CHUBB®



Managing the Velocity of Risk:

Artificial Intelligence, Litigation, and Resilience

2026 Cyber Claims Report

Section One

Introduction: Divergence



The nature of cyber risk continues to evolve, while the scope of vulnerability and exposure to risk expands. Driven by the successful integration of AI-driven detection systems and improved resilience, a number of global markets have seen the frequency of cyber incidents stabilize in 2025, according to recent reports. The U.S., meanwhile, marked an historic high in severity, with the average cost of a data breach in 2025 **exceeding $10.2 million** – more than twice the global average of $4.4 million.

Ultimately, the success of any individual company – or any geographic market – in protecting against cyber incidents rides on understanding the ever-evolving threat landscape, the legal and regulatory frameworks that govern its data acquisition and storage activity, and the interconnectedness of business partners who increase exposure up and down a company's supply chain.

This edition of the Chubb Cyber Claims report explores Chubb's historical claims data through December 2025 to reveal insights on claim frequency and severity trends – and factors fueling these trends – to help businesses navigate a complex cyber risk environment and build financial and operational resilience.

Source: *IBM Cost of Data Breach Report 2025*

Section Two

Global Claims Trends

Across all markets, increases in cyber claims were driven by shifts in technology and legal landscapes as well as the interconnectedness of supply chains. Three trends stand out:

01

AI accelerating the speed of risk.

The same AI technology that has enabled faster and more thorough detection of cyber incidents has fundamentally altered the velocity of incidents: By incorporating agentic and autonomous AI into malware, bad actors are now compromising multiple systems in a matter of minutes – all but eliminating the opportunity for manual intervention. Bad actors' use of advanced AI, such as Large Language Models (LLMs) is increasing at nearly the same pace as AI adoption by everyday consumers.

02

The "litigation-first" reflex.

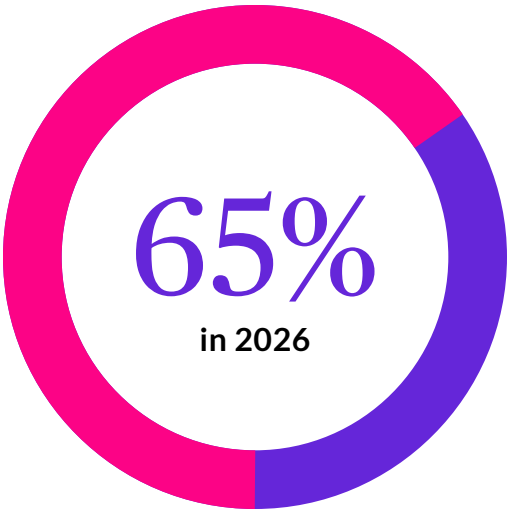
A cyber incident is no longer just a technical failure to be remediated: it is frequently a trigger for legal action shortly after an incident. Over the past 30 years, privacy and data protection laws have been enacted at an extraordinary pace, increasing the complexity of compliance and the frequency of privacy litigation. The gap between a breach and the first class-action filing has diminished, with litigation often ensuing within days, with varying allegations irrespective of the size of the entity or any controls perceived to be lacking.

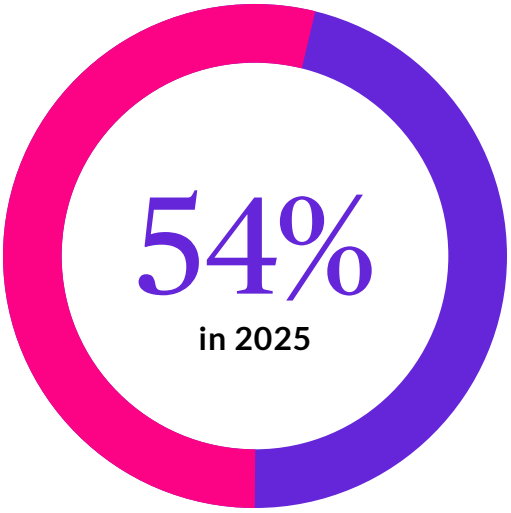
03

Systemic interdependency.

Just a few years ago, risk managers were primarily focused on preventing their own cyber failures from impacting their customers and suppliers. Today, there is widespread awareness of the heavy impact the organization's own supply chain can have on its frequency and severity of cyber incidents.

According to the World Economic Forum, 65% of large companies currently view third-party and supply-chain vulnerabilities as their greatest cyber-related challenge – up from 54% in 2025.





The Jaguar Land Rover Cyber Incident

As described in more detail later, events such as the August 2025 Jaguar Land Rover cyber incident underscored the heavy economic and operational impacts of a cyber incident at any level of a supply chain. The event sent shock waves throughout the entire British economy, wreaking widespread impact in an instant. In addition to the massive financial losses that the carmaker sustained from production shutdowns, it now faces numerous class-action lawsuits relating to the incident.

Section Three

Frequency and Severity of Cyber Incidents

Frequency, the number of claims per policy, and severity, the average cost per claim, are the fundamental components of insurance loss costs and the main drivers of changes in insurance premiums. Since insurance is inherently a business where the premium charged lags the actual cost of claims, recent historical trends in frequency and severity are a leading indicator of rates in the coming year.

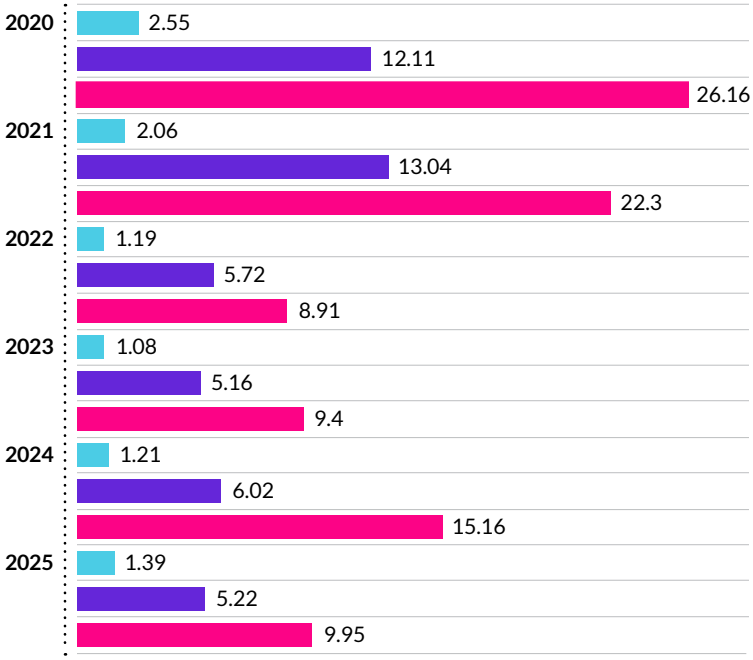


The adjacent tables show a mixed picture of frequency and severity trends within the U.S. cyber landscape over the past six years.

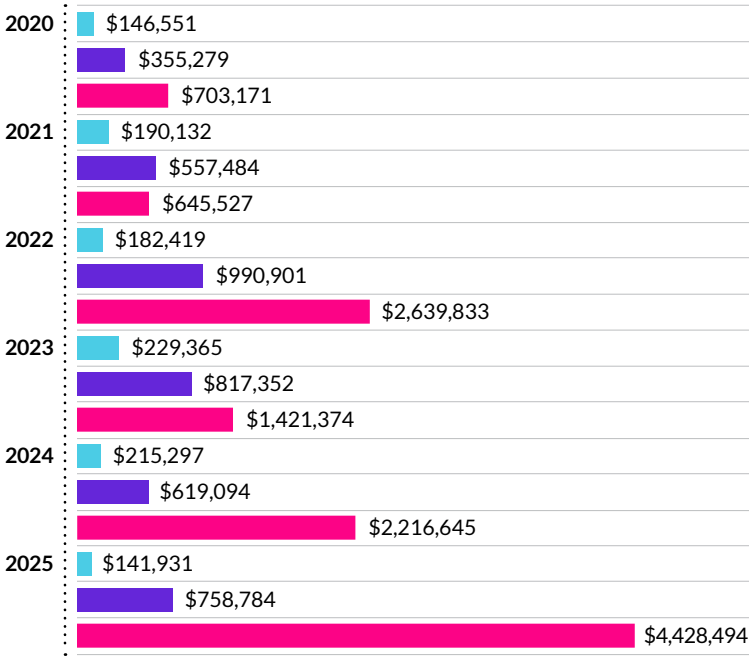
The improvements in clients' security profiles and resilience capabilities are reflected in the significant reduction in claims frequency across businesses of all sizes between 2020 and 2022. At the same time, the data reflects a general increase in frequency within the Small and Medium sized Enterprises (SME) and large risk cohorts since 2022, while the middle market remained more stable during the same period.

Limit deployment has decreased since 2021, even as severity has increased. While severity remained stable in the SME segment, it increased considerably in the middle market and even more dramatically in the large account segment. There are several contributing factors to this increase, including the rise in business interruption expenses and the increasing cost of both data breach- and privacy-related litigation.

Frequency of Cyber Claims per 100 Policies (U.S.)



Average Severity of Cyber Claims (U.S.)



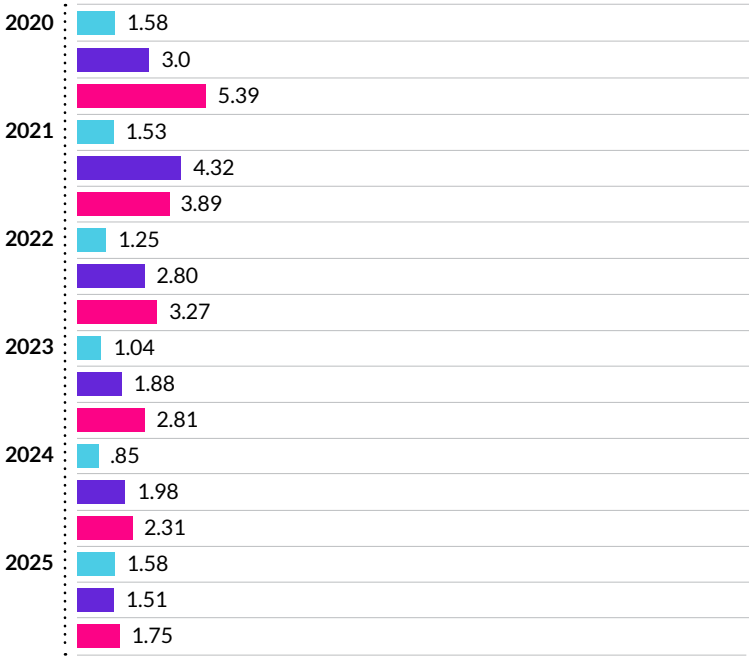
SME: $0-$99M revenue
Middle Market: $100M-$999M revenue
Large: $1B+ revenue

Trends in Europe and the U.K. exhibit similarities and differences compared to the U.S.

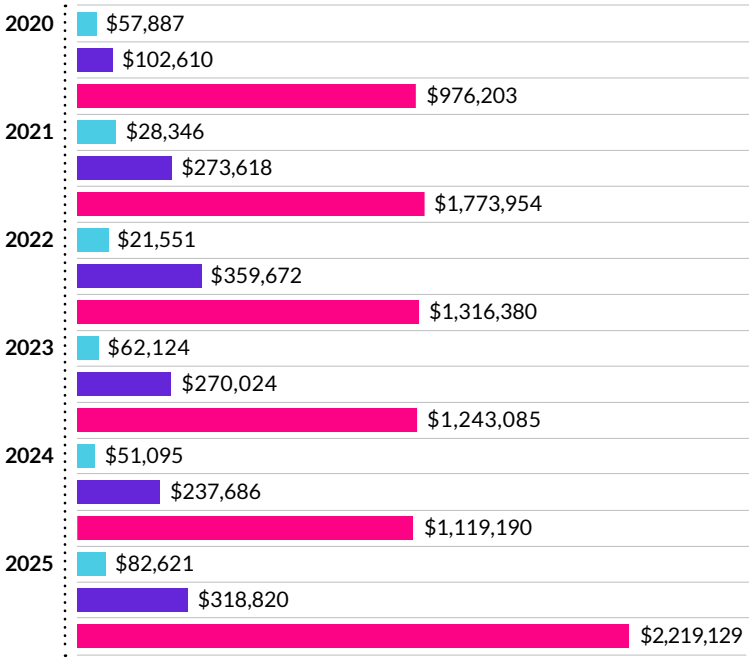
Levels of frequency are similar in the SME cohort, but much lower in the middle market and large account segments. This suggests that the propensity to be attacked and the general security profile and controls in place are similar across SMEs in the U.S., Europe, and the U.K. On the other hand, there is a clear reduction in exposure in the middle and large company segments in Europe and the U.K. versus the U.S. – driven largely by the absence of third-party litigation-related claims.

Severity is lower across all Europe and U.K. cohorts, also largely due to the absence of any material third-party litigation expenses from either data breach or non-data breach privacy claims. While severity is clearly increasing across all cohorts, it remains more stable than in the U.S.

Frequency of Cyber Claims per 100 Policies (Europe + U.K.)



Average Severity of Cyber Claims (Europe + U.K.)

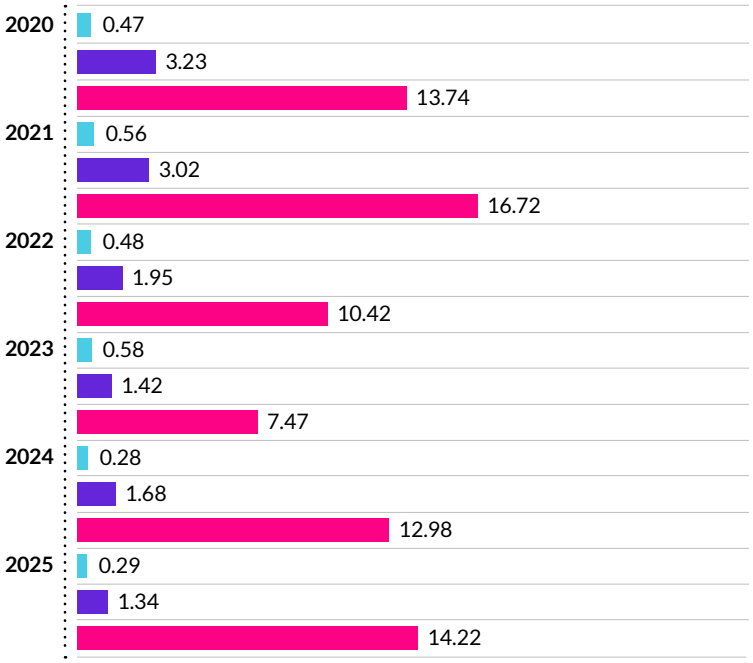


SME: $0-$10M revenue
Middle Market: $11M-$499M revenue
Large: $500M+ revenue

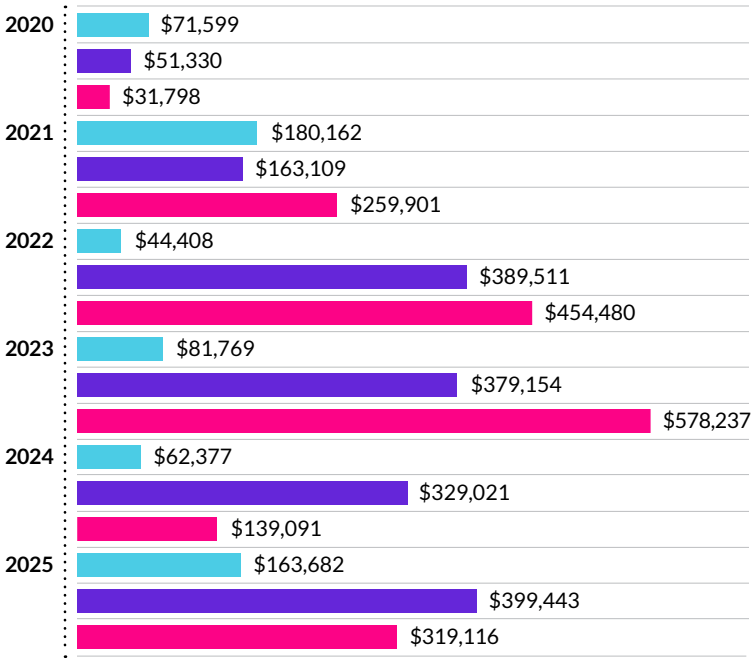
In Australia and New Zealand, absolute levels of frequency and severity and overall trends differ compared to other parts of the world but follow the same general trajectory.

Frequency dropped considerably while severity generally increased after 2021. SME frequency is a fraction of the levels in other parts of the world, yet severity is roughly in line. Middle market frequency is in line with Europe and the U.K. – and much lower than in the U.S. – reflecting the relatively benign legal environment for cyber data breach and non-data breach privacy actions. Also notable, the middle market and large company segments experienced lower severity levels with more modest increases over time.

Frequency of Cyber Claims per 100 Policies (Australia & New Zealand)



Average Severity of Cyber Claims (Australia & New Zealand)



SME: $0-$10M revenue
Middle Market: $11M-$499M revenue
Large: $500M+ revenue

Section Four

The AI Arms Race: Attack & Defend

Increased adoption and advancement of AI globally have driven increasingly sophisticated adversarial use of technology, as well as beneficial detection and remediation tools.



In November, for example, Anthropic – the company behind the AI tool Claude – reported that it had been the victim of "a highly sophisticated espionage campaign" by criminals who used AI's agentic capabilities to an unprecedented degree.

AI was used not just as an advisor, but to execute the cyberattacks themselves. The attack, which targeted large technology companies, financial institutions and government agencies, among other organizations, was, in Anthropic's estimation, "the first documented case of a large-scale cyberattack executed without substantial human intervention."

Other developments in the hostile use of agentic AI and autonomous malware include:



New strains that can rewrite themselves mid-execution to evade signature-based detection.



Autonomous reconnaissance swarms – "digital locusts" – that map entire corporate networks and launch targeted attacks after instantly identifying vulnerabilities.



AI that refines and optimizes hyper-realistic deepfakes to expertly mimic the voices of CFOs or other executives and trick employees into making unauthorized fund transfers.

Chubb's cyber insurance products address cyber incidents of all kinds including those related to AI. The effectiveness of market alternatives to express coverage – such as affirmative AI endorsements, sublimits or narrower coverages – should be carefully assessed by insureds and brokers.

In addition, less complex AI-related incidents continue, such as an employee mistakenly uploading Personally Identifiable Information (PII) into a publicly accessible LLM, leading to a cyber incident.

On the defensive side, businesses and organizations can institute proven, AI-focused risk mitigation tools to respond to these threats and reduce their risk.

These include:

AI-First Defenses: Adopting AI-driven security operations (AISO) for real-time threat detection.

AI Governance: Maintaining a strict inventory of all AI systems and auditing third-party data-handling practices.

Enhanced training: Educating employees about AI-driven security risks, such as advanced phishing and deepfakes.



Section Five

The Impact of Social Engineering Fraud

Social engineering fraud claims can be severe – especially for small and mid-sized businesses. The potential for financial losses, operational disruption, and reputational harm highlight a critical need for effective response and recovery strategies.



Social Engineering Fraud Cyber Incident



The Event: Acting on an email that appeared to be from a representative of a longtime machine supplier, a new employee changes the banking details for the vendor's payment to a new bank, without first attempting to verify the email by calling the supplier at their office.



The Impact: The company later realizes the employee fell victim to social engineering fraud when the supplier's actual employee followed up for payment, only to learn that the email was fraudulent and the payment had been made to an imposter.

$100,000

The Solution: Loss of more than $100,000. No recovery from the bank or the supplier.



The Outcome: Cyber policy, with an endorsement for cybercrime, reimburses the policyholder for the unrecoverable losses.

Section Six

The Privacy Frontier & Litigation-First Reflex

As cyber incidents increasingly become legal events, companies are grappling with new legal challenges posed by novel theories of liability – particularly regarding wiretapping and digital tracking technologies.



Major factors affecting legal liability include:



The "Litigation-First" Reflex: Plaintiff attorneys are leveraging decades-old wiretapping statutes (such as the **California Invasion of Privacy Act**) and video privacy laws (such as the federal **Video Protection Privacy Act**) to target standard web technologies, including the tracking of pixels.



Mass Arbitration: Companies are being forced to pay substantial upfront administrative fees for each individual filing. In a suit involving 10,000 claimants, for example, these non-refundable fees can exceed $10 million before the merits of the case are even heard.



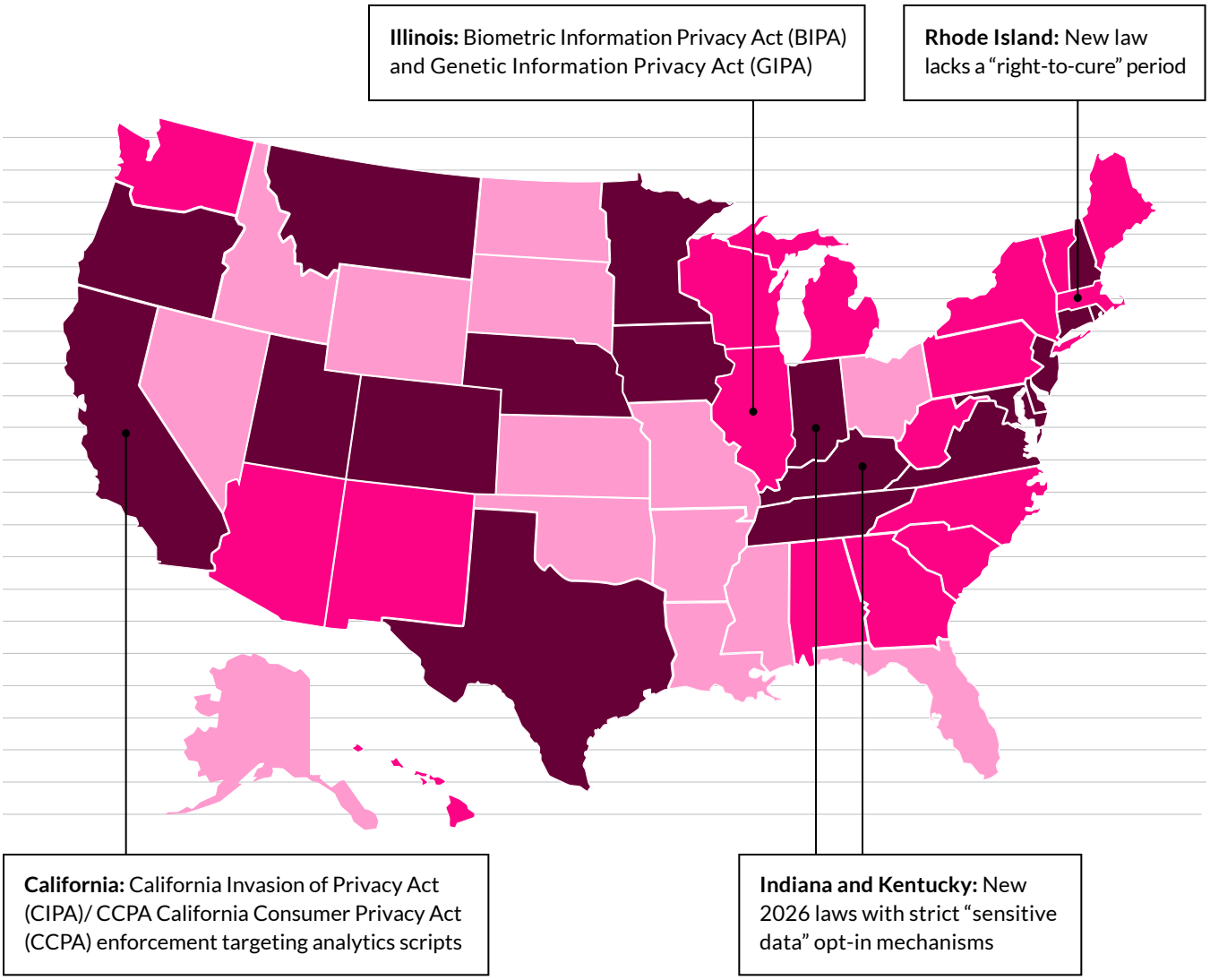
Data Suppression: Attackers are moving toward intentionally deleting or leaking data rather than just encrypting it – creating a permanent "loss of control" – which can increase the stakes in litigation.

A growing body of privacy laws in the U.S. and the EU are imposing complex, layered obligations for companies that store and/or transfer personal data. These include the right to opt out of profiling or automated decision-making, disclosure requirements for AI-driven processing, and mandated risk assessments for high-risk use cases.

United States

Privacy Legislation Tracker

There is no federal legislation, but rather a patchwork of regulation by state.



Statute/bill in legislative process:

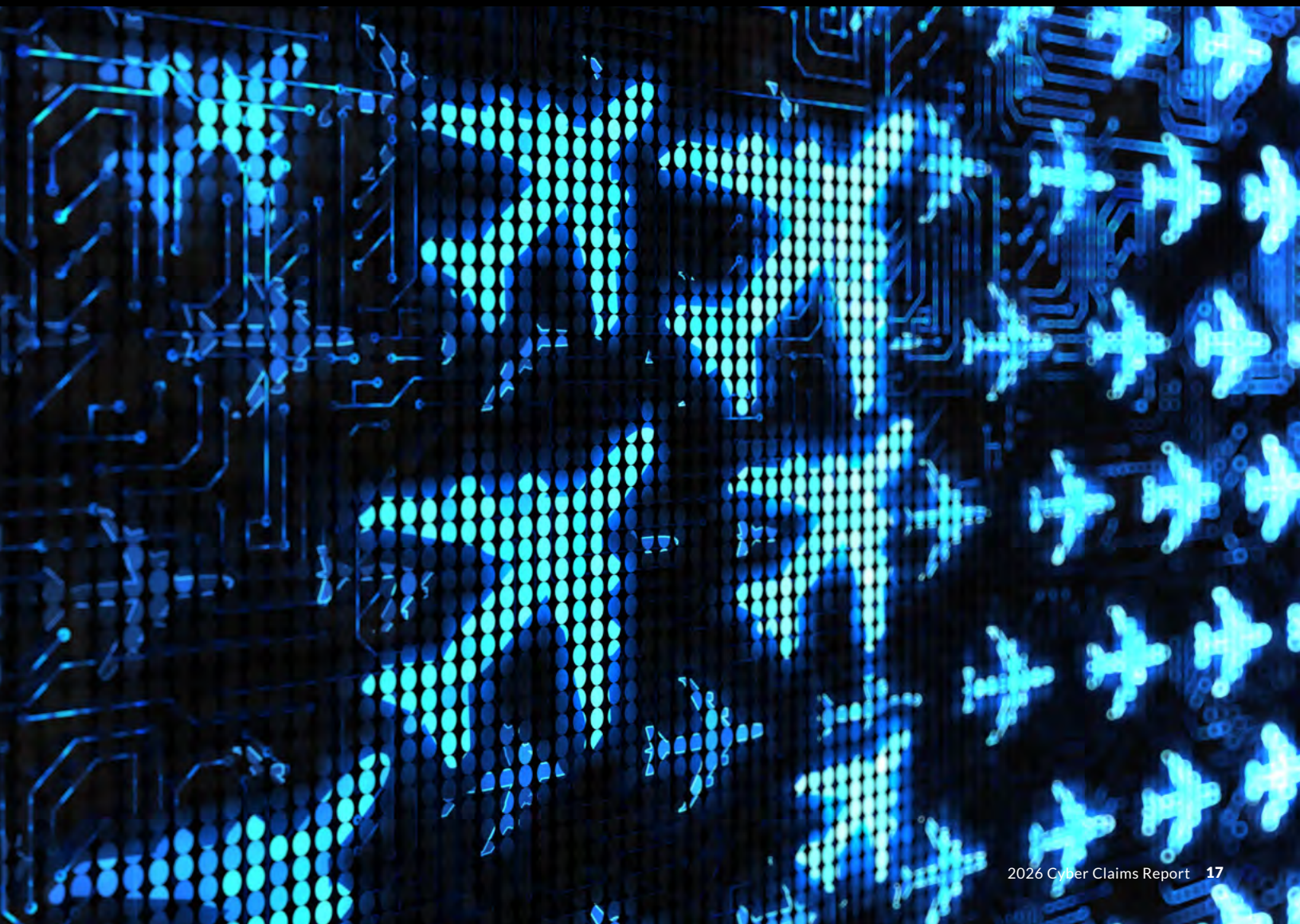
Passed legislation **Pending legislation** **No legislation**

Source: *US Federal Privacy Legislation Tracker*

Section Seven

Safeguarding Sensitive Data

Privacy incidents are an escalating source of both frequent and severe cyber claims. With evolving regulations and the rise of large-scale litigation, managing privacy risk has become more complex and costly. Every organization may face distinct challenges in safeguarding data in a constantly evolving threat landscape.



Middle Market Privacy Incident



The Event: The insured operates a subscription-based website and mobile application which uses tracking technologies, including cookies and pixels. The pixel tracks certain data, including the user ID of the website user, and transmits that data to third parties.



The Impact: Multiple law firms issued thousands of pre-arbitration demands alleging the use of the pixel violated the California Invasion of Privacy Act, which prohibits the interception of communications without consent.

$40M+

The Problem: The insured's privacy policy required all disputes to be resolved via arbitration. The rules of the arbitration forum, however, would have required the insured to pay several million dollars in initial filing fees before even considering the merits of the demands. Thus, if the claims were arbitrated it could have resulted in a potential statutory damages award plus arbitration fees of more than $40 million.



The Solution: Chubb retained counsel experienced in privacy litigation and the plaintiff law firms, which led to mediation of the dispute.

$6.5M

The Outcome: The multiple claims were resolved globally in the range of $6.5 million.

Managing consumer privacy risks and ensuring regulatory compliance is essential. To support our insureds, Chubb has partnered with privacy risk management platforms that enable insureds to protect their organizations by assessing and pro-actively managing privacy risks, safeguarding sensitive data, and maintaining compliance.

Section Eight

The Effect of Ransomware on Small Medium-sized Enterprises

Ransomware attacks continue to pose significant risks for small and mid-sized enterprises (SME), often resulting in complex and costly data breaches. Even when initial encryption attempts are thwarted, the exfiltration of sensitive of information can trigger extensive notification requirements and remediation efforts.



SME Ransomware Incident



The Event: Attempts by a threat actor group to encrypt an insured's computer were significantly thwarted by the insured's endpoint detection and response tool. However, the threat actor was able to exfiltrate the health information and Social Security numbers of over 4 million people.



The Impact: The insured needed to quickly identify exactly what data and personal health information was compromised to comply with notification obligations mandated by applicable statutes and regulations.



The Problem: Understanding the extent of the data breach, ensuring prompt notification to those impacted, and ensuring that the potentially exploited unpatched vulnerabilities were remediated as quickly as possible.

$4M

The Solution: Legal counsel, a forensic team and a data mining team were immediately retained to assist the insured in responding to this event. Following their detailed review of the impacted data, 4 million individuals and numerous regulators were notified of the event. Chubb's Risk Advisor team was also engaged to help the client address its unpatched vulnerabilities.

$4.7M

The Outcome: The total cost reimbursed to the insured was $4.7 million, including notification costs of $2.4 million and $1.2 million in credit monitoring costs for victims. The insured was also notified of its unpatched vulnerabilities and assisted with remediation.

Chubb has considerable experience with ransomware claims and provides highly regarded legal, IT forensic, public relations, and other specialized services to help our insureds respond and smoothly navigate ransomware incidents: repairing or replacing damaged systems, minimizing downtime, and returning to business.

Section Nine

Ransomware Without Borders

Ransomware attacks continue to pose serious risks for organizations worldwide. Even institutions with advanced cybersecurity measures can face widespread disruption when threat actors exfiltrate sensitive data and publish it publicly. The consequences often extend across jurisdictions, triggering regulatory scrutiny, legal obligations, and operational challenges.



As this incident in Europe illustrates, ransomware knows no geographic boundaries.

Global Ransomware Incident



The Event: A ransomware attack by a then unknown threat actor group hit a global academic institution and its publishing arm. Over 575,000 sensitive documents were exfiltrated and later published on the group's leak site.



The Impact: Operations were disrupted globally. Sensitive data, including author earnings, government research, and future exam papers, was exposed across more than 40 countries. Recovery was especially challenging in regions with complex IT dependencies.



The Problem: The academic institution had to assess all 575,000 leaked documents for regulatory risk. Legal advice was required across 40 jurisdictions, significantly increasing complexity and pressure to meet global compliance requirements.



The Solution: Chubb deployed legal and forensic experts, and advanced data mining identified high-risk content, enabling a rapid, largely automated review. Coordinated legal input across continents ensured precise, timely regulatory notifications.

$14.2M

The Outcome: The loss totaled $14.2 million, including cyber incident response expenses and business interruption loss. Thanks to swift action and coordinated legal support, the academic institution avoided fines, regulatory investigations, or sanctions. Despite the breach's scale, reputational and regulatory impacts were successfully contained.

Section Ten

Widespread Events: The Rippling Costs of Interdependence

No business operates in isolation: they rely on partners, suppliers, and clients. Two noteworthy cyberattacks from 2025 illustrate just how damage from a ransomware encounter can affect multiple businesses up and down a company's supply chain. While Chubb was sounding the alarm on this issue in 2022, the severity of these types of events is now coming into greater focus across the cyber universe.



United Kingdom – August 2025

Jaguar Land Rover

The late August 2025 attack on Jaguar Land Rover (JLR) is the most damaging cyber incident in British history. Details of the event are a cautionary tale with important lessons for all companies.



The Incident

Attributed to "Scattered Lapsus Hunters," the attack forced JLR to deactivate its global IT networks to contain the breach.



The Operational Impact

Manufacturing was halted for five weeks across sites in the U.K., Slovakia, Brazil, and China. Paralyzed systems included production line controls, CAD/PLM design equipment, and dealer ordering platforms.



The Security and Legal Fallout:

Hackers exfiltrated payroll data and customer records for up to 7.4 million individuals, resulting in extensive litigation.

The Systemic Financial Fallout

£1.9B

Economic

The U.K. economy suffered an estimated £1.9 billion ($2.5 billion) loss, contributing to a Q3 2025 GDP slowdown.

£1.2B

Supply Chain Impact

Over 5,000 U.K. organizations were affected; the government intervened with £1.2 billion in emergency loans to stabilize the chain.

£485M

Company Loss

JLR reported a £485 million pre-tax loss, reversing a £398 million profit from the previous year.

United States – February 2025

Oracle Health Data Breach

In early 2025, Oracle Health (formerly Cerner) experienced a major data breach that analysts have deemed one of the most massive in the history of the U.S. healthcare industry.



The Incident

Attackers used stolen credentials to access legacy Cerner data migration servers not yet moved to Oracle Cloud.



The Key Vulnerability

The breach targeted a legacy environment – parts of which had not been used since 2017 – demonstrating that "forgotten" data is a prime target.



The Impact

The attack seized records from approximately 80 hospitals, exposing the Social Security numbers of patients as well as their medical histories, including diagnoses and treatment images.



The Extortion Factor

A threat actor operating under the alias Andrew demanded millions in cryptocurrency to prevent the release of the stolen files.

These and other events from 2025 – including many stemming from errors or accidents as opposed to malfeasance (e.g., the October Amazon Web Services outage) – underscore the need to identify and institute the most stringent cyber risk mitigation protections available.

SME Vendor Incident



The Event: The insured retailer contracted with a third-party technology provider for the software needed for day-to-day operations. When the technology provider was the target of a ransomware attack, all of its systems went offline.



The Impact: Unable to use the software, the insured could not conduct sales of certain products, order inventory, or schedule client appointments.



The Solution: Chubb retained a forensic accountant to assist the insured in calculating the resulting contingent business interruption loss. The insured's preparation with its incident response plan and integration with Chubb claims helped manage an event that was largely outside the insured's control.

$1.2M

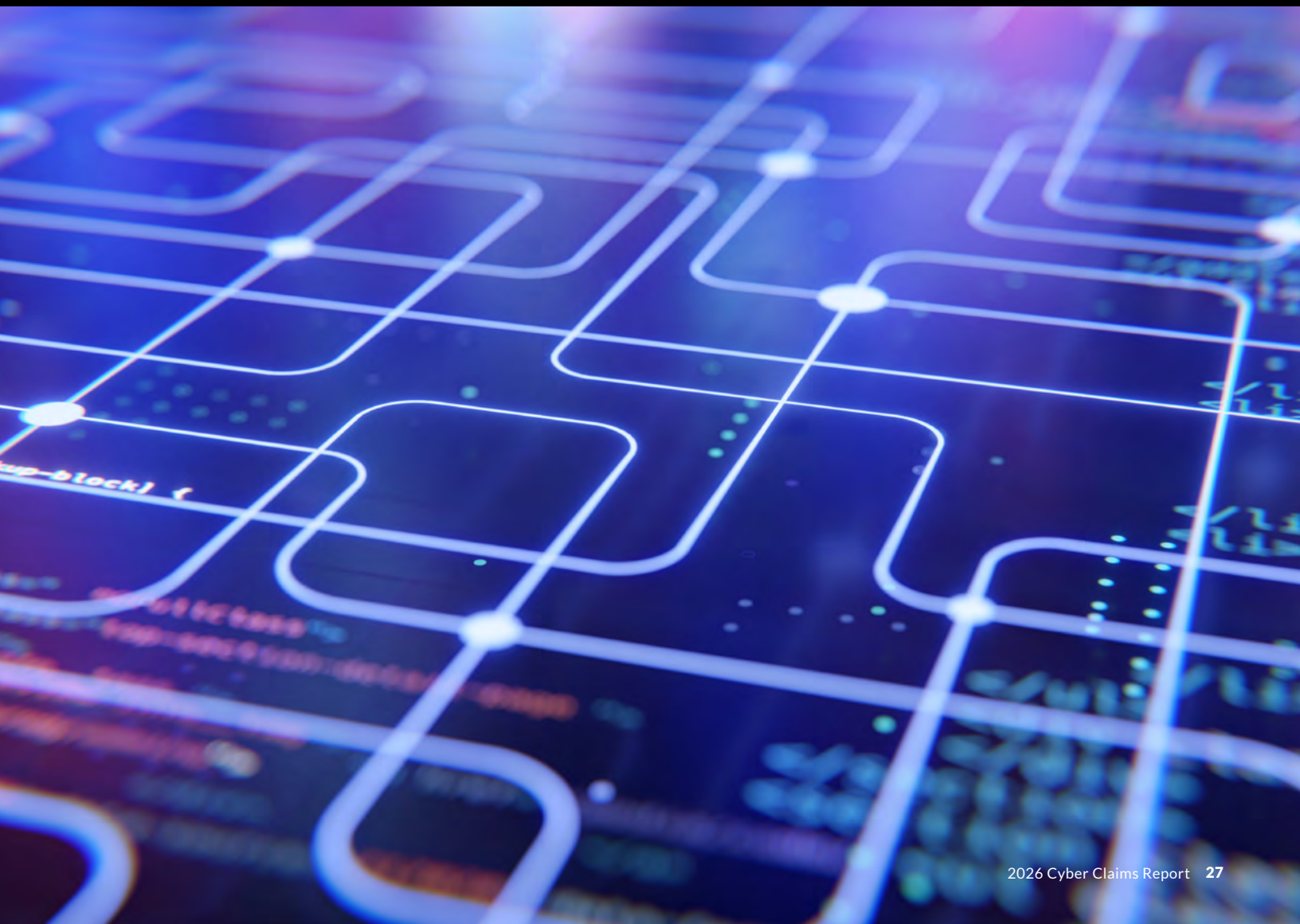
The Outcome: The loss totaled $1.2 million.

While these scenarios may seem distant to small businesses, Chubb's experience demonstrates this is far from reality.

Section Eleven

Chubb: Empowering Companies with Insights to Mitigate Cyber Risk

In addition to risk mitigation tools, knowledge is one of the best defenses against evolving cyber threats. Chubb provides insureds with a range of insights to support cyber incident prevention and mitigation.



The Chubb Cyber Index

The Chubb Cyber Index, launched in 2015, provides real-time access to Chubb's global proprietary claims data and insights into current cyber threats, trends and costs.

The searchable platform allows users to set parameters and view historical trends based on:



Incident Activity: Breaking down cyber threat trends impacting organizations - by size, industry, and geographic region.



Claim Costs: Breaking down Chubb cyber claims costs by organization size and industry.



Cyber Risk Calculator: A tool that provides insights into the broader spectrum of cyber exposures and potential cyber loss costs.

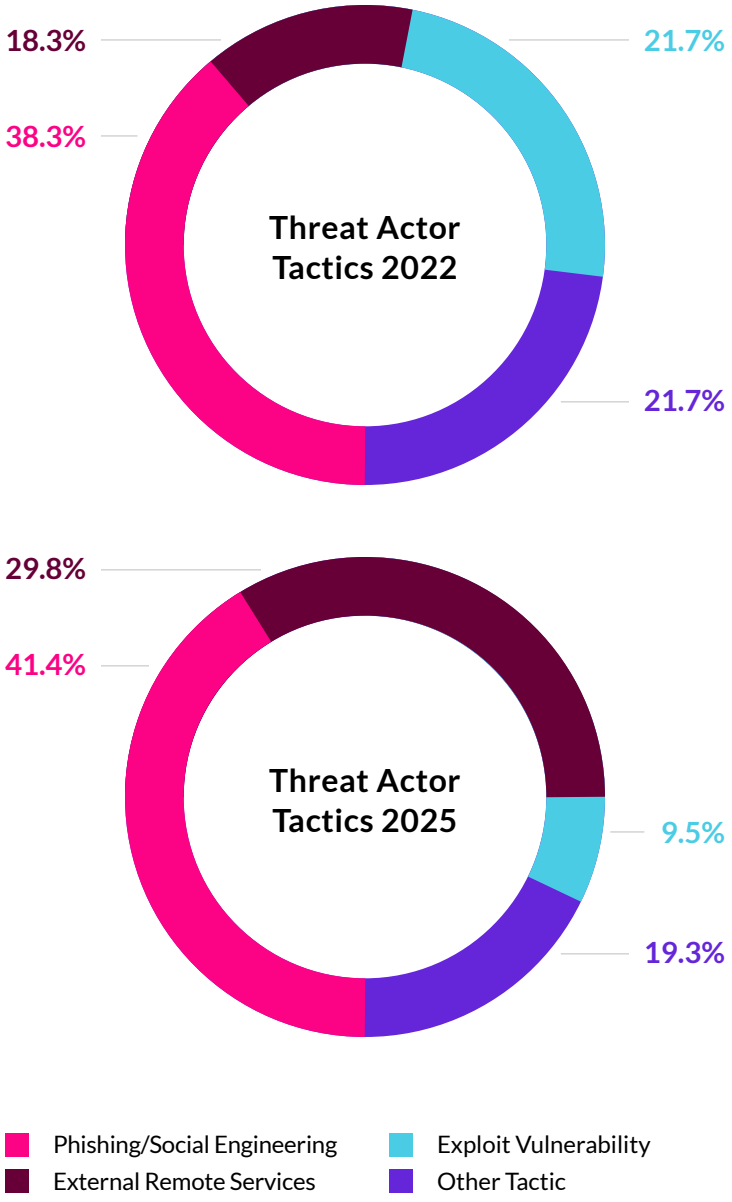


Peer Purchasing Insights: Enabling companies to benchmark their own cyber protection versus those of similar organizations.

Chubb Threat Intelligence

In addition to our Cyber Claims Report, Chubb issues a quarterly Threat Intelligence Report to provide cyber professionals with concise, actionable insights on the latest developments in cyber threats and Chubb's claims experience.

A recent report showed that the most common initial access tactic resulting in a ransomware incident in 2025 was phishing. External remote service exploitation (e.g., VPN abuse, open ports) was second, while severe vulnerability exploits ranked third.



Compared to 2022, the proportion of claims emanating from severe vulnerability exploits declined from nearly 22% to 9% – corresponding with Chubb's launch of its Vulnerability Management Outreach Program, whereby our Cyber Threat Intelligence team prioritizes the most severe exploitable vulnerabilities and provides targeted alerts to only those policyholders potentially affected by these vulnerabilities. Chubb's Threat Intelligence team prioritizes only the most severe exploitable vulnerabilities and provides targeted alerts to only those policyholders potentially affected by these vulnerabilities. This service is offered on a complimentary basis to all Chubb Cyber policyholders.

Through our Vulnerability Management Outreach Program, Chubb continuously scans our portfolio and notifies brokers and policyholders of severe, exploitable issues in need of patching, either at renewal or during the policy period. This service is offered on a complimentary basis to all Chubb Cyber policyholders.

In addition to our Vulnerability Management Outreach Program, Chubb offers phishing-focused services specifically to help insureds mitigate exposure to phishing attacks, including:

Training

Security awareness and phishing prevention courses and games for employees, based on the latest threats.

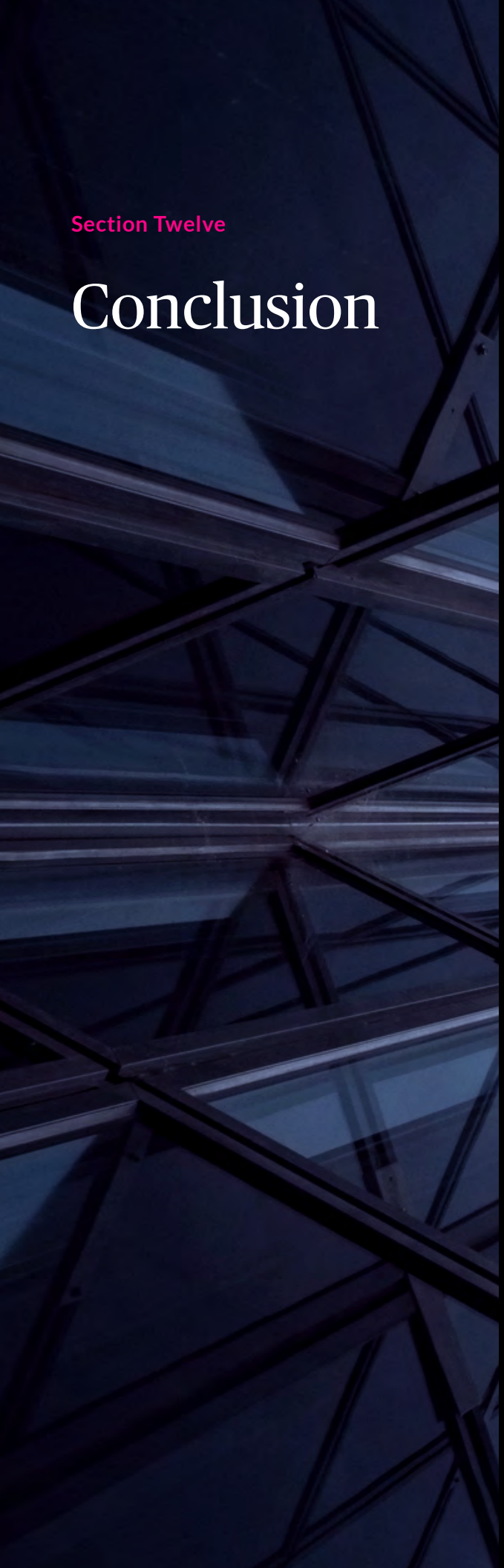
Testing

Phishing email simulations, including deepfake technology simulations, to test employee decision-making.

Technology

An AI-enabled email security tool to help spot phishing intent, language, and behavioral anomalies a human is likely to miss.





Section Twelve

Conclusion

Resilience in an Age of Acceleration

Cyber risk in 2025 was defined by acceleration. Autonomous AI attacks, expanded privacy regulations, and mass arbitration tactics are among the factors compressing timelines and amplifying the potential consequences of cyber incidents.

Investing in advanced detection capabilities, strengthening governance over AI and data practices, and stress-testing third party ecosystems are among the many ways organizations can materially reduce their vulnerability.

As we have been for decades, Chubb is here to help. Our global cyber experience, deep claims data and integrated risk mitigation and response capabilities empower our clients to anticipate, withstand and recover from today's complex cyber events – and prepare for what's coming next. We look forward to continuing our work with clients worldwide, building financial and operational resilience against cyber risk.

To learn more, visit
Chubb Cyber Insurance

CHUBB®

Count on Chubb for comprehensive cyber protection and resilience.

The information contained in this document is intended for general informational purposes only and is not intended to provide legal or other expert advice. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Neither Chubb nor its employees or agents shall be liable for the use of any information or statements made or contained in any information provided herein. This document contains links to third-party Web sites solely for informational purposes and as a convenience to readers and not as an endorsement by Chubb of the entities referenced or the contents on such third-party Web sites. Chubb is not responsible for the content of linked third-party sites and does not make any representations regarding the content or accuracy of materials on such linked Web sites. Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services.