenance, is increasingly becoming a back door for devastating cyber attacks. These challenging areas are attracting increasing scrutiny, including from regulators and insurers, however, and we expect to see companies within the manufacturing industry place an increased focus on managing these risks in the coming years.

Cyber Domains | 2024 Industrials & Manufacturing Industry

Overall Risk Score: 2.53

Highest Scoring

2.83	Endpoint Protection	3.04

Insurance Claim Management

Endpoint Security	Logging & Monitoring	2.84
	Secure Config.	2.74
2.80 Remote Work	Remote Connectivity	3.40
	Authentication & Identity	2.92
	Device Vuln. & Monitoring	2.65
2.79 Network Security	Pen Testing	3.03
	Enviroment	2.84
	Wireless	2.72

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Lowest Scoring

1.97 Third Party	Due Diligence	1.78
	3rd Party Contracts	2.07
	3rd Party Inventory	2.57

1.98 Application Security		Training	1.76
		Software Mgmt.	2.01
		Secure Dev.	2.03
2.39 Business Resilience		BCM/DR	2.22
		Incident Response	2.42
		Backup	2.59

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

In the U.S., Aon's CyQu red flag controls data shows that our renewal clients' red flags decreased 12 percent year over year, a substantially faster rate of improvement than the cross-industry average of 9 percent. But clearly, work remains to be done, especially in building resilience.

One of the most common red flags is a lack of recent tabletop exercises; 69 percent of middle-market companies and SMEs and 56 percent of global and enterprise clients did not complete this control during the year preceding the survey. Companies that do not perform these exercises regularly may suffer significantly greater damage in the aftermath of an attack, given that they may not be familiar with the appropriate response sequence. Holding regular tabletop exercises is comparatively straightforward, so addressing this vulnerability should be a priority.

In addition, many companies lack several other resilience-related controls, including implementing multifactor authentication for key systems and backups, and storing backups in a secondary data center. These vulnerabilities could significantly increase the amount of time it would take a company to get back up and running in the aftermath of a ransomware attack, which in turn could increase the likelihood of a ransom being paid. Companies lacking key resilience-related controls may also achieve less favorable outcomes in the insurance market.

Top 10 Critical Red Flags | 2024 Industrials & Manufacturing Industry

---

Global & Enterprise

2024

Middle Market & SME

2024

When it came to OT[2], our renewal clients' red flags showed minimal improvements between 2023 and 2024, although some progress was made on including ransomware in OT tabletop exercises and MFA on key OT systems. Many manufacturing companies still lack crucial controls — including segmentation of the OT environment from the IT environment and the internet, with 31 percent and 21 percent of companies, respectively, lacking these key controls. Regular OT assessments based on standards such as NIST 800.82[3] or IEC62433[4] are crucial to identify the biggest cyber risks in OT and prioritize the right measures.

Industrials & Manufacturing Operational Technology Red Flags | YE 2024

2023

2024

These findings on common critical red flags appear to support the idea that when it comes to incident response and recovery, companies tend to focus more on securing technology than on people, policy and procedure.

Given the size and prominence of the sector, it is perhaps unsurprising that a significant portion of ransomware attacks appear to have targeted manufacturing companies.[5] According to Aon Threat Intelligence data, manufacturing is the third-most-targeted industry for ransomware attacks.

Key Observations | 2024 Industrials & Manufacturing Industry

Ransomware Victims by Sector (Threat Intel)

Consumer & Industrial Products

Professional Services & Consulting

Manufacturing

Real Estate

Life Sciences & Healthcare

Public

Technology, Media & Telecom

Energy, Resources & Agriculture

Nonprofit

Financial Services

Others

Target Victims by Sector (Q4’24 Access Claims)

Now What? Actions for Manufacturing Organizations

Risk management involves building resilience and transferring risk. Many manufacturers may have historically looked to cyber insurance, rather than building resilience, as their main route to managing cyber risks. However, securing a comprehensive and

affordable policy without demonstrating resilience has — and will continue to — become more challenging. Identity management, backup security and regular f tabletop exercises may be key areas in need of attention. The good news for many manufacturers is that reasonably priced coverage for well-managed cyber risks is growing in breadth.

Map and manage third-party risks. Third-party vulnerabilities have long been a key element of cyber risk for manufacturing companies, and this has only increased in recent years due to growing supply chain complexity. While insurance options for third-party risks are growing and broadening in scope, insurers will want to see that companies fully understand — and are managing — these risks.

Stay ahead of regulations. NIS2[6] and the European Cyber Resilience Act[7] will have far-reaching implications for some or all manufacturers. As a result, we expect to see a significant move from protecting stand-alone technology to securing connected devices. Companies will need to fully understand these and other regulatory developments to ensure that they are getting ahead of key requirements.

Segment IT and OT. Segmentation of systems is imperative — as is end-of-life planning for legacy systems. Insurers require clear separation between the IT and OT environments to help minimize the risk of a threat actor moving across the network. Penetration testing, in which a company simulates a cyberattack to identify system vulnerabilities, can be very helpful in ensuring that systems are functioning correctly.

Focus on response and recovery. As we have seen, Aon's CyQu red flag controls data indicate that manufacturing companies still have a lot of work to do in building business resilience. Manufacturers often focus heavily on the technology piece of recovery after a significant cyber incident, but true business resilience demands much more. Companies need comprehensive incident response and recovery plans with clear lines of responsibility, and they will need to test their plan — ideally with both executive- and technical-level reviews — at least annually to ensure it is fit for purpose.

References

[1] “Top Risks Facing Industrials and Manufacturing Organizations,” Aon, November 28, 2023, https://www.aon.com/en/insights/reports/global-risk-management-survey/top-risks-facing-industrials-and-manufacturing-organizations.

[2] Of all clients that responded to our OT Supplemental Red Flags survey, 35 percent were from the industrials and manufacturing sector. Respondents in this sector reported a stronger average performance across OT red flags than respondents in other sectors (such as construction and real estate, healthcare, and professional and business services), though the rate of improvement for industrials and manufacturing companies has generally been slower than for companies in other sectors.

[3] Keith Stouffer et al., NIST SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security, National Institute of Standards and Technology, September 2023, https://csrc.nist.gov/pubs/sp/800/82/r3/final.

[4] “Cyber security,” IEC, accessed June 23, 2025, https://www.iec.ch/cyber-security.

[5] According to both Aon Intelligence team analysis of information posted on ransomware leak sites on the dark web and Aon Access Claims data.

[6] “NIS2 Directive: new rules on cybersecurity of network and information systems,” European Commission, accessed June 23, 2025, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[7] “Cyber Resilience Act”, accessed June 23, 2025, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Insurance products and services are offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida, and their licensed affiliates.

The information contained herein and the statements expressed are of a general nature, not intended to address the circumstances of any particular individual or entity and provided for informational purposes only. The information does not replace the advice of legal counsel or a cyber insurance professional and should not be relied upon for any such purpose. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Asia-Pacific’s Commitment to Cyber Security Pays Off

Key takeaways

Now is the time to consider obtaining cyber risk insurance. Asia Pacific businesses generally compare favorably to the global

marketplace and can benefit from the competitive and growth-oriented industry.

Cyber incident frequency was up 29% year-over-year and 134% over the last four years, contributing to a 22% rise in cyber insurance claims in 2024 over the prior year.

AI is a driving force of cyber risk. The rise in AI-driven deepfake attacks resulted in a 53% increase in social engineering incidents year-over-year, and social engineering and fraud claims increased by 233%.

The good news is that many businesses across the Asia-Pacific (APAC) region are growing in cyber maturity. The 2024 overall reported risk score for Aon clients, according to Aon's CyberQuotient (CyQu) data, was 2.73 out of four, or approaching managed — close to North American clients' maturity scores. Year-over-year, the risk score across cyber domains saw an almost 16 percent improvement, and responding companies recorded the most substantial scores in network security and data security, which includes governance and user awareness and training.

More like this

Podcast

On Aon Podcast: How has CrowdStrike Changed the Cyber Market?

Article

Cyber Domains | 2023 vs 2024 Asia-Pacific Data - Total Score by Domain

2023

2024

Risk Capital and Human Capital Perspectives

Report

Global Risk Management Survey

16%

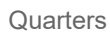
improvement in risk score across cyber security domains in Asia-Pacific

Explore More Cyber Offerings

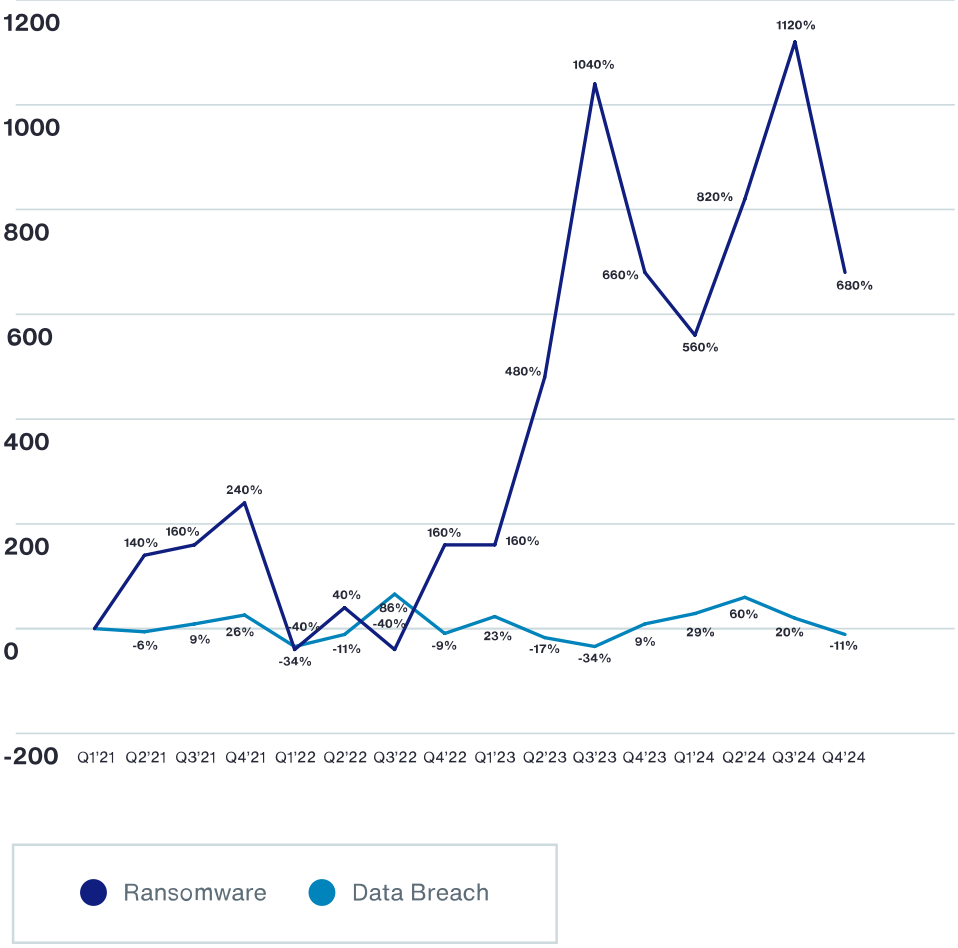
- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation
- Business Continuity Management for Cyber Risk

APAC aligned with its global counterparts and saw a substantial rise in cyber claims notifications, an increase of 22 percent over 2023, while cyber incident frequency was up 29 percent year-over-year, and up 134 percent across the past four years (2020-2024).

APAC Claims Stats – year-on-year change in claims frequency



APAC Incident Stats – rate of claims frequency index on Q1 ‘21



Source: Risk Based Security, analysis by Aon. Data as of 22/03/2025.

Despite the increased activity, insurers across the Asia Pacific remained profitable and did not realize significant losses across the year as businesses were able to recover systems and operations quickly post-breach. This is a testament to the success of proactive cyber risk management, the role played by cyber insurance premium relief, stricter underwriting by carriers and the growing prevalence of self-insured retention.

Geopolitical Forces and Regulations Shape Risk Profile

In the “year of elections,”[2] more than 12 nations across the Asia Pacific region held federal or state elections across 2024, including Bangladesh, Bhutan, Cambodia, India, Indonesia, Japan, Pakistan, South Korea, Sri Lanka, Taiwan, Thailand and Australia.[3] This

record political activity also sparked a significant increase in the use of nation-state-sponsored deepfakes in what appeared to be an effort to confuse and create distrust in elections. This was reflected in a 53 percent increase in social engineering incidents year over year.

Geopolitical forces, such as trade disputes or tensions, territorial disputes or the reconfiguration of the supply chain, also shaped how companies thought about cyber risk. According to the Council on Foreign Relations, 63 percent of all suspected nation-state-sponsored cyber operations originated in the region.[4] Asia-Pacific has become a dynamic hotbed of tension involving geopolitical rivals. Many critical industries have become the focus of advanced threat campaigns to support nation state's objectives, destabilize rivals and reinforce influence.[5] Accordingly, 2024 witnessed an escalation of cyber campaigns that targeted key industries, critical infrastructure operators, and supply chains of strategic importance.[6] The increasing intensity of these campaigns was reflected in the number of incidents targeting the public sector, financial institutions, manufacturing, and technology. The APAC region is increasingly playing a significant role in key manufacturing and technology industries, and the manufacturing industry's economic importance and the intellectual property it holds make it an attractive target for cyber espionage and intellectual property theft.[7] In response to the rising risk, companies invested in key controls across physical and third-party security and resilience.

Cyber Domains | 2024 Asia-Pacific Data

Overall Risk Score 2.73

Highest Scoring

2.94 Network Security	Pen Testing	3.17
	Network Environment	3.04
	Wireless	2.73
2.92 Data Security	Governance	3.15
	User Awareness Training	3.12
	Data Classification	2.83
2.87 Physical Security	Physical Access	3.28
	Environmental	3.13
	Tampering & Alteration	2.10

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Lowest Scoring

2.35 Application Security	Training	1.87
	Software Mgmt.	2.38
	Secure Dev.	2.47

2.45 Third Party	Due Diligence	2.36
	3rd Party Contracts	2.52
	3rd Party Inventory	2.73
2.68 Business Resilience	BCM/ DR	2.56
	Backup	2.58
	Incident Response	2.88

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

The regulatory landscape covering privacy, security, and artificial intelligence (AI) topics continued to evolve across the Asia-Pacific region, forcing risk leaders to adapt their approaches to cyber risk governance and data security. There are now 25 in-force or proposed cyber security and data privacy regulations across 14 Asia-Pacific countries.[8] Furthermore, to address the risks associated with developing and deploying AI, 11 legislations and regulations covering the technology have been in force or proposed, and many companies have also issued AI governance frameworks and regulatory guidance.[9] Several of these regulatory frameworks (for example in Australia and Indonesia) have been modeled on European Union risk-based models such as the General Data Protection Regulation, the Network and Information Security 2 Directive, and the EU AI Act. Indonesia was a regional leader in introducing privacy law, with the 2022 introduction of the

Personal Data Protection (PDP) Law (Law No. 27), which established a comprehensive legal structure to protect personal data across all sectors.[10]

As the region continues implementing more robust regulatory models for cyber security, data privacy and AI risk management, maturity is improving across key controls, such as governance, data classification and third-party risk management of critical technology vendors.

The Shadow Risk — AI and the Expanding Digital Attack Surface

The Asia-Pacific region is experiencing a rapid acceleration in adopting AI and generative AI technologies, including software, services, and hardware designed for AI-driven systems.[11] Palo Alto Networks warns that 2025 will see a perfect storm of AI-driven cyber threats that will escalate in scale, sophistication and impact.[12] The increasing role of AI in security attacks explains the significant rise in incidents and claims involving deepfake social engineering and fraud (233 percent).[13] Asia-Pacific experienced a 1,530 percent surge in deepfake cases from 2022 to 2023, marking it as the second-highest region in this concerning trend.[14] In a high-profile case in Hong Kong, cybercriminals utilized an AI deepfake, a digitally manipulated video of a senior executive, to induce a finance department employee to transmit wire transfers valued at $25.6 million.[15] Threat analysis of hacking groups, particularly Advanced Persistent Threats and nation-state-aligned groups, revealed that AI technologies, such as GenAI, are increasingly being used to scale and deliver campaigns across the region.[16]

Furthermore, the urgency to capture economic opportunities associated with new AI technologies has seen a rush to market of new products and services. Unfortunately, it is often at the expense of conducting robust legal, security and risk management reviews before launch. The unsanctioned or unknown uses of AI has created a wide and unsecured digital attack surface. Of the companies surveyed in Aon's 2024 Intangible Versus Tangible Risks Comparison Report,[17] 79 percent of businesses reported using or intending to use artificial intelligence products and

services, with only 32 percent reporting the existence of a formal inventory of all generative AI implementations. This risk is compounded by Aon's analysis that 98 percent of chief risk officers reporting being "somewhat" or "not ready" to manage these new AI risks.[18]

There is also a growing trend in sophisticated scams and money laundering, underscoring the necessity to address and combat evolving fraud patterns. Bangladesh and Pakistan had the highest fraud rates in Asia-Pacific — and the world — in 2023, with rates of 5.44 percent and 4.59 percent, respectively. Singapore stands out for successfully reducing its fraud rate and Japan, Australia and Thailand have maintained their fraud rates at under two percent over 2021-2023.[19]

To combat these trends, companies in Asia-Pacific increased investment in user awareness training, to manage social engineering attacks; application security, to strengthen the security of new AI technologies; and third-party improvement, to help manage exposures from the deployment of AI vendors.

Cyber Domains 2023 vs 2024 Asia-Pacific Data - Data Security and Third Party Domain

2023

2024

Growth-Oriented Cyber Insurance Marketplace

There is an intense focus on Asia-Pacific as a growth area for cyber insurance. Overall, organizations are proving to be more mature than the global market has historically anticipated and cyber insurance take-up in the region is markedly low, sitting at about 6 percent of the addressable market. Due to this, the region is experiencing significant competition among the many international insurers and increasing numbers of cyber insurance carriers entering from the London market. In response, the local insurance market is mobilizing to improve their policies and servicing. Collectively, this presents an ideal cyber insurance buyers' marketplace. New and expanding risk necessitates a cyber insurance policy to protect against financial loss, while insurance

carriers are lining up to help clients better understand, manage and transfer cyber risk.

Recommended Actions:

Consider cyber risk insurance and enter the buyer's market with confidence. Our CyQu data suggests that Asia-Pacific businesses compare favorably to the global marketplace.

Use data and analytics to evaluate your organization's cyber risk and maximize insurance. Forecasting loss scenarios, exposure assessment and total cost of risk are some of the essential data points for evaluating risk transfer mechanisms.

When considering investing in AI, make certain to help protect that investment with proper cyber risk management and insurance protection.

Download these findings

References

[1] How North Korea's unstoppable hackers are weaponizing AI. South China Morning Post. Leopold Chen. March 9, 2025. https://www.scmp.com/week-asia/economics/article/3301554/how-north-koreas-unstoppable-hackers-are-weaponising-ai

[2] The Year of AI and Elections. Council on Foreign Relations. Podcast. Gabrielle Sierra. https://www.cfr.org/podcasts/year-ai-and-elections. Lee Kuan Yew School of Public Policy. Report. https://lkyspp.nus.edu.sg/gia/article/a-record-year-of-elections-observations-from-2024

[3] A record year of elections: Observations from 2024. Council on Foreign Relations. Podcast. Gabrielle Sierra. https://www.cfr.org/podcasts/year-ai-and-elections

[4] Cyber Operations Tracker. Council on Foreign Relations. www.cfr.org

[5] The current impact of State-Sponsored Cybersecurity attacks in the Asia-Pacific Region. Modern Diplomacy. Guilherme Schneider. December 18, 2024. https://moderndiplomacy.eu/2024/12/18/the-current-impact-of-state-sponsored-cybersecurity-attacks-in-the-asia-pacific-region/

[6] The current impact of State-Sponsored Cybersecurity attacks in the Asia-Pacific Region. Modern Diplomacy. Guilherme Schneider. December 18,

2024. https://moderndiplomacy.eu/2024/12/18/the-current-impact-of-state-sponsored-cybersecurity-attacks-in-the-asia-pacific-region/

[7] The Changing: Cyber Threat Landscape Asia-Pacific Region – Volume 1. Cyfirma Decoding Threats. June 8, 2024. https://www.cyfirma.com/research/the-changing-cyber-threat-landscape-asia-pacific-apac-region-volume-1-2/

[8] Data Protection Laws of the World. An overview of key privacy and data protection laws across over 160 jurisdictions. DLA Piper. https://www.dlapiperdataprotection.com/

[9] Global AI Law and Policy Tracker. IAPP. November 2024. https://iapp.org/resources/article/global-ai-legislation-tracker/

[10] A New Chapter: Preparing for Indonesian Personal Data Protection Legislation. Aon. https://www.aon.com/apac/insights/blog/default/a-new-chapter-preparing-for-indonesian-personal-da

[11] Asia/Pacific* AI Investments to Reach $110 Billion by 2028, IDC Reports. IDC. Press Release. September 23, 2024. https://www.idc.com/getdoc.jsp?containerId=prAP52613324

[12] 2025 Cybersecurity Predictions. Asia-Pacific Region. Palo Alto Networks. December 21, 2024. Simon Green, President Asia-Pacific and Japan.

[13] How North Korea's unstoppable hackers are weaponizing AI. South China Morning Post. Leopold Chen. March 9, 2025. https://www.scmp.com/week-asia/economics/article/3301554/how-north-koreas-unstoppable-hackers-are-weaponising-ai

[14] APAC Deepfake Incidents Surge 1530% in the Past Year Amidst Evolving Global Fraud Landscape. Sumsub Annual Identity Fraud Report. Press Release. November 28, 2023. www.prnewswire.com

[15] Company Loses Millions on Deepfake Scam. NFP. March 6, 2024. https://www.nfp.com/insights/company-loses-millions-on-deepfake-scam/

[16] Chinese and Iranian Hackers are Using U.S. AI Products to Bolster Cyberattacks. The Wall Street Journal. Dustin Volz and Robert McMillan. January 29, 2025. https://www.wsj.com/tech/ai/chinese-and-iranian-hackers-are-using-u-s-ai-products-to-bolster-cyberattacks-ff3c5884

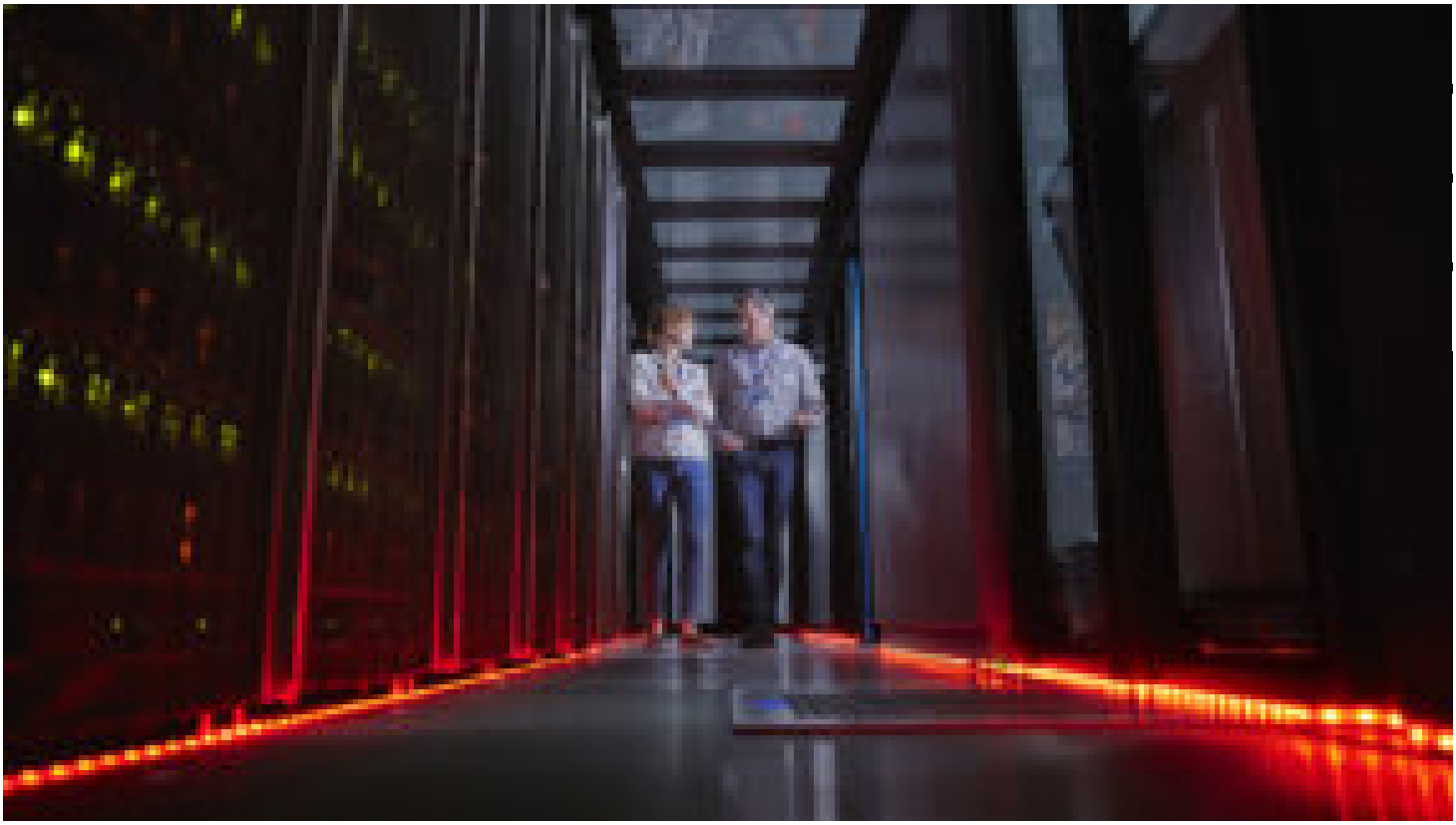
[17] 2024 Global Intangible Versus Tangible Risks Comparison Report: De-risking AI, IP, and Cyber. Aon and Ponemon Institute. Report. 2024. https://assets.aon.com/-/media/files/aon/reports/2024/intangible-vs-tangible-risk-comparison-report-2024.pdf

[18] Aon global analysis.

[19] APAC Deepfake Incidents Surge 1530% in the Past Year Amidst Evolving Global Fraud Landscape. Sumsub Annual Identity Fraud Report. Press Release. November 28, 2023. www.prnewswire.com

relied upon for any such purpose. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Riding the Wave: EMEA Approaches Cyber Maturity



Key takeaways

Organizations were more engaged and resilient in 2024, approaching maturity across key cyber risk domains. However, they were

least prepared when it came to third-party risk and business resilience.

Ransomware attacks were more frequent but stronger cyber controls meant that the severity declined. Globally, the ratio of payment to demand size decreased to 28%.

The cyber insurance marketplace has never been more accessible, especially for middle-market businesses. New entrants and a flood of new capital led to declining prices and great scope and scale for renewals.

While differences persist across countries, Europe rode the tide towards cyber security maturity in 2024. The market moved away from data-centric regulations towards resilience and an increased focus on the organization's ability to withstand and recover from attack and avoid business interruption. We witnessed an uptick in the effective deployment of security controls, particularly with respect to managing and recovering from ransomware attacks, maturation in the cyber insurance market in both underwriting capability and coverage capacity and the influence of regulatory frameworks on resilience.

Major systemic-type cyber events impacted Europe in 2024, and geopolitical tensions deepened, leading to volatility and more risk.

More like this

Podcast

On Aon Podcast: How has CrowdStrike Changed the Cyber Market?

Article

The UK's National Health Service suffered multiple attacks throughout the year, notably the June ransomware attack against a pathology services provider. This breach led to canceled appointments and procedures and disruptions to blood transfusions and test results.[1] The CrowdStrike outage in July 2024 served as a timely reminder of the potential loss severity associated with digital supply chain interconnectedness. The incident caused more than 8.5 million systems to crash, disrupting operations worldwide for days and impacting commercial flights, hospitals and financial services.[2]

Volatility also led to more aggressive and pernicious nation-state-style actors, whether direct or through ancillary bodies. Critical infrastructure was a key target and between January 2023 and January 2024, global critical infrastructure faced over 420 million cyber attacks, or 13 attacks per second, with varying levels of severity.[3] These attacks occurred worldwide, with the U.S. being the most frequently targeted country, followed by the UK and Germany.[4] As the U.S. and China compete more commercially, we anticipate increased commercial-style espionage, likely impacting Europe. Many insurance carriers are already reacting to this volatility. There has been growing consensus in the market that if an attack is state-backed and causes significant or major disruption in a country, losses might be excluded provided such disruption is of enough scale to be non-insurable.

Technical Controls Get Stronger But Third-Party Risk Climbs.

The year saw a more engaged and resilient client base emerging as organizations made significant progress in implementing technical controls and strengthening digital domains. Aon clients across Europe reported an overall Aon global risk score — a key metric that measures preparedness across six critical cyber security domains — of 2.53 out of four. Organizations performed best across endpoint security, network security and access control, while unsurprisingly, organizations were least prepared to manage third-party risk and business resilience.

Cyber Domains | 2024 EMEA Data

Risk Capital and Human Capital Perspectives

Report

Global Risk Management Survey

77%

Is the decline of the average ransomware payment amount.

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation
- Business Continuity Management for Cyber Risk

Overall Risk Score 2.53

Highest Scoring

2.80 Endpoint Security	Endpoint Protection	2.99
	Secure Config.	2.80
	Logging & Monitoring	2.79
2.76 Network Security	Network Environ.	2.85
	Pen Testing	2.84
	Wireless	2.63
2.74 Access Control	Password Config.	2.89
	MFA	2.77
	Access Mgmt.	2.65

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Lowest Scoring

2.01 Third Party	Due Dilligence	1.81
	3rd Part Contracts	2.04
	3rd Part Inventory	2.75
2.12 Application Security	Training	1.84
	Software Mgmt.	2.08
	Secure Dev.	2.21
2.33 Business Resilience	BCM/ DR	2.15
	Incident Response	2.35
	Backup	2.54

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Ransomware attacks persisted across Europe in 2024. While the law enforcement actions of the past few years to dismantle ransomware threat actor groups destabilized the space, they also gave rise to dozens of splinter groups.

Top Ransomware Groups

Group	Number of Published Victims
LockBit 3.0	404
RansomHub	387
Play	308
Akira	250
Hunters international	195

As the frequency of ransomware attacks grew, attack groups broadened their efforts and targeted smaller organizations. However, the severity of attacks declined, partially supported by stronger cyber security controls and ransomware preparedness. Globally, the ratio of payment to demand size decreased to 28 percent, from 41 percent in 2023, and the average ransomware payment amount declined by 77 percent. While this decrease in severity is a promising picture, the rise in ransomware event frequency necessitates guidance around reporting and navigating notices.

Ransomware Severity (in $)

Average Demand Amount

Average Payment Amount

Third-party risk, which refers to the potential risk from suppliers, vendors or partners, continued to prove challenging. This score is a call to action for many businesses. The events of 2024 highlight the potential downstream impact of a third-party breach. Organizations also underperformed at managing business resilience, including back-ups, incident response, and business continuity management. Phishing and social engineering attacks increased by a third in 2024, accounting for nearly one in five of the primary incident vectors when joined with identity theft/account cracking. The majority of examined large telecommunications, financial services and e-commerce operators saw an increase in overall fraud attacks, including identity thefts and account takeovers.[5] [6] As a result, we expect organizations to devote more time and effort on fraud prevention, business resilience policies and procedures in order to safeguard the overall environment.

Cyber Insurance and Regulations Help Drive Maturity

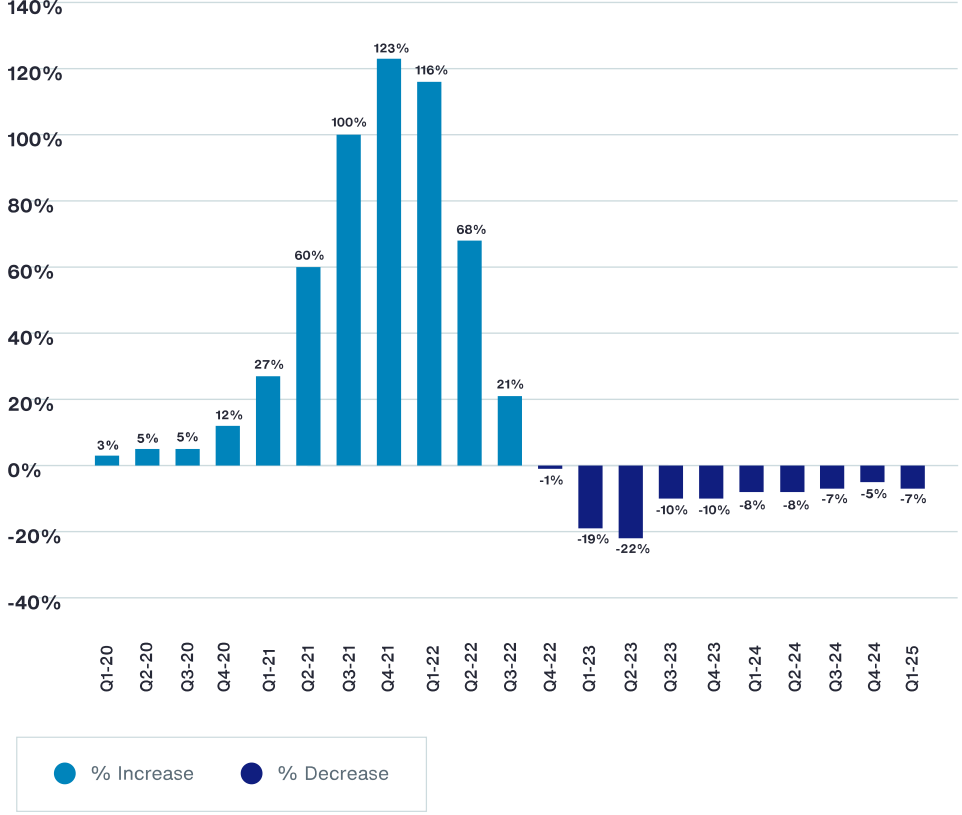
Across 2024, cyber regulations demanded that more organizations identify, assess and mitigate their cyber risks. The European

Union's Network and Information Security Directive (NIS2) expanded regulations to 18 sectors, including energy, transport, health, finance and digital infrastructure, encompassing both essential and important entities within these sectors. It also called on EU member states to define their national cyber security strategies and collaborate on cross-border reaction and enforcement.[7] Another piece of EU legislation, the Digital Operational Resilience Act (DORA), focuses on cyber security across financial institutions such as banks, insurance companies, and investment firms, working to ensure that Europe's financial sector is more resilient in the event of a severe operational disruption.[8]

As organizations complied with regulations in 2024, they also worked to secure cyber insurance and underwriting — all of which helped drive cyber security. At the same time, insurance carriers experienced increased competition. The European insurance marketplace has never been more accessible thanks to many new entrants and a flood of new capital into the cyber insurance marketplace, resulting in declining prices, great scope and scale for renewals and new buyers.

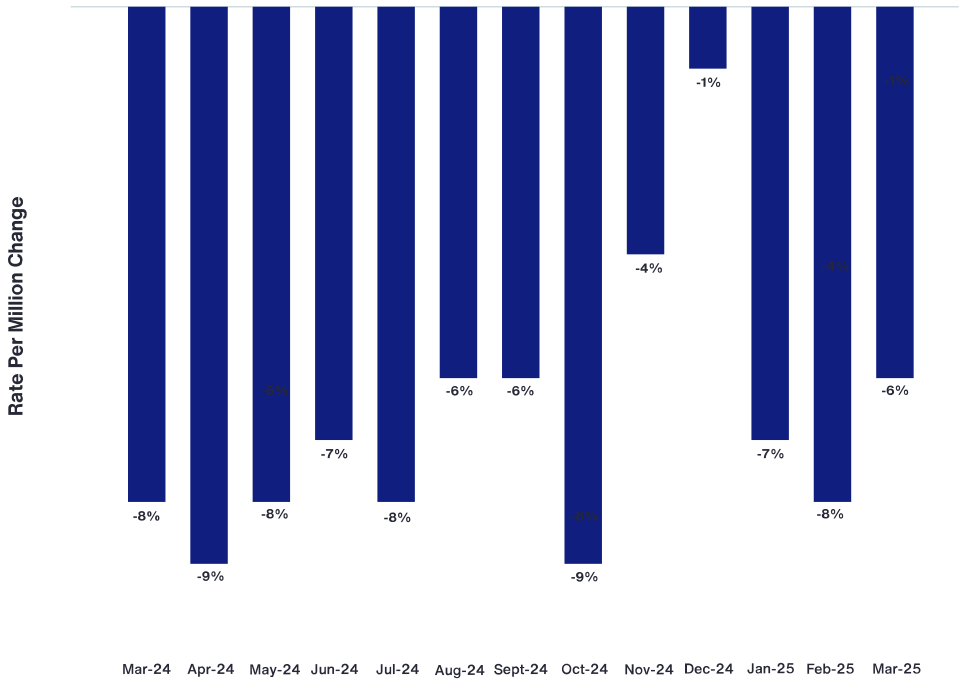
2020–2025 Cyber Premium Changes by Quarter

Average Year–over–Year Change (Same Clients)



Cyber Monthly Pricing All Layers

Average Year–over–Year Change (Same Clients)



A broadening of coverage emerged in unexpected areas, including third-party risk. Many managing general agents now offer turnkey solutions and bundles, such as packaging a threat-hunting or endpoint detection and response (EDR) with substantial reactive cyber insurance in one complete package.

As competition continues, insurance carriers will become more innovative in their products and coverage. On the incidents and claims front, carriers will need to manage more complex supply chain claims, deal with a continued uptick in notifications and make more complex business interruption adjustments.

Recommended Actions

- Conduct a data-driven analysis of your organization's cyber risk posture. Strengthen third-party and business resilience domains.
- Engage in regular horizon-scanning and collaborate with industry peers to identify sector-specific challenges and threats. Work to close or reduce vulnerability to these threats.
- Secure a broad cyber insurance policy that considers and covers supply chain risk. Use feedback from the insurance marketplace to inform cyber security planning.
- Ensure robust data security and governance controls exist before deploying AI technologies. Have clearly defined use cases for all AI deployments and robustly evaluate the risks associated with those cases to determine appropriate mitigation strategies.
- Develop AI usage policies and hunt down shadow AI or employees' unauthorized use of AI tools and technologies. Execute an internal education and awareness campaign.

Download these findings

References

[1] Update on Cyber Incident: Clinical impact in southeast London – Thursday 26 September 2024. NHS England. https://www.getronics.com/nhs-cyber-attack-2024/

[2] Raphael Yahalom. What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk. Harvard Business Review. January 10, 2025.

[3] A growing geopolitical weapon. World Pipelines. Alfred Hamer. December 31, 2024. https://www.worldpipelines.com/

[4] ibid.

[5] Rapporto Clusit 2025. Sulla Cybersecurity in Italia e nel mondo. Clusit. https://www.cybertrends.it/rapporto-clusit-2025/

[6] Tackling evolving fraud threats. Experian, by Forrester Consulting. 2025. https://experianacademy.com/forrester-fraud-research-report-2024

[7] NIS2 Directive: new rules on cybersecurity of network and information systems. European Commission. January 15, 2025. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive#:~:text=The%20NIS2%20Directive%20establishes%20a,and%20cybersecurity%20education%20and%20awareness.

[8] Digital Operational Resilience Act (DORA). European Insurance and Occupational Pensions Authority. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Cyber Risk is a Corporate Risk — Latin America Responds

Key takeaways

Businesses across Latin America made progress in combating cyber attacks, leading

to slight improvement in the region's overall risk score.

Ransomware is still with us — and Latin America was no exception. The large number of small to mid-sized enterprises in the region makes it an ideal target.

Many Latin American businesses are well positioned to secure a cyber insurance policy thanks to their substantial cyber maturity scores and a more accommodating market.

According to the World Bank, by 2024, Latin America and the Caribbean was the world's fastest-growing region for disclosed cyber incidents, with a 25 percent average annual growth rate over the past decade.[2] The most attacked countries in Latin America across 2024 were Brazil with 47 percent of attacks, followed by Mexico with 23 percent, and Colombia with 8 percent.[3]

The most attacked countries in Latin America

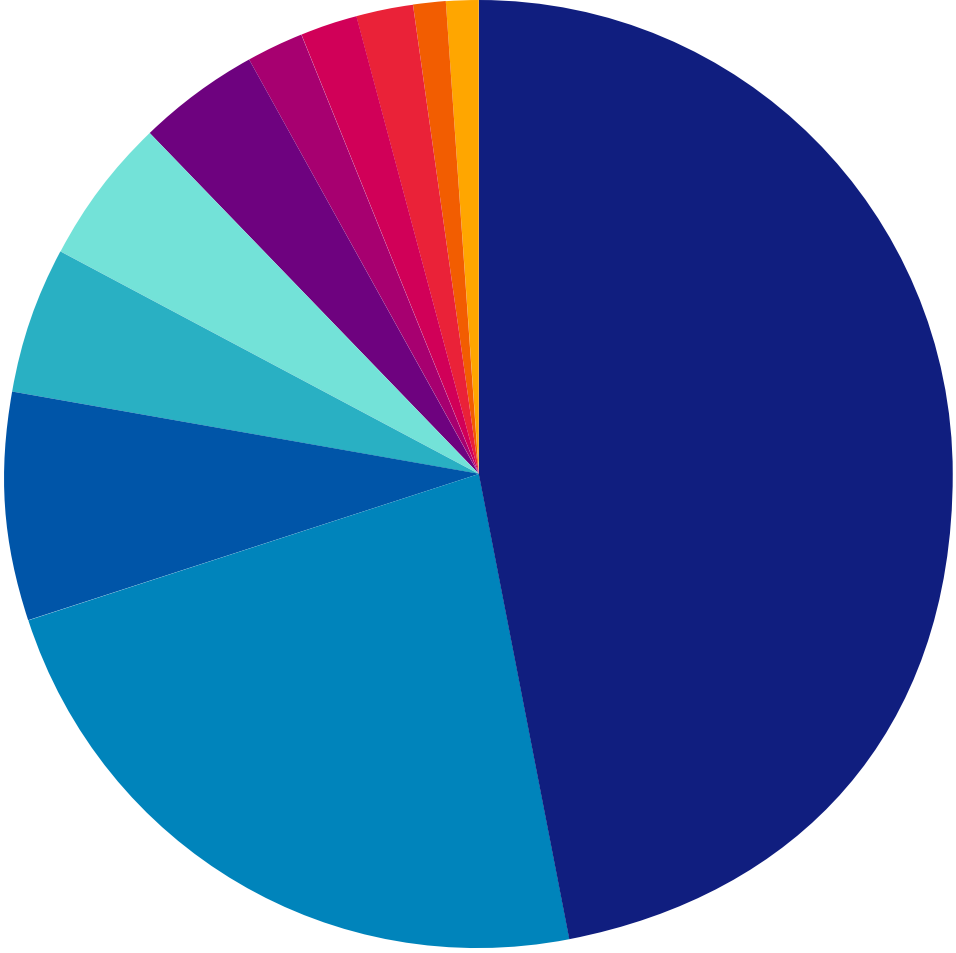
More like this

Podcast

On Aon Podcast: How has CrowdStrike Changed the Cyber Market?

Article

Risk Capital and Human Capital Perspectives



Report

Global Risk Management Survey

47%

Of attacks in Latin America in 2024 in Brazil, followed by Mexico with 23%

Insight about the data in this chart.

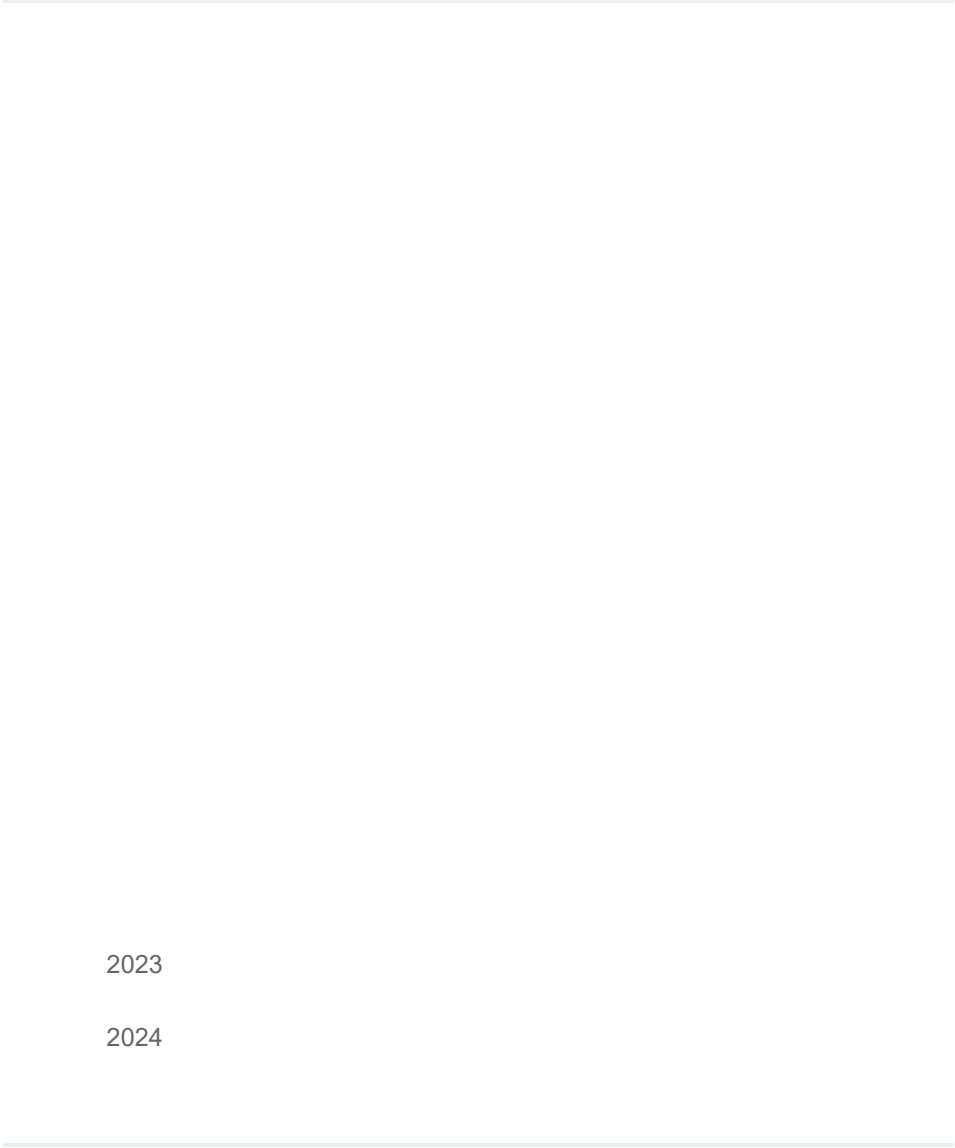
- Brazil - 47%
- Mexico - 23%
- Colombia - 8%
- Peru - 5%
- Other - 5%
- Ecuador - 4%
- Chile - 2%
- Venezuela - 2%
- Colombia - 8%
- Bolivia - 1%
- Paraguay - 1%

In response to the heightened risk environment, many businesses across Latin America strengthened their efforts to combat attacks. What was often seen before by businesses as solely an information technology risk is now generally viewed as a whole-enterprise risk, and we are starting to see more alignment and engagement between cyber risk, information security and business leaders.

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation
- Business Continuity Management for Cyber Risk

This focus on cyber risk is evidenced by the consistent, though slight, improvement in risk scores reported by Aon clients. The overall risk score for Latin American businesses across 2024 was reported as 2.59 out of four, sitting between basic and managed preparedness and slightly under the global risk score of 2.71.



Latin American businesses, like many of their global counterparts, continued to struggle with managing third-party risk, application security, training and business resilience. From an industry perspective, financial institutions, transportation and logistics, business and professional services and retail and consumer goods scored the highest in cyber maturity. Interestingly, the technology, media and communications industry fell in its total risk score by seven percent year-over-year. This was likely due to the rapid adoption of new technologies to remain competitive and only serves to illustrate the risk that new digital business models pose.

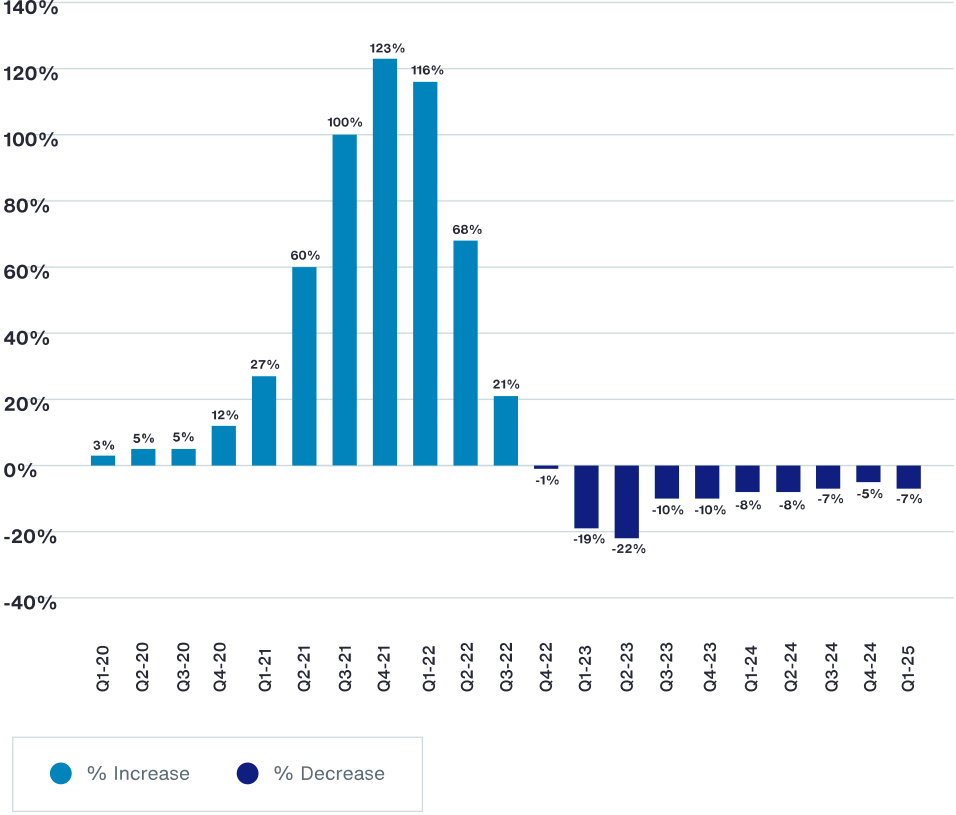
Securing SMEs

Globally, ransomware claims persisted in 2024, increasing 24 percent year-over-year.[4] The Latin America region was no exception. In 2023, it experienced 1,498 ransomware attacks carried out by 33 different ransomware groups.[5] Underinvestment in cyber security and the large percentage of small to mid-size enterprises— 99.5 percent of the market — make Latin America an ideal target for ransomware threat groups.[6]

The risk is significant and strengthening security controls is only one step in achieving and maintaining cyber risk preparedness. Cyber insurance is of growing importance to businesses across the region and is needed to help transfer the risk of data breach, business interruption or other cyber-related risks. As the region matures and strengthens its score across critical controls, Latin American businesses can be better positioned to purchase cyber insurance policies. Globally, cyber insurance premium pricing declined 7 percent in Q1 2025, and in most markets, broader coverage and increased limits are now available for risks with appropriate cyber security controls.

2020–2025 Cyber Premium Changes by Quarter

Average Year–over–Year Change (Same Clients)

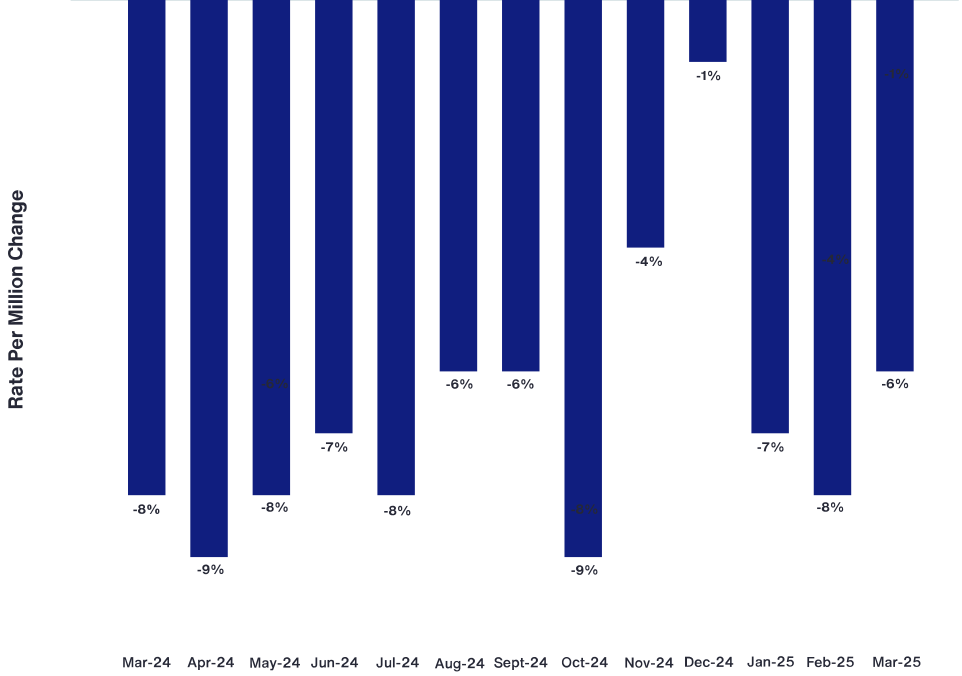


Amid this softer market and increased competition, some insurers are becoming more willing to pick up the risk with lower limits or on an aggregated basis. For carriers, Latin America presents an opportunity to help secure and support the region's economic growth. As such, insurers are encouraged to adopt new approaches to packaging policies for SMEs with limited resources.

It can be seen how insurers have adapted their products to the rapid changes taking place in different industries. Improved coverage and lower prices have helped the market continue to grow. We must also highlight the increase in cyberattacks, which has forced CISOs and IT leaders to transfer risk through cyber policies. Finally, Artificial Intelligence (AI) has played a fundamental role in the need to acquire cyber policies, generating a larger market, forcing supply and demand in Latin America to continue to increase, reflected in the price decreases.

Cyber Monthly Pricing All Layers

Average Year–over–Year Change (Same Clients)



Regulation and Disclosure

The movement toward greater cyber incident disclosure also has the potential to strengthen Latin America's cyber maturity, just as the Global Data Protection Regulation did for Europe. Chile, for example, has enacted the Chilean Law on Cyber Security and Critical Infrastructure in March 2024[7], which applies to public and private organizations that provide services that impact critical infrastructure. Organizations will have to increase their cyber security to prevent attacks following the establishment of two new regulatory institutions: the National Cybersecurity Agency (Agencia Nacional de Ciberseguridad) and the Multisectoral Council (Consejo Multisectorial). The legislation also introduces a National Computer Security Incident Response Team, which is responsible for the protection and security of networks for organizations and services that handle critical infrastructure critical to the smooth running of the country.8 Data protection and technology regulations are simultaneously being introduced on a country-by-country basis[9], but disparities continue to exist across the region, amplifying the threat level.

Recommended Actions

Cyber risk is a corporate risk. Business leaders therefore need to align across business functions and use data and analytics to

forecast loss scenarios, exposure assessment, and total cost of risk. Use this insight to make better decisions around cyber security planning.

Strengthen application security controls, particularly training and third-party management. Conduct due diligence across your vendor network and determine which are the most business critical.

Enter the cyber insurance buyer's market with confidence. Our CyQu data suggests that Latin American businesses compare favorably to the global marketplace.

Download these findings

References

[1] SME Policy Index: Latin America and The Caribbean 2024. Towards an Inclusive, Resilient, and Sustainable Recovery. OECD. July 4, 2024.

[2] From Fiction to Reality: How Latin America became the world's most critical cyber battleground. Estefania Vergara Cobos and Hualong Diao. November 28, 2024. The World Bank.

[3] Latin America Records 5,000 Ransomware Attacks per Day. ITseller Paraguay. October 2020.

[4] Ransomware Payouts Decline Despite Growing Cyber Claims Frequency. Aon Global Cyber Risk Report. May 2024

[5] LATAM Threat Landscape Report. SOCRadar. April 2024.

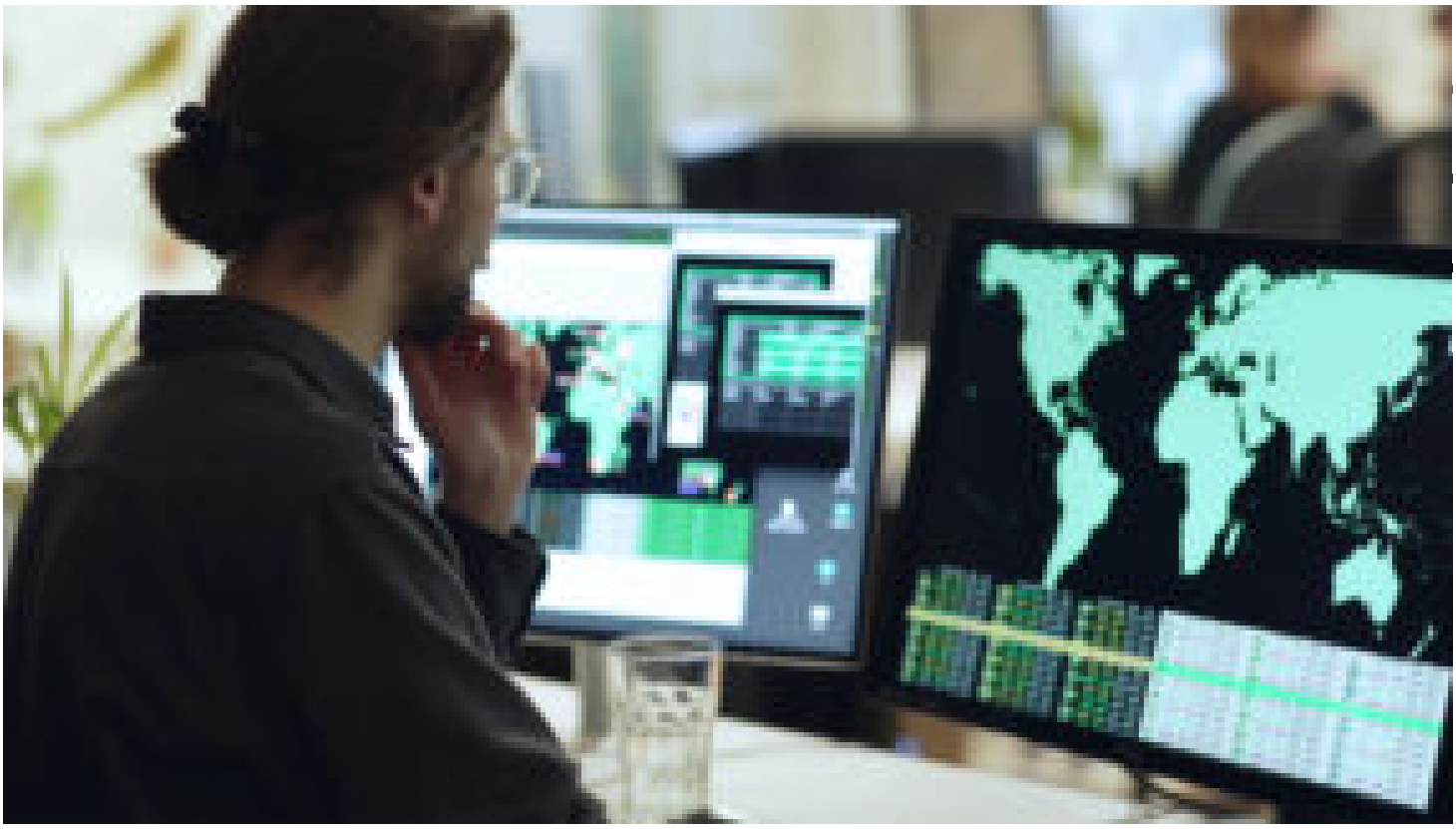
[6] SME Policy Index: Latin America and The Caribbean 2024. Towards an Inclusive, Resilient, and Sustainable Recovery. OECD. July 4, 2024.

[7] Stepping Up in Latin America: Chile enacts a new Cybersecurity Law. Nicolas LeBlanc and Astrid Hardy. DAC Beachcroft. April 9, 2024.

[8] Stepping Up in Latin America: Chile enacts a new Cybersecurity Law. Nicolas LeBlanc and Astrid Hardy. DAC Beachcroft. April 9, 2024.

[9] Latin America Tech Regulatory Developments: What has changed in the region in 2023 and 2024. Baker McKenzie.

North America – Cyber Risk Maturity Grows Amid Systemic Cyber Events



Key takeaways

Cyber risk insurance claims rose 22%, while ransomware claims payouts declined 77%. The insurance industry had a strong wake-up call but proved immune to the systemic cyber events of the year.

Payment trends and preparedness placed insureds in a more resilient position despite the continued impact of ransomware. The complexity of supply chain risk persisted, and privacy risk ticked up amid an increasingly litigious environment.

Insurer confidence was restored in most industries and on average, U.S. buyers achieved a 7% premium decrease in Q1 2025, while Canadian clients saw a 15% decrease. Underwriting rigor became more established, and clients made great strides improving critical — or red flag — security controls and domains.

Systemic cyber security events across North America demonstrated the compounding risk associated with growing technology interdependencies and how quickly a cyber event can impact entities.[2] The World Economic Forum identified supply chain interdependencies as a leading factor in the increasing complexity of cyberspace in 2025.[3] The ransomware breach of a significant U.S. healthcare payments technology provider involved the private data of approximately 190 million individuals. The glitched CrowdStrike Cloud software update caused more than 8.5 million systems to crash, disrupting operations worldwide for days and impacting commercial flights, hospitals, and financial services.[4] These major events contributed to rising cyber insurance claims across the year. Aon's U.S. Cyber Solutions broking data revealed 1,228 reported incidents across broking clients in 2024, or an increase of 22 percent, and cyber incident or litigation represented most claims with a rise of 31 percent.

Aon U.S. E&O-Cyber Broking Reported Incident - Year

More like this

Podcast

On Aon Podcast: How has CrowdStrike Changed the Cyber Market?

Article

Risk Capital and Human Capital Perspectives

Report

Global Risk Management Survey

22%

Rise in cyber risk insurance claims, while ransomware claims payouts declined 77%

Incident reports by year

Aon U.S. E&O-Cyber Broking Reported Incident - Quarter

Incident reports by quarter

Aon U.S. E&O-Cyber Broking Reported Incident

Explore More Cyber Offerings

- Cyber Risk Analyzer
- Cyber Insurance
- Cyber Quotient (CyQu) Evaluation
- Business Continuity Management for Cyber Risk

Cyber - Incident or Litigation

E&O - Professional Liability

E&O - Tech E&O

E&O - Media Liability

Other/ Unidentified

Despite the turbulence of systemic cyber events and rising claims, the financial impact on the insurance industry was not as impactful as it could have been due to purchasing trends, program structure changes and business continuity measures by insureds. However, the industry is on alert. The past year's series of events amounted to near misses and could have been devastating. These events provided a great lesson on what risks the insurance industry — and organizations — must manage.

Cyber Insurance Market Competition Intensifies

Organizations across North America took cyber risk very seriously in 2024. According to data from Aon's Cyber Quotient Evaluation (CyQu), our eSubmission platform, clients saw improvements in their risk scores across key domains. Insurer confidence was restored in many industries as clients took deep dives into critical — or "red flag" — security controls and domains. For both the U.S. and Canada, the strongest cyber security domain in 2024 was endpoint security, which comprises penetration testing, network environment and network capacity. Application security and third-party security were the two lowest-scoring domains.

Cyber Domains | 2024 North America Data

Overall Risk Score 2.78

Highest Scoring

3.04 Endpoint Security	Endpoint Protection	3.17
	Logging & Monitoring	3.15
	Secure Config.	3.00
2.99 Network Security	Pen Testing	3.31
	Network Environ.	2.96
	Wireless	2.89
2.96 Access Control	Password Config.	3.13
	MFA	3.00
	Access Mgmt.	2.86

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Lowest Scoring

2.31 Application Security	Software Mgmt.	2.19
	Training	2.34
	Secure Dev.	2.42
2.36 Third Party	Due Diligence	2.17
	3rd Party Contracts	2.45
	3rd Party Inventory	2.91
2.66 Business Resilience	BCM/ DR	2.56
	Backup	2.71
	Incident Response	2.72

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Cyber Domains | 2024 Canada Data

Overall Risk Score 2.66

Highest Scoring

3.01 Endpoint Security	Pen Testing	3.35
	Endpoint Protection	3.05
	Network Capacity	2.78
2.96 Endpoint Security	Endpoint Protection	3.13
	Logging & Monitoring	3.13
	Vunerability Mgt.	2.84
2.91 Remote Work	Remote Connectivity	3.40
	Authentication & Identity	3.16
	Device Vuln. & Monitoring	2.81

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Lowest Scoring

1.99 Application Security	Training	1.87
	Software Mgmt.	2.01
	Secure Dev.	2.03
2.14 Third Party	Due Diligence	1.94
	3rd Party Contracts	2.27
	3rd Party Inventory	2.65
2.57 Business Resilience	BCM/ DR	2.39
	Backup	2.58
	Incident Response	2.74

CyQu Risk Maturity Scoring

Initial: 1.0 - 1.9

Basic: 2.0 - 2.5

Managed: 2.6 - 3.4

Advanced: 3.5 - 4.0

Critical controls also improved. Seven percent of clients improved the target time for critical patching, moving from more than seven days to three-to-seven days, and noticeable growth was reported in disaster recover/backups and multi-factor authentication (MFA).

Renewal Clients Critical Controls | YE 2024

2023

2024

6% Improvement YoY Aon Renewal Clients

The Red flags shown are categorized as ‘imperative’ and ‘critical’ as determined by the market conditions – higher criticality weightings are more likely to impact underwriting.

Improvements YoY were noted in:

- 7% of clients improved from target time for critical patching >7 days to 3-7 days
- Disaster Recovery/Backups
- Multi-Factor Authentication (MFA)

Data for over 1,350 renewal clients in the US. SME ($0-$100M) and Middle-Market ($100M-$2B) account for 78% of the data.

Notably, the impact of ransomware diminished in 2024. The global average ransomware payment amount declined by 77 percent compared to the same period in 2023, as more robust security controls and business continuity planning made it more difficult for attackers to deploy successful attacks. We also saw more organizations withhold ransomware payments, instead engaging with the event. Meanwhile insurance became more confident in underwriting ransomware risk. The industry’s response to the growing supply chain risk in 2024 was also proactive, and Aon clients invested in modeling their cyber exposure across vendors. However, due its complexity, third-party risk continued to hold its position as one of the lowest-scoring risk domains for Aon clients in the U.S. and Canada.

Cyber Domains | 2023 vs 2024 North America Data - Total Score by Domain

Cyber Domains | 2023 vs 2024 North America Data - Total Score by Industry

2023

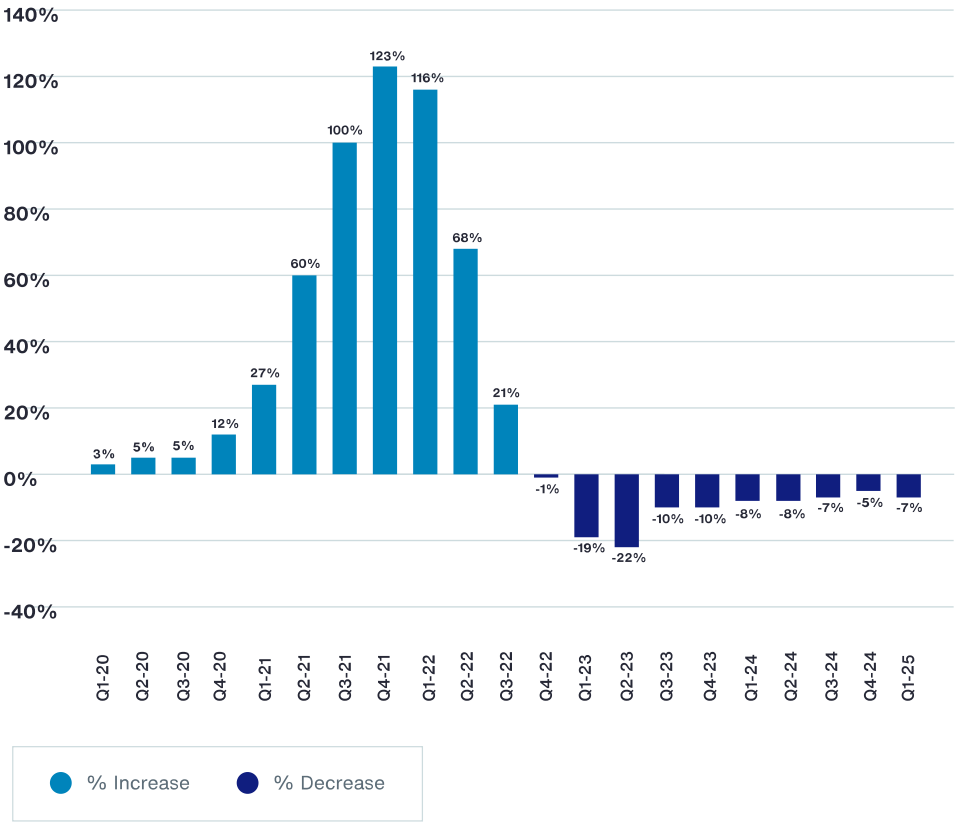
2024

* ‘Other Industries’ category represents responses from clients in the following industries: Financial Sponsors, Hospitality, Travel & Leisure, Insurance, Life Science, Sports & Entertainment.

As organizations strengthened their controls, competition soared across the cyber insurance industry. Despite the increase in claims frequency in 2024 and poor loss development on 2023 claims, buyers’ market conditions continued through the year in a well-

capitalized and competitive environment. On average, U.S. buyers achieved a seven percent premium decrease in Q1 2025.

2020–2025 Cyber Premium Changes by Quarter
Average Year–over–Year Change (Same Clients)



The Canadian market saw accelerated softening through 2024 and ultimately realized a 15 percent decrease year-over-year. Insureds became more sophisticated, harnessing cyber modeling to evaluate their purchasing decisions, determine the appropriate limit levels, and protect their balance sheets. Aon saw 25 percent of clients purchase additional limits in 2024

Reports of abundant and alternative capacity in North America led to a favorable January 2025 cyber reinsurance cycle, indicating that buyer-friendly market conditions will likely continue.

Volatility Heightens and Insurers Act

With intense geopolitical volatility marking the start of 2025, cyber risk is anticipated to continue to heighten. In March, the U.S. announced the pause of offensive cyber operations against Russia by U.S. Cyber Command, rolling back some efforts to contend with a key adversary even as national security experts call for the U.S. to expand those capabilities.[5] China's espionage and intelligence collection capabilities reached an inflection point in 2024[6] and, among nation-states, China-nexus activity surged 150 percent overall, with some targeted industries suffering three to four times more attacks than the previous year.[7] This risk environment puts substantial pressure on the insurance industry and organizations to respond.

Insurance companies are expected to bolster investment in the underwriting process and risk modeling to better understand the risk ecosystem and potential exposure. Privacy liability is another risk that insurers and organizations alike must manage. The recent cyber security incident involving an education technology company resulted in the unauthorized exfiltration of certain personal information of minors and the disclosure of millions of student records.[8]

Privacy Liability and Supply Chain Risk Come to the Forefront

In the U.S., multiple instances have occurred where settlements went north of $30 million because of a failure to properly protect customer data.[9] We are beginning to see a more punitive climate and while is this not seen to the extent present in the U.S., Canada is not exempt from this trend. In previous years, courts across Canada exercised their gatekeeping role to halt to data breach class actions that lacked evidence of harm to the proposed class members.[10] This tide is shifting. Common allegations in new class action filings in 2024 ranged from misuse of information to a lack of protections for children and teenagers who use online services. Canadian courts are continuing to consider and grapple with potential new privacy torts.[11]

Insurers must be mindful of this situation and consider policy structure changes such as advising clients on additional coverage

as settlement values climb. Strengthening technology strategies and controls around privacy or data breaches and knowing where the data sits —and classifying that data — is critical. It is ever more important that cyber, marketing and legal teams align to understand the risk better and prepare to manage and respond to an incident in compliance with regulatory frameworks. A subset of class action lawsuits will likely emerge as new technologies emerge, such as artificial intelligence. These lawsuits are already happening with companies facing a new cyber threat based on “pixels,” the code placed on a webpage or an online advertisement to collect information about a user’s interaction.[12]

Recommended Actions

Use data analytics and risk modeling to make informed decisions around investment in security controls, business continuity planning and cyber insurance purchasing.

For insureds — evaluate your cyber insurance policy and take advantage of ripe market conditions. Consider supply chain and privacy risk exposures.

For insurers — ensure stability of your portfolio as uncertainty prevails. Consider long-term rate agreements, auto-renewals, and above all, partnership between client and insurer.

Download these findings

References

[1] $45 Million MGM Settlement Resolves Data Breach Lawsuits Over 2019, 2023 Cyber Attacks. ClassAction.org. Kelsey McCroskey. February 20, 2025.

[2] Key Market Trends: Growing Cyber Claims Frequency, Ransomware Dominance, and Declining Payouts. Aon Risk Report. Aon. June 2025.

[3] 5 risk factors from supply chain interdependencies in a complex cybersecurity landscape. World Economic Forum. Akhilesh Tuteja. January 31,

2025. https://www.weforum.org/stories/2025/01/5-risk-factors-supply-chain-interdependencies-cybersecurity/

[4] Raphael Yahalom. What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk. Harvard Business Review. January 10, 2025.

[5] Hegseth orders suspensions of the Pentagon's offensive cyberoperations against Russia. AP News. Lolita C. Baldor and David Klepper. March 3, 2025.

[6] CrowdStrike 2025 Global Threat Report. CrowdStrike. February 2025. https://www.crowdstrike.com/en-us/

[7] Ibid.

[8] PowerSchool data breach exposes student records in massive cyber-security incident. ETIH. The Future of EdTech. Emma Thompson. February 5, 2025. https://www.edtechinnovationhub.com/news/powerschool-data-breach-exposes-student-records-in-massive-cyber-security-incident

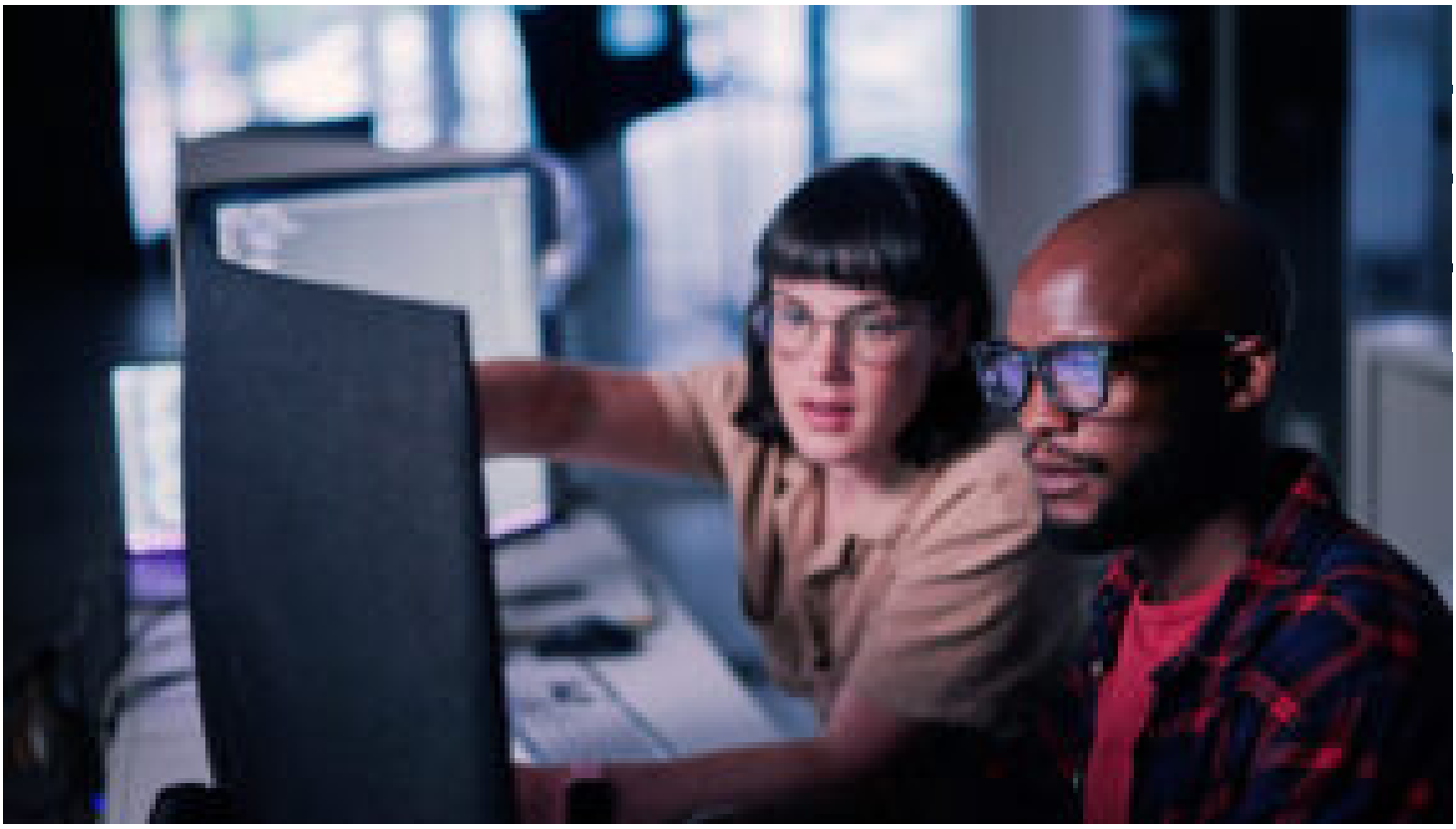
[9] $45 Million MGM Settlement Resolves Data Breach Lawsuits Over 2019, 2023 Cyber Attacks. ClassAction.org. Kelsey McCroskey. February 20, 2025.

[10] Canadian privacy class actions evolve beyond traditional data breaches. Osler. Robert Carson. January 11, 2023. https://www.osler.com/en/insights/updates/canadian-privacy-class-actions-evolve-beyond-traditional-data-breaches/

[11] Canadian privacy class actions evolve beyond traditional data breaches. Osler. Robert Carson. January 11, 2023. https://www.osler.com/en/insights/updates/canadian-privacy-class-actions-evolve-beyond-traditional-data-breaches/

[12] Pixels and Privacy. A New Wave of Class Action Litigation. LAW.COM. Ian M. Ross and Sidley Austin. March 15, 2024.

The Five Drivers That Can Help Mitigate Growing Reputation Risks



Key takeaways

There are certain cyber attack techniques that are much more likely to become reputation risk events than others.

Reputation risk events can cause shareholder value to fall by an average of 27%.[1]

Reputation risks are nontransferable, but five drivers of value recovery can help companies mitigate them.

Damage to Brand or Reputation is a top-10 risk facing organizations globally today, according to Aon's latest Global Risk Management Survey (GRMS)[2] — and has been one since 2007.

It should be no surprise that businesses are concerned about reputation risks. In this highly volatile, highly digitalized world, any single disruptive event can significantly and rapidly threaten a business's reputation. Such events — which include cyber events — may then cause financial markets to reassess their projections around future cash flows, affecting shareholder value. Where a potential negative event, such as a cyber attack, is mishandled, the damage can also go beyond the reputational premium: consumer

More like this

Short Questionnaire for complementary report

Value Recovery Index (VRI)

Report

and employee trust may erode, with knock-on effects for sales and brand value.

As the world becomes increasingly interconnected and cyber attacks get more sophisticated, these risks will only continue to grow. Large cyber attacks on critical U.S. infrastructure and services in December 2024 are an example of the significant threat now posed by this class of risks. As part of these attacks, hackers broke into the U.S. Treasury Department's systems, accessing unclassified documents and employee workstations.[3] In addition, at least nine U.S. telecom companies were compromised through a coordinated cyber espionage operation, with hackers able to record the phone calls of — and even geolocate — millions of Americans.[4]

While reputation risk has historically been challenging to quantify, Aon's research shows that a major attack can have a significant long-term impact on a company's share price. Our 2023 analysis of 47 prominent cyber events showed, for example, that a major cyber incident resulted in an average 9 percent decrease in shareholder value in the year following the event.[5]

How then should businesses approach these reputation risks? Reputation risk is one of the most important of a growing number of risks that are either uninsurable or only partially insurable.[6] Businesses looking to avoid incurring losses as a result of these risks will need to make sure they have a thorough understanding of the risks in question and take steps to manage them. This article concludes with our five drivers of value recovery, which are the levers that companies will need to help minimize their risk of a value-destroying reputation risk event.

When a Cyber Event Becomes a Reputation Risk Event

This year, the Aon team has extended its previous research to assess the impact on shareholder value of different types of cyber events. As with our 2023 research, the findings are derived using a clear, objective definition of reputation risk and proprietary algorithms that can help accurately identify the magnitude of reputational damage, including a shareholder value algorithm that

Global Risk Management Survey

Article

A Highlight Year For Systemic Risk – And Single Point Of Failure Events

-45%

Average impact on shareholder value for reputation risk events stemming from Network and System Attacks [10]

Explore More Cyber Offerings

- Reputation Risk Consulting
- Business Continuity Management for Cyber Risk
- Cyber Risk Analyzer
- Cyber Impact Analysis

can isolate changes in share price that are caused by company-specific factors from those that are due to market noise.

We analyzed 1,407 cyber events reported in the media up to the end of 2024, of which more than 96 percent were of a malicious nature. We split these events across five categories, based on the cyber-attack technique involved:

- Malware/Ransomware: Malware damages or disrupts access to a computer system. Ransomware is a type of malware that blocks user access until a ransom is paid.
- Unauthorized Access and Credentials Attacks: Attempts by an attacker to gain user credentials to access networks or systems.
- Human Factors: Cyber events stemming from unintended actions by employees such as falling for a phishing scam or failing to follow security protocols.
- System Exploits: Events in which attackers exploit system vulnerabilities by, for example, injecting malicious code using Structured Query Language.
- Network and System Attacks: Events that aim to compromise the integrity and availability of a system — such as denial of service attacks.

Of the 1,407 cyber events we examined our analysis shows that 49 developed into reputation risk events, causing shareholder value to fall by 27%.[7] Our findings suggest that some cyber-attack techniques are more likely to become reputation risk events than others. Malware/Ransomware attacks make up a disproportionate number of the identified reputation risk events, accounting for approximately 60 percent of reputation risk cyber events but only 45 percent of all cyber events.

Cyber Attack Techniques - Counts - All Events

Malware/Ransomware

Unauthorized Access and Credential Attacks

Human Factors

System Exploits

Network and System Attacks

Cyber Attack Techniques - Counts - Reputation Events

Malware/Ransomware

Unauthorized Access and Credential Attacks

Human Factors

Network and System Attacks

System Exploits

Key Observations:

- Ransomware/Malware is by far the most common type of cyber attack
- At a reputational risk level, it becomes even more prevalent

Why is it that some event categories are more likely to break through into reputation risk events than others? Malware/Ransomware attacks had a 18 percent chance of developing into a reputation risk event, compared with, for example, just an 6 percent chance for System Exploits attacks.[8] For cyber events, as for other types of events, there is most likely to be large-scale media pickup where there are emotive issues at stake or issues that could be deemed to be in the public interest. Malware/Ransomware attacks fall squarely into these categories.

While Malware/Ransomware attacks may be most likely to become reputation risk events, they may not have the biggest impact. From a severity perspective, Network and System Attacks were typically the most damaging, causing a 45 percent fall in shareholder value. At the other end of the spectrum — though still representing a major risk — Unauthorized Access and Credentials Attacks showed an average effect on shareholder value of –25 percent.

Cyber Attack Technique - Impact

Cyber Attack Technique	RR Likelihood	Mean SVI*
Network and System Attacks	16%	-45%
Human Factors	10%	-31%
Malware/Ransomware	18%	-27%
Unauthorized Access and Credential Attacks	8%	-25%
System Exploits	6%	-13%

Cyber Attack Techniques – Best/Worst Impact

Human Factors

Malware/Ransomware

Network and System Attacks

System Exploits

Unauthorized Access and Credential Attacks

As these results show, there is a fairly weak correlation between the types of attack that are most likely to evolve into a reputation risk event and the types that — once they become a reputation risk event — are likely to have the most severe impact on shareholder value. This is because it is media attention that determines whether an issue breaks through, while the level of shareholder value destruction will typically depend on the magnitude of the direct impact on the customer. Network and System attacks, for example, can often result in a rupture of service, which can severely inconvenience — or even harm — customers.

Recommended Actions The Five Drivers of Value Recovery

As we have seen, the number of uninsurable risks is growing and in many cases these risks are also becoming more severe. In the absence of risk transfer options, companies should consider how to mitigate these risks while also setting aside resources to help absorb any shocks that do occur.

Based on our many decades of serving clients on this issue, we have derived five drivers of value recovery:

> Preparedness: Companies need to ensure they have access to the analytical insights required to develop a full understanding of reputation risks and take

appropriate steps to help prevent and mitigate potential losses.

Leadership: Where events do occur, strong and visible leadership is essential.

Action: Companies need to take rapid, targeted, and credible action in response to any event.

Communication: Affected companies need to communicate quickly, openly and honestly about both what has transpired and their response.

Change: Following the event, companies will need to demonstrate true remorse and a commitment to meaningful change.

Those companies that can use these levers successfully can help mitigate shareholder value destruction and may even gain a reputational boost. Our 2023 research found that companies successfully navigated 17 of the 47 studied cyber attacks, realizing an average increase in shareholder value of 18 percent.[9] For the remaining 30 events, however, shareholder value saw an average 21 percent drop. Understanding and mitigating reputation risks can help companies preserve significant value and should be a high-priority investment.

Revised statistics as of July 2, 2025

References

[1] Over and above the movement of the market.

[2] Global Risk Management Survey: Ninth Edition, Aon, 2023, https://www.aon.com/en/insights/reports/global-risk-management-survey.

[3] Nadine Yousif and Joe Tidy, “US Treasury says it was hacked by China in ‘major incident,’” BBC, December 31, 2024, https://www.bbc.com/news/articles/c3weye2j0e7o.

[4] A.J. Vincens, “US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage,” Reuters, December 27, 2024, https://www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27/.

[5] “Build a Plan to Address the Perils of Reputational Risk,” Aon, August 1, 2023, https://www.aon.com/2023-cyber-resilience-report/risk/build-a-plan-to-address-the-perils-of-reputational-risk.

[6] “Key Findings,” in Global Risk Management Survey: Ninth Edition, Aon, 2023, https://www.aon.com/en/insights/reports/global-risk-management-survey.

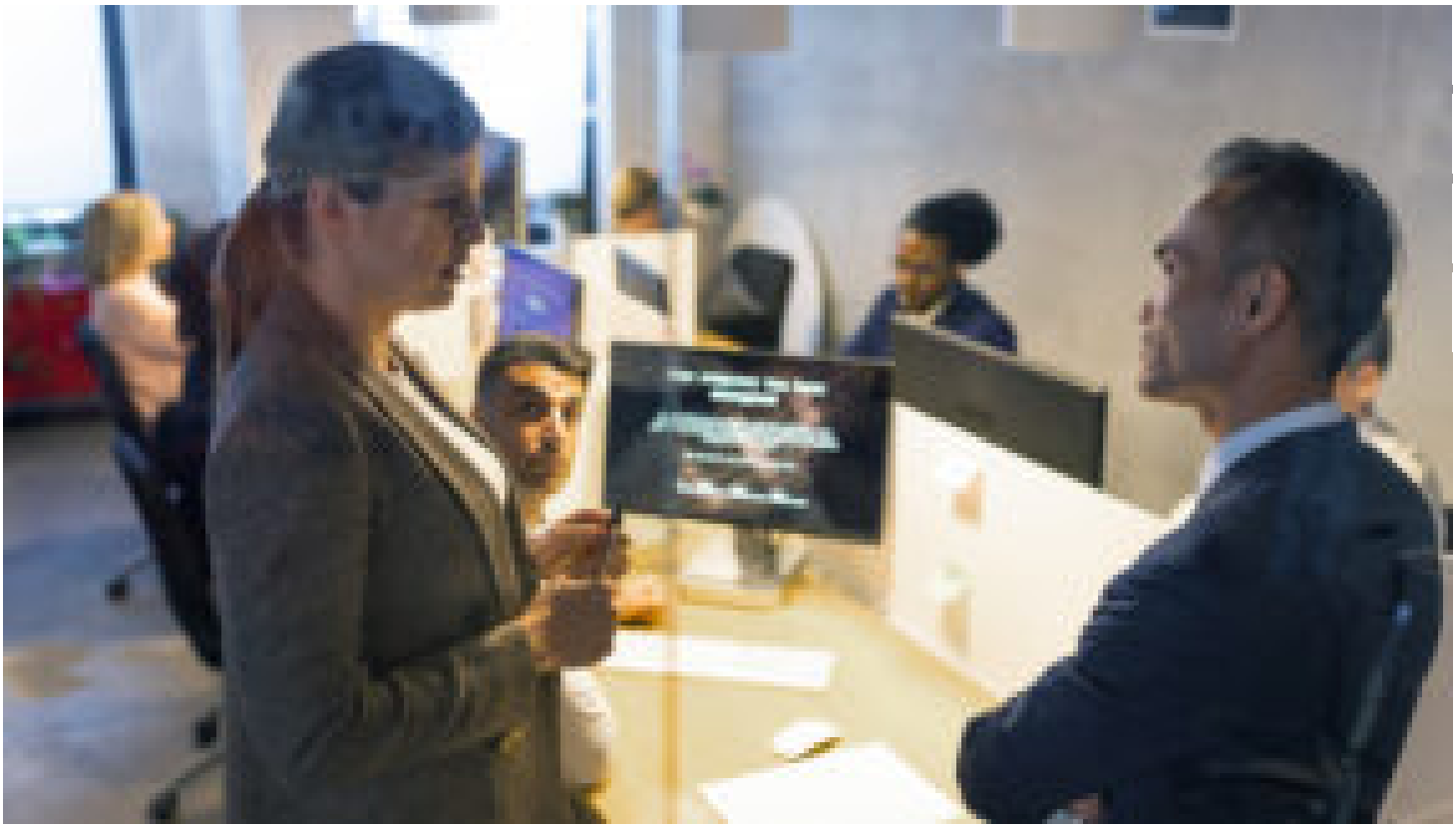
[7] We judge that a cyber event became a reputational risk event if it targeted a publicly listed company, garnered a very substantial portion of the media attention devoted to that company, and had a negative effect on shareholder value within the following year. To be able to assess the medium-term effects, an event had to have taken place more than a year before the date of the analysis to qualify as a reputational risk event.

[8] These probabilities are not calculated using the full set of 1,407 cyber events, because these include events that happened within the last year and that targeted companies that were not publicly listed — and therefore could not have been classified as reputational events by our definition. There were 188 Malware/Ransomware events that targeted public companies and that happened more than a year before the date of analysis, of which 33 were flagged as developing into reputational events.

[9] “Build a Plan to Address the Perils of Reputational Risk,” Aon, August 1, 2023, https://www.aon.com/2023-cyber-resilience-report/risk/build-a-plan-to-address-the-perils-of-reputational-risk.

[10] Over and above the movement of the market.

A Highlight Year For Systemic Risk – And Single Point Of Failure Events



Key takeaways

2024 was a highlight year across the cyber reinsurance space. It revealed new and undiscovered single points of failure and served as a call to action.

Insurers continued to collect data surrounding technology dependencies and moved to collect more intelligence around contingent business interruption or system failure risk.

Organizations found that managing systemic risk is a shared responsibility. Identifying which vendors are the most business-critical and employing cyber risk scenario modeling is essential.

Technology interdependence is a Faustian pact. The interconnectedness that defines our world ushers in innovation, collaboration, and business growth — yet brings with it great risk.

Systemic cyber risk — the potential for a cyber incident to cause widespread disruption and instability across multiple entities or

More like this

Podcast

industries — is escalating. It's becoming more evident that many organizations cannot control the vendors with which they do business or the technology platforms which drive their business operations. Aon's U.S. Cyber Broking data shows that supply chain issues contributed to 28.5 percent of reported cyber incidents in 2024.[1] The risk is growing. Gartner predicts that by 2025, 45 percent of companies will have experienced attacks on their software supply chains, a threefold increase from 2021.[2] Regardless of what organizations do when it comes to assessing their vendors' business continuity or disaster recovery processes, the potential entry point to introducing new risk is very real and unavoidable.

As was seen throughout 2024, losses typically result from an aggregate event and can either be malicious or non-malicious.[3] The ransomware breach of a healthcare payments technology provider involved the private data of approximately 190 million individuals and also rippled to doctors' offices and hospitals, resulting in severe cashflow problems and threatening patients' access to care.[4] The direct financial costs for the breached company was likewise extreme, tallying $3.09 billion pre-tax,[5] [6] and the company also provided $9 billion in interest-free loans to impacted businesses. The June ransomware attack on a company that provides software for automotive dealerships disrupted operations at thousands of dealerships across the U.S., resulting in tens of millions of dollars in lost earnings for a wide range of companies.[7] The 'CrowdStrike event' caused 8.5 million systems to crash, disrupting operations across thousands of organizations worldwide and resulting in a revenue impact of $500 million for a major U.S. airline.[8] Wrapping up the year, the ransomware attack on a U.S. supply chain management provider rippled globally.

Single Points of Failure

A single point of failure refers to any technology or system that, if it fails, will cause disruption to many companies. Last year was a notable year across the cyber reinsurance space for the sheer number of single points that may exist. For businesses and insurers, this was a catalyst for action. However, gaining visibility into this risk is a real challenge. Fortunately for insurers, the losses across 2024 were lower than expected. For Aon clients, through

Special Edition: Global Trade and its Impact on Supply Chain

Article

The Five Drivers That Can Help Mitigate Growing Reputation Risks

Report

Climate and Catastrophe Insight

29%

Of reported cyber incidents in 2024 can be contributed to supply chain issues.

Explore More Cyber Offerings

Supply Chain Risk Management

Cyber Insurance

January 2025, 70 claims were reported in response to the CrowdStrike incident, and of those, only 10 percent remain open, and 90 percent closed without any payment. Despite this positive outcome for carriers, the marketplace remains on high alert.

In response to systemic risk, organizations are striving to protect themselves contractually. Many organizations, especially technology platform providers, are attempting to mitigate their potential limitational liability. On the counter-side, businesses that depend on certain technologies are trying to increase their limitation of liability so that, in the case of a system failure, a written demand can be issued. While contracts can protect, systemic risk is a shared responsibility. Large organizations, for example, might distribute cloud computing dependencies across several geographic regions. This way, they are not solely dependent on a single point of failure associated with a cloud provider. These large organizations might also think through business continuity disaster recovery to help mitigate as much of the financial exposure as possible.

As insurers become more educated about systemic risk, coverage waiting periods surrounding business interruption and contingent business interruption are more common within policies. These waiting periods specify a timeframe during which the insured must cover losses before activating insurance benefits, almost like a deductible in time. Straight-period deductibles pay benefits based on the total business interruption time minus the “time deductible.” With a franchise deductible, businesses are paid for the complete downtime once the “time deductible” window has passed. Waiting periods present another layer of protection for insurers from single points of failure risk. For retail insurers, it is essential to be aware of the policy nuances regarding business interruption, as this can have a meaningful difference on loss.

Ultimately, insurers know that certain risks are unavoidable. For example, most businesses will be interdependent on large cloud providers. This web of interdependencies is challenging even to contemplate — let alone manage. Insurers can still work to help balance systemic risk by investigating which clients and providers are connected — including their downstream dependencies — and then segmenting that data within industry, country, and business size groupings. They should also identify which combinations have

Supply Chain Risk
Diagnostic and Analytics
Cyber Risk Analyzer

higher concentration with specific single points of failure and build a portfolio considering the difference in levels of diversity across the technology stack. This segmentation can be critically vital for smaller companies, as this segment typically relies on the same subset of managed service providers and the take-up of cyber insurance is significantly lower for small businesses. Less than 5 percent of companies with annual revenue of less than $1 million have cyber insurance, and approximately 20 percent to approximately 40 percent of companies with annual revenue of $1 million to $10 million have cyber insurance. Contrasted with over 55 percent of companies with annual revenue over $10 million have cyber insurance, scaling up with company size.[9]

Financial quantification and cyber scenario modeling are essential for organizations to understand their systemic risk exposure. Devising a roadmap and investment strategy for scenarios that could cause the most material financial loss can make the risk more manageable. Organizations are urged to invest in critical, or red flag, controls defined by the cyber insurance industry.

Based on 2024 Aon global data, 57 percent of global and enterprise clients reported cyber vulnerability scans that cover less than 100 percent of the enterprise, and 36 percent had greater than 10 service accounts. Rounding out the top five red flags for large and multinational organization were backups not stored in a secondary data center, no tabletop exercises performed in the last year and target time for patching that exceeded seven days. Middle market and small to mid-sized enterprise critical red flags differed, with 59 percent reporting a lack of annual tabletop exercises and 49 percent reported backups not stored in secondary data center. The next three critical red flags included vulnerability scans that covered less than 100 percent of the enterprise, no incident response plan for ransomware, and no multi-factor authentication to combat ransomware.

Global & Enterprise

2024

Key Observations:

Although the number of service accounts is greater in larger organizations, privileged service accounts tend to be better managed.

When a client has less than 100% covered in vulnerability scanning, segmentation is reviewed which is not captured in the above.

Middle Market & SME

2024

Key Observations:

Privacy, while not necessarily from a risk perspective is an increased focus of carriers in terms of the controls that are in place around how insureds collect user information.

*IBM's Cost of a Data Breach Report found that having an incident response team and formal incident response plans enables organizations to reduce the cost of a breach by almost half a million US dollars (USD 473,706) on average.

Across 3,200 Aon global clients, of which North America and EMEA account for 94 percent of the data, the average global risk score was 2.71 or approaching managed. Endpoint Security at 2.96 was the highest scoring domain, and within that are contained the subdomains endpoint protection, logging and monitoring and security configuration. Conversely the lowest scoring domain was third-party at 2.26 with its top scoring subdomains of due diligence, third-party contracts, and third-party inventory.

While companies can't eliminate reliance on third parties, they can identify which are the most business-critical to operations and develop a mitigation plan and a response playbook in the event one or more of those vendors suffer a significant event.

Recommended Actions

Analyze the impact of systemic risk. Understand the interdependencies across your technology stack and develop a response playbook in the event one or more vendors suffer a significant event.

Be cognizant of cyber insurance policy nuances regarding business interruption, as this will have a meaningful difference on loss. Consider waiting periods, what events your business interruption and contingent business interruption (BI/CBI limits

cover and, for insurers, strategically balance cyber risk portfolios.

Strengthen third-party risk controls, including back-ups, incident response (IR) and business continuity management.

References

[1] Based on manual tracking data that Aon's claims team maintained for a few of the widespread events in 2024, comparing our manual tracking to our total claims volume for 2024 as documented in CRP.

[2] Gartner Identifies Top Security and Risk Management Trends for 2022. Gartner. Press Release. March 7, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

[3] 2024 Cyber Risks Update. Beazley. October 1, 2024. https://www.beazley.com/globalassets/ir-documents/presentations/2024/cyber_risks_1st_october_update.pdf

[4] Chairman Brett Guthrie. What We Learned: Change Healthcare Cyber Attack. U.S. Department of Energy and Commerce. May 3, 2024. https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack

[5] United Health Group Incorporated. Form 8-K. January 16, 2025. Securities and Exchange Commission (SEC). https://www.sec.gov/ix doc=/Archives/edgar/data/731766/000073176625000022/unh-20250116.html

[6] UnitedHealth hikes number of Change cyberattack breach victims to 190M. Emily Olsen. CybersecurityDive. https://www.cybersecuritydive.com/news/change-healthcare-attack-affects-190-million/738369/#:~:text=Dive%20Insight:,and%20file%20prior%20authorization%20requests.

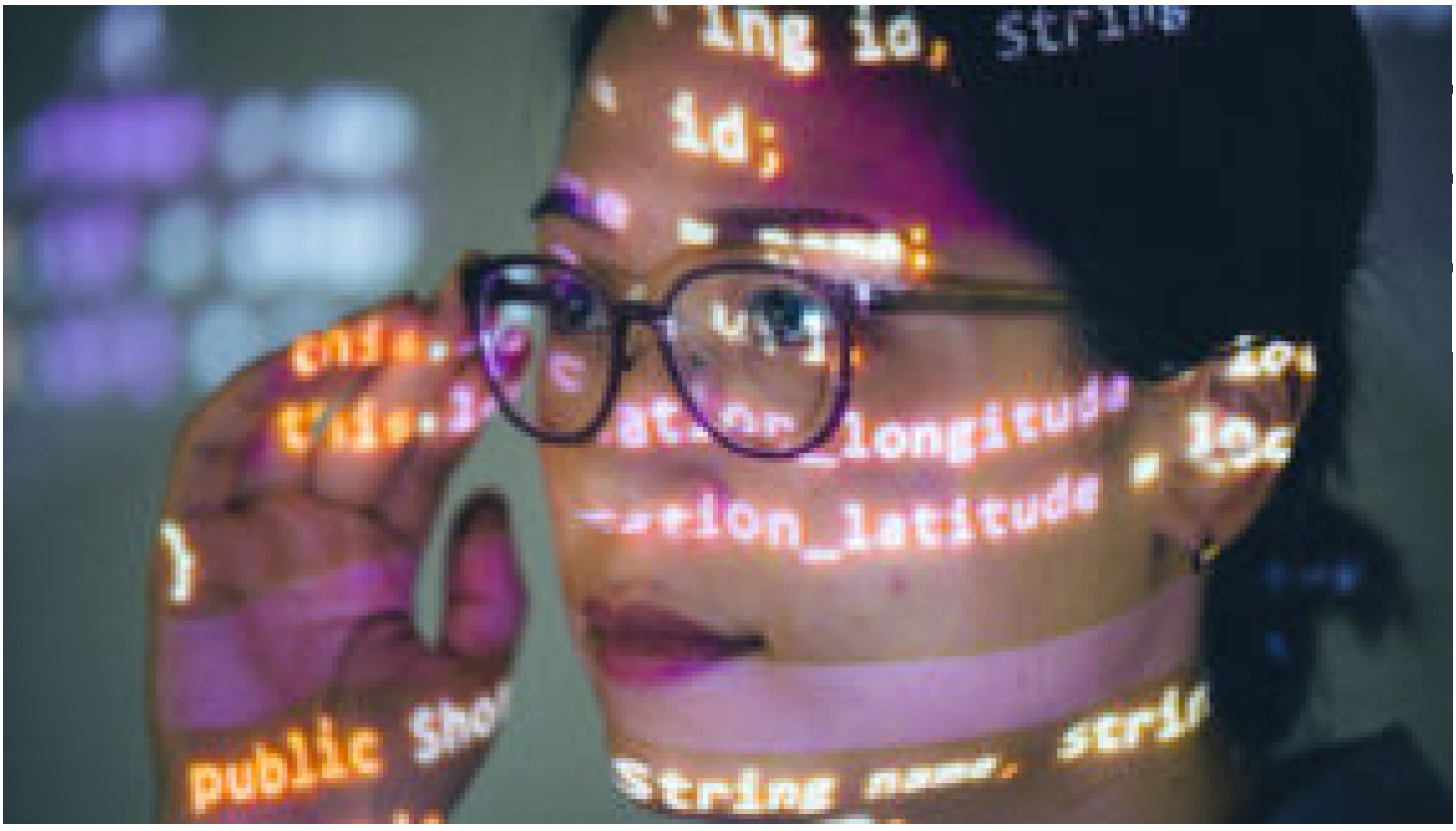
[7] AutoNation, Inc. Form 10-Q. September 30, 2024. SEC. https://www.sec.gov/ix?doc=/Archives/edgar/data/350698/000035069824000111/an-20240930.htm; Sonic Automotive, Inc. Form 10-Q. September 30. 2024. SEC.

[8] Delta Airlines Inc. Form 8-K. August 8, 2024. https://www.sec.gov/ix?doc=/Archives/edgar/data/0000027904/000168316824005369/delta_8k.htm

[9] Moody's Cyber Industry Exposure Database. Aon Analysis. March 2025. https://www.moodys.com

The information contained herein and the statements expressed are of a general nature, not intended to address the circumstances of any particular individual or entity and provided for informational purposes only. The information does not replace the advice of legal counsel or a cyber insurance professional and should not be relied upon for any such purpose. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Tackling Ransomware: Helping Insurers and Their Clients Keep Pace with Change



Key takeaways

The level and type of cyber threat will be different from company to company. That also means there's typically no one-size-fits-all cyber control.

Companies and insurers need to stay up-to-date on the potential effectiveness and relevancy of certain controls — like end-point detection and response

This study can help everyone involved in cyber security better understand, manage and price risk.

Improving cyber-risk posture and minimizing the attack surface area can have benefits and incentives for both the commercial buyer and their insurers. And understanding and sharing valuable insights can be a critical driver in helping to reduce the frequency and severity of cyber security incidents and claims.

Insurance data is important in helping to guide insurers and commercial buyers make better-informed cyber security decisions. Buyers can use the information to understand what can actually

More like this

Article

Buyer-Friendly Cyber Risk Insurance Market Persists

move the needle from a cyber-security perspective. Meanwhile, insurers can use it to understand which practices and controls can have a material impact on the frequency and severity of events and claims.

To gain a better view into how security controls and claims correlate, Aon Risk Capital (encompassing Aon's Cyber Solutions and Aon's Reinsurance Solutions) conducted a study using red flag data from Aon's Reinsurance Solutions' Experience Benchmark Database and from CyQu, Aon's proprietary eSubmission platform. Red flags are defined as the missing critical security controls that may affect insurability based on key technical underwriting concerns. These issues are reviewed and updated regularly based on market conditions and feedback from Aon brokers, consultants and insurers to help insureds improve their buying process while also helping to improve their understanding of cyber resilience.

The study looked at claims experience and security posture data by size of insured buckets — small and medium-sized enterprises or those in the middle market (SME/MM), defined as more than $1 billion in revenue and "large" companies.[1]

The findings shed new light on the shape of the market and the opportunities available to mitigate risk today — and in the future. With sophisticated ransomware attacks keeping pace with the speed of technology adoption, and IT teams and analysts frequently doing more with less, building a comprehensive cyber security program starts with leveraging data and insights from both commercial buyers and insurers. These insights can help lead to better cyber security outcomes, benefiting both parties — a powerful prospect for all.

Controls and Claims: Insights from the Data and Market Experience

One of the key takeaways from the study was the crucial importance of comprehensive controls for both large and SME/MM companies. High correlation was observed between the security controls themselves for both Large and SME insureds, indicating an

Article

Ransomware Payouts Decline Despite Growing Cyber Claims Frequency

Article

Data Methodology

Explore More Cyber Offerings

Cyber Risk Analyzer

Cyber Insurance

Cyber Quotient (CyQu) Evaluation

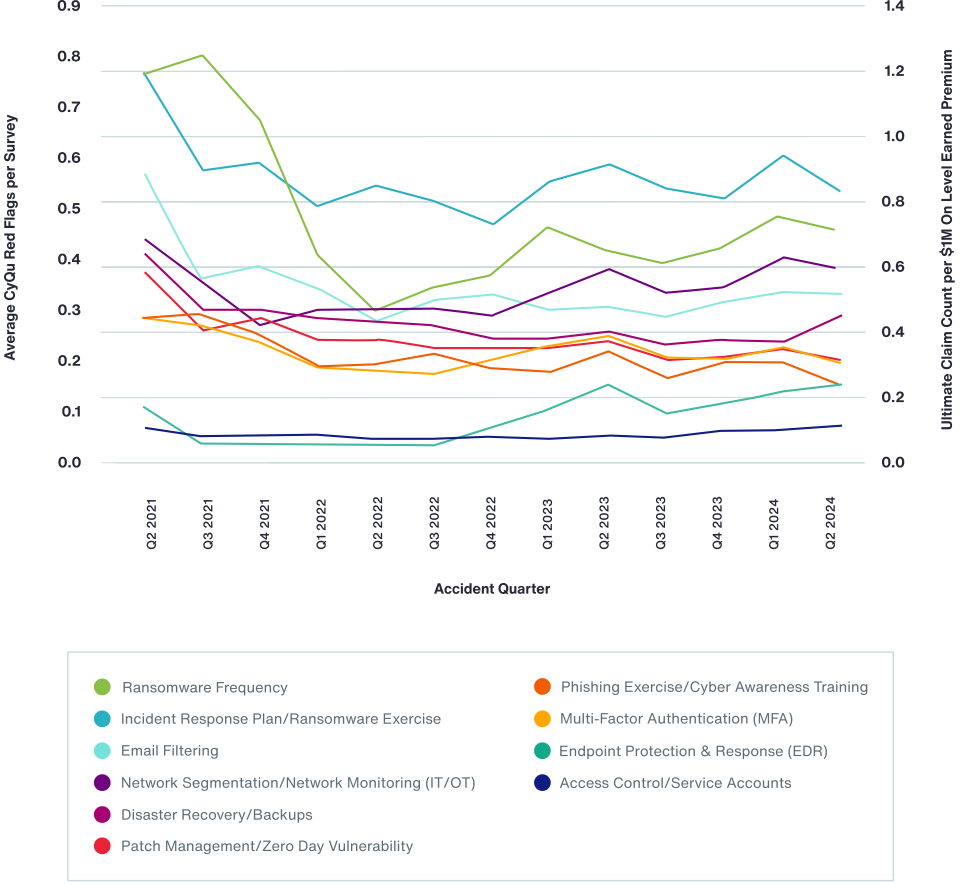
insured is likely to not have other controls in place if one or two essential controls are missing. And gaps in security controls, at the outset, impact a company's insurability.

Importantly, there are different areas where certain controls can affect frequency of ransomware and cyber-attacks compared to their severity — and vice versa. Having comprehensive strategy makes a difference. For instance, practices such as multifactor authentication and phishing education and awareness were observed to play into event frequency, while backup and recovery controls were more likely to affect the severity of an incident. Our CyQu assessment can help companies identify a set of red flags when it comes to severity and frequency and help define a triage plan. Beyond that, gaps in security controls, at the outset, demonstrated to affect a negative company's insurability.

The study shows that ransomware frequency is more closely linked to security controls across large and small to medium-sized companies than non-ransomware frequency. SME/MM-focused portfolios showed stronger correlation between security controls and claims than large- focused portfolios.

Meanwhile, large ransomware portfolio frequency has generally increased over time, while ransomware red flags have generally decreased, helping to explain the negative correlation between some controls and large ransomware frequency. But the findings don't negate the need for comprehensive controls and cyber-security practices. In fact, they highlight other factors in the threat landscape that can have a more sizable impact on large-insured ransomware claims than common security controls alone.

The frequency of ransomware portfolios of SME/MMs with revenue less than $1 billion is a different story. Frequency has decreased over time, while red flags have generally decreased, leading to a positive correlation between controls and SME/MM ransomware frequency.



Other key findings from the study include:

A drop in ransomware frequency observed for SME/MM businesses between second quarter 2021 and second quarter 2022 coincided with significantly reduced security red flags across all security domains, with the most observable reductions occurring within the domains of email filtering and incident response planning.

From second quarter 2022 to second quarter 2024, a steady increase in ransomware frequency coincided with a slight increase in reported endpoint detection and response (EDR) red flags and network segmentation/monitoring red flags.

The change in EDR red flags over time is likely due, in part, to better data capture on end-point detection and response controls over time.

These figures prompt the question: Why does large ransomware frequency appear to be less linked to cyber security controls than SME/MM ransomware frequency? Several factors observed in our study appear to contribute to this dynamic.

Timing. Data from second quarter 2021 to second quarter 2024 show that large insureds generally have fewer red flags in this analysis than SME/MM insureds, so it is plausible that there would be less downward movement on large red flags than on SME/MM red flags over this time period.

The nature of large and SME/MM attacks. Attacks on larger companies are often more likely to be tailored to an individual organization, whereas an attack on an SME/MM insured is likely less effort for a threat actor. Therefore, common security issues could be more likely to be exploited for an attack on an SME/MM, potentially contributing to the higher correlation we see in these results.

Scale. Large-insured CyQu questionnaire responses are less likely to encompass information for the entire company's network as compared to SME/MM insured questionnaire responses, because capturing a security flaw over a vast, interconnected network is more difficult than doing so in a much smaller SME/MM network.

Understanding the Cyber-Security Landscape — Today and Tomorrow

It is encouraging to see cybersecurity posture improve over time across both SME/MM and large companies, as confirmed by data from Aon's CyQu applications. SME/MM companies improved by 22 percent, on average, across insureds and the CyQu security domain categories between the second quarter of 2021 and the same period in 2024.

While recent media coverage suggests that the frequency of ransomware incidents is increasing steadily (except for a lull in 2022), ransomware claim frequency compared to size of portfolio on SME/MM-focused portfolios decreased by 40 percent between quarter two 2021 and quarter two 2024.[2] The positive correlation between this trend and the changes in security posture for SME/MM companies over the same time period suggests that

improved cyber-security controls may be contributing to this favorable ransomware frequency trend.

The data on large-focused portfolios illustrates the changing cyber threat landscape. With ransomware claim frequency on these portfolios increasing between the second quarter of 2021 and the same period in 2024 even as CyQu scores and red flags have improved, it's clear that large companies typically have different vulnerabilities than SME/MM companies. From greater complexity or legacy technology to the scale of potential payments, controls are only one piece of a larger interconnected cyber strategy. The figures highlight the need for further and granular analyses into how changes in cyber security posture affect the frequency of large-insured claims.

Takeaways for Commercial Buyers and Insurers

A major takeaway from the study — and from decades of working with carriers and buyers — is the importance of taking a complete approach that evolves over time in response to threats and technology changes. Threat actors continually adjust their tactics to exploit the weakest areas, and weaknesses can change rapidly. Changes in the most pertinent security controls are captured in Aon's CyQu application and its red-flag methodology as the application evolves to adjust the controls captured and criticality of those controls based on underwriter feedback. Additionally, insureds can benefit from collaborating with Aon's brokers to identify key risks, understand marketplace trends and assess their loss exposure. This can also help improve renewal outcomes.

Insurers

Insurers can make the most of their extensive experience and control data to better calibrate their expectations for insurability and risk selection. In addition to supporting the establishment of these minimum baseline security controls, such data is also essential in the context of deciding which security controls are most important and portfolio management. Often, systematic analysis of experience and loss data reveals subtle trends that can help

insurers evolve beyond a purely “reactive” underwriting and portfolio management posture. Finally, understanding these underlying risk trends can enable insurance carriers to better serve and advise clients on coverage and control optimization and further improve pricing frameworks for individual risks.

All this means that these high-impact, risk-based insights may ultimately promote enhanced underwriting profitability, reduced portfolio volatility and improved client retention rates.

Commercial Buyers

Buyers can use the CyQu assessment to understand their gaps, areas of opportunity and what to prioritize. They can also lean on their claims teams and brokers to provide advice as they develop a comprehensive cybersecurity program. No matter an organization’s size, demonstrating knowledge of risk and effective mitigation strategies, along with investing in controls, can make a difference. Getting the knowledgeable and informed advice, especially when it is focused on the relevant industry and type of data or sensitivities, is a critical component in managing and mitigating risk. And it’s just as important to focus on business continuity and recovery measures to help buyers get on track should an incident occur.

Research Considerations

Aon normalized the responses to these scores by category to look at the correlation between claims and the security scores on an apples-to-apples basis over time, because the questions included in the questionnaire change based on market security priorities. This included dividing the number of missing “critical” controls by the number of possible “critical” controls missing at that point in time.

Severity trends vary significantly by insurance portfolio, so relating insureds severity posture to their security posture needs to be done on an individual-portfolio basis or even policy-level basis rather than at the market level.

Generally, seeing correlation between claims and security scores is difficult at the market level, given the many additional factors driving claim activity. This study would be better conducted by tracking individual insured losses with those particular insureds' security scores. This would also provide more data points in correlation calculations over a short time frame.

Large-focused portfolio correlation metrics were sensitive to updated data in cases where SME/MM-focused portfolio results stayed more consistent in Aon's Trend Study year over year. This is because large-focused portfolios have a much smaller number of claims than SME/MM-focused portfolios, causing volatility in frequency results.

The findings and recommendations take into account potential differences in questionnaire responses between SME/MM and large insureds, the self-reported questionnaire data, as described throughout the article.

References

[1] Aon's Experience Benchmark Database, where the claims information is extracted from, splits loss experience by insurer segments, so an approximately 60 percent threshold is used to determine whether a portfolio segment is classified as "large" or "SME/MM." In the study, SME/MM represents insureds with revenue below $1 billion per year, while "large" represents insureds with $1 billion or more in revenue per year.

[2] Reinsurance Experience Benchmark Database.

timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Behind the Data: Better Decisions Facilitated Through Aon’s Cyber Broking Process

Aon's 2025 Cyber Risk Report leverages proprietary data from the Cyber Quotient Evaluation (CyQu), a patented global cyber e-submission platform, that helps streamline the insurance intake process and strengthens clients' cyber risk management programs by delivering insights into exposures and insurability factors. CyQu, aligned with ISO and NIST frameworks, aids organizations in identifying performance gaps, prioritizing key controls, and tracking changes in cyber maturity. Regular updates, informed by cyber insurance underwriters, improve Aon's brokerage process and ensure alignment with over 65 insurers in the U.S. and EMEA[1]. The CyQu client portal transcends traditional paper applications by providing peer comparisons and security control benchmarks as part of the submission process. It uses analytics and a comprehensive evaluation framework to offer detailed insights into cyber risk posture, enabling vulnerability identification and risk mitigation prioritization.

These insights, along with client benchmarking, claims modeling, and guidance from Aon's account teams, enable clients to enhance their control posture annually[2] and align stakeholders. The Cyber Risk Analyzer[3], integrated with the CyQu platform via Application Programming Interface (API), supports limit adequacy and loss-based modeling, facilitating strategic balance sheet protection. It empowers risk managers to convey the value of insurance and the Total Cost of Risk (TCOR) to the C-suite, fostering stakeholder alignment.

Aon's Broking team leads a collaborative process that improves the insurance purchasing experience by identifying control deficiencies and prioritizing key improvements to optimize pricing and coverage scope. This strengthens Aon's holistic approach, allowing clients to leverage analytics to inform their cyber risk management strategy.

This global process underpins the insights published in this report.

Data and Analytics Team

Nancy Eaves
Managing Director Product Leader – Cyber Solutions

Cario Lullo
Vice President, D&A – Cyber Solutions

Samuel Tashima
Head of Cyber Risk Consulting & Analytics – North America
Director & Actuary, US – Actuarial & Analytics, Global Risk Consulting

Annie Fishbain
VP, Product Management – Cyber Solutions

Data Methodology

Controls: The CyQu assessment evaluates risk across 35 critical controls within nine security domains, providing insights into significant risks and control effectiveness.

The CyQu database benchmarks over 10,000 clients and has 20,000 client users. This 2025 Risk Report is based on CyQu scores from 3,226 Aon clients reported in 2024 across APAC, EMEA, LATAM, and North America, with representation across industries and revenue bands. Scores range from 1 to 4, with trend insights derived from comparisons of 2020, 2021, 2022, 2023, and 2024 data.

CyQu Global Submission data: Companies distribution

Global

Enterprise

Middle-Market

Small and Medium Entity

Market Segment Definitions.

Small Medium Enterprises (SME): < $100 million in revenue

Middle-Market (MM): $100 million – 2 billion in revenue

Large Enterprise: $2-5 billion in revenue

Global: $5+ billion in revenue

CyQu Global Submission data: Regional

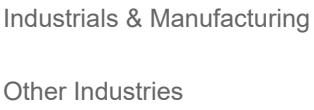
2024

CyQu Global Submission data: Global Industry Distribution

2024

* ‘Other Industries’ category represents responses from clients in the following industries: Financial Sponsors, Hospitality, Travel & Leisure, Insurance, Life Science, Sports & Entertainment.

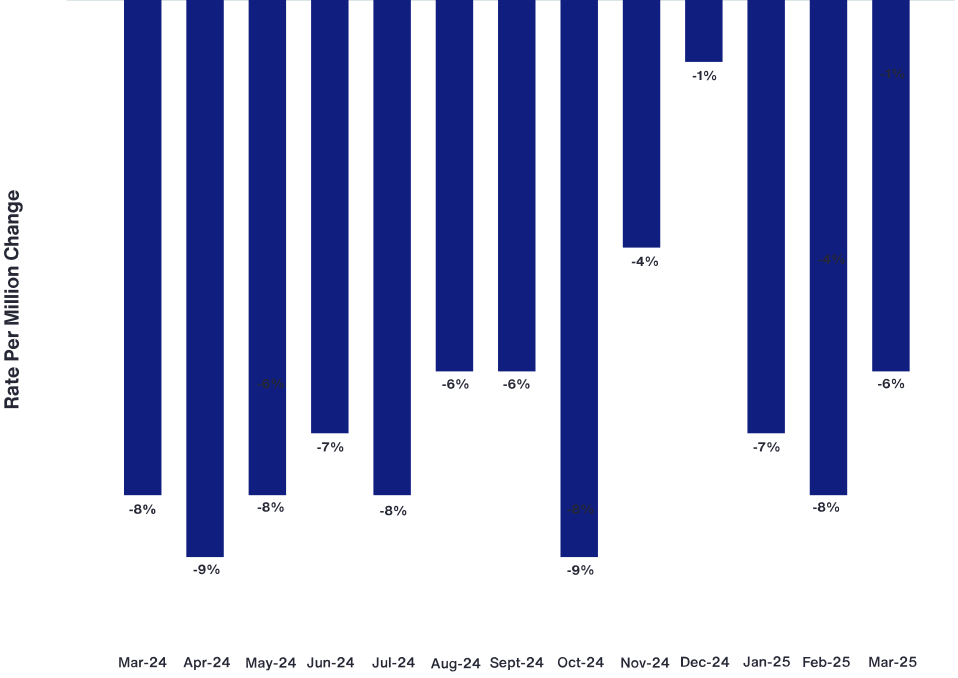
U.S. Operation Technology Industry Distribution



Pricing: Pricing data is collected from over 1,300 Aon clients in the U.S., using a trailing 13-month trend. SME and Middle-Market segments account for 70% of the data. The CyQu Broker Dashboard stores data from over 2,300 active and 7,000 past program towers.

Cyber Monthly Pricing All Layers

Average Year–over–Year Change (Same Clients)



Claims: This 2025 Report's claims analysis is derived from multiple proprietary platforms, including CyQu Broker Dashboard's U.S. Claims Submissions Data (2023-2024), Aon's Global Claims Resolution Database, and Aon's Digital Forensics and Incident Response (DFIR) team's OpenCTI data. Additional sources include Flashpoint (Risk Based Security) analysis by Aon, ransomware statistics from Aon's proprietary large claims data (2023-2024), and intelligence from ransomware leak sites on the dark web. Aon's Reinsurance Experience Benchmark Database offers insights into ransomware and non-ransomware frequency and severity, segmented by SME (insureds with < $1 billion annual revenue) and large insured portfolios (insureds with > $1 billion annual revenue) across various accident quarters split by SME versus Large insured-focused portfolios.

Glossary

Aon's Ransomware Supplemental Application and CyQu Questionnaire provides visibility into an organization's Information Technology (IT) controls to evaluate the vulnerability of a ransomware attack.

As risks continue to evolve, so do Aon's key underwriting controls and risk weightings. The below list reflects a year-over-year control comparison but is a subset of the key underwriting categories and Red Flags Aon helps clients prioritize today.

Key Security Controls Definition

Information Technology (IT)

Disaster Recovery/Backups	Backup capabilities of the clients for its robustness, frequency, storage location and recovery.
Incident Response Plan/Ransomware Exercise	Plans for prompt and effective continuation of business-critical services in the event of a disruption.
Network Segmentation/Network Monitoring (IT/OT)	Measures taken to protect network and data integrity and privacy from attack and infiltration.
Multi-factor Authentication (MFA)	Controls around authentication for remote access, critical networks, and privileged access accounts before accessing organizational data.
Access Control/Service Accounts	Grants authorized users the right to use a service while preventing access to non-authorized users.

Endpoint Protection & Response (EDR)	Delivery and administration of infrastructure services, systems monitoring, endpoint detection, configuration management, storage management, and infrastructure operations.
Email Filtering	Business email security that protects from phishing attacks and prevents data exfiltration.
Patch Management/Zero Day Vulnerability	Vulnerability management by improving, fixing, and updating application systems.
Phishing Exercise/Cyber Awareness Training	Annual phishing training/simulations campaigns, reducing the risk of successful phishing attacks and improving overall cybersecurity posture.

Operational Technology (OT)

Operational Technology	Hardware and software that detects or causes a change in physical processes or events through the direct monitoring and/or control of physical devices (e.g., industrial equipment) in the enterprise.

The following Industries and subindustries are in this report.

Industry	Subindustry
Construction and Real Estate	Commercial Construction, Engineering, Real Estate, Residential Construction, Other
Natural Resources	Mining, Oil, Gas, & Petrochemicals, Power Generation & Distribution, Renewables, Other
Financial Institutions	Asset & Alternative Managers, Banks, Markets Data & Exchanges, Payment & Fintech, Other
Financial Sponsors	Infrastructure & Real Assets, Private Equity (buyout/mid-market/growth capital), Sovereign Wealth Funds, Venture Capital, Other
Food Agribusiness and Beverage	Ag & Food Tech, Agribusiness, Beverage, Food Service, Processing & Manufacturing, Wholesale & Distribution, Other
Healthcare Providers and Services	Providers, Services, Other

Hospitality Travel and Leisure	Casinos, Cruise Lines, Hotels & Resorts, Travel, Other
Industrials and Manufacturing	Advanced Manufacturing, Aerospace & Defense, Automotive, Chemicals, Heavy Industry, Other
Insurance	Health, Life, MGA, Multi-line, Property & Casualty, Reinsurance, Other
Life Sciences	Biotech, Medical Tech & Devices, Nutraceuticals & AgroSciences, Pharmaceutical, Service (CRO/CDMO), Other
Professional and Business Services	Accounting Firms, Business Services, Consultants, Law Firms, Other
Public Sector	Education, Federal, NGOs & Non-profits, State/Local, Other
Retail and Consumer Goods	Consumer Durables, e-Commerce, Leisure Products, Retail, Other
Sports and Entertainment	Film, TV, Radio, & Print, Special Events, Sports, Other
Technology Media and Communications	Content/Media Distribution, Data & Analytics Platforms, Digital Platforms, Hardware & Equipment, Semiconductors & Equipment, Software &

	Services, Telecom Equipment & Services, Other
Transportation and Logistics	Transport Select, Airlines, Integrated Logistics, Marine, Rail, Trucking, Other

References

[1] The majority of largest cyber insurance markets, including Aon Structured Portfolio Solution for clients between $100 million and $2 billion, accept CyQu as their main submission document. Aon Supplementals ransomware, errors and omissions, media content liability, operational technology, privacy and vendor are incorporated into and made part of any application for cyber coverage submitted by the applicant.

[2] Aon Cyber Broking Renewal Critical Controls improved by 6% YOY between 2023 & 2024.

[3] Cyber Risk Analyzer | Aon