Navigating the Cyber Claims Landscape

KEY INSIGHTS FROM
CHUBB'S GLOBAL
CYBER RISK TEAM

CHUBB®

Table of Contents

6

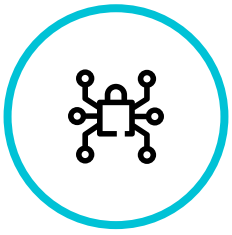
Frequency and Severity of Cyber Incidents

11

The Ransomware Dilemma: To Pay or Not to Pay?

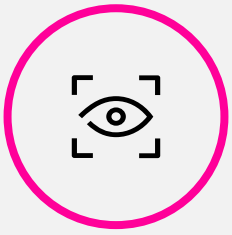
17

The Primacy of Privacy



20

Controls Matter: Adopting a Zero Trust Approach to Cybersecurity



22

Chubb's Cyber Index: Empowering Companies With Data-Driven Insights

24

Helping Businesses Become More Secure

At Chubb, we have 25 years of history providing robust cyber insurance solutions, reinforced by a wealth of historical claims data and underwriting acumen all geared toward optimal risk selection.

Now, in the first edition of the Chubb Cyber Claims Report, we explore Chubb's historical claims data through December 2024 to reveal insights on frequency and severity trends, ransomware incidents and privacy claims in order to help businesses navigate the complexities of today's cyber risk environment.

1999 Chubb begins offering cyber insurance solutions.

2014 Chubb debuts our **Loss Mitigation Services** suite of products, the first of its kind.

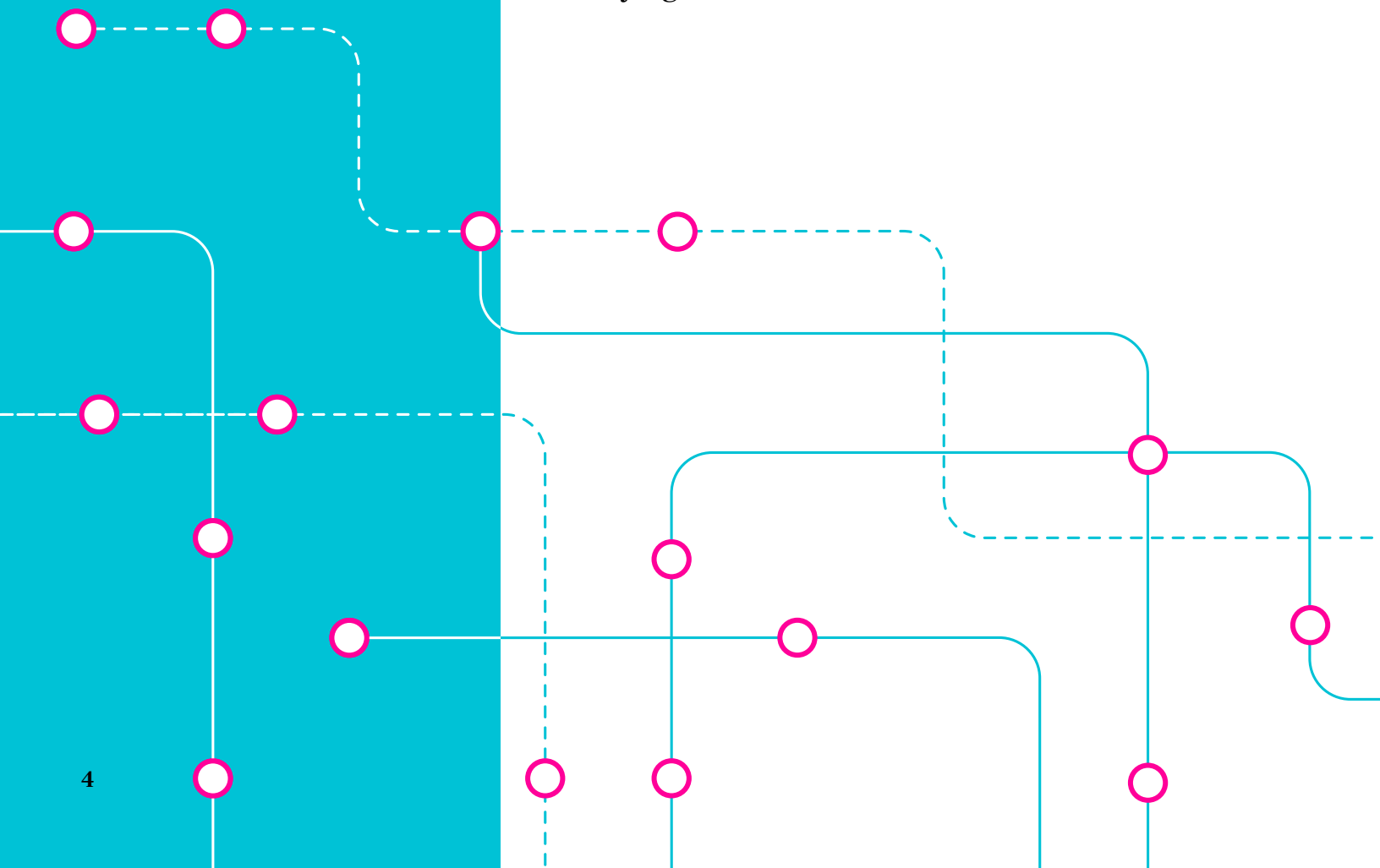
2018 Chubb introduces the market's first claim index, **Chubb's Cyber Index**, accompanied by our quarterly "**Cyber InFocus" newsletters**.

2025 Chubb launches the first edition of the Chubb Cyber Claims Report.

The claims- and loss-related data contained in this report are proprietary and based solely on Chubb claims, except as otherwise stated.

Over the past 24 months, both the frequency and severity of cyber claims have increased, even as the businesses we insure have become more secure.

While ransomware incidents have driven severity, several widespread events have contributed to the increase in frequency in 2024. In addition, privacy liability has become a more prominent driver of claims activity, due in part to recent court decisions and novel legal theories of liability that are being advanced. These trends have impacted clients of different sizes, industries and geographies in varying measures.



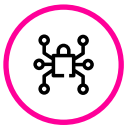
Chubb's experience writing cyber insurance for more than two decades has generated insights that are borne out by our own internal cyber claims data, providing a valuable snapshot of today's global cyber risk claims environment.

Here are some key takeaways:

The frequency and severity of cyber claims in the U.S. continue to grow – most dramatically for larger clients with over $1 billion in revenues. Outside the U.S., however, frequency and severity are declining.

Ransomware encounters remain the main driver of cyber insurance claims and loss severity. As threat actors become more sophisticated, companies of all sizes must be prepared to grapple with the difficult question of whether to pay a ransom and bear the operational consequences of this decision.

Privacy-related liability is becoming more complex as lawmakers around the globe pass or amend laws regulating the collection, sharing and use of biometric data and other personal information. Companies and organizations must stay up to date on how these regulations will affect them and ensure adherence to regulations based on their operations.

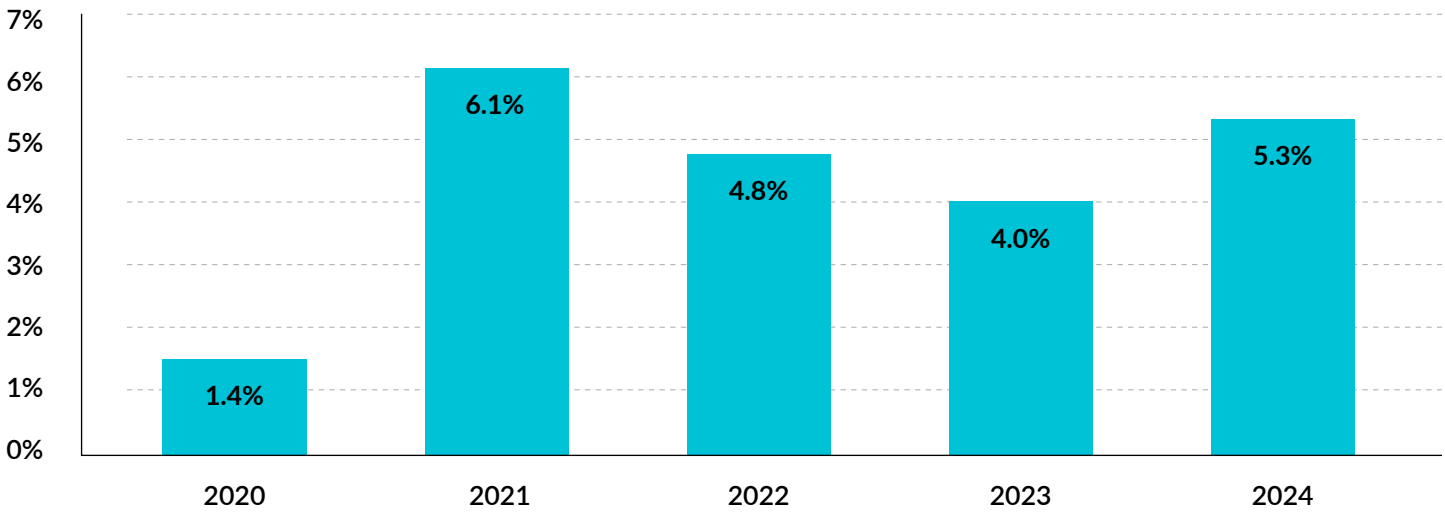


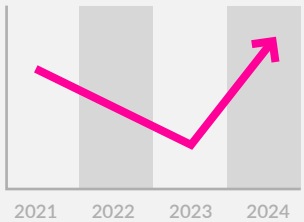
One of the best ways for organizations to arm themselves against a debilitating cyber incident is to adopt a strategy that combines a zero-trust security model with raised risk awareness among leaders and employees.

Frequency and Severity of Cyber Incidents

Few insurers have the global reach and diversity of business across all client sizes and industries that would allow them to identify credible claims trends at a granular level. Security controls and resilience capabilities of clients have helped mitigate the impact of cyber threats, but widespread cyber events – which can be rooted in attacks, as well as software malfunction or human error – cause significant economic and operational disruption and are becoming more frequent.

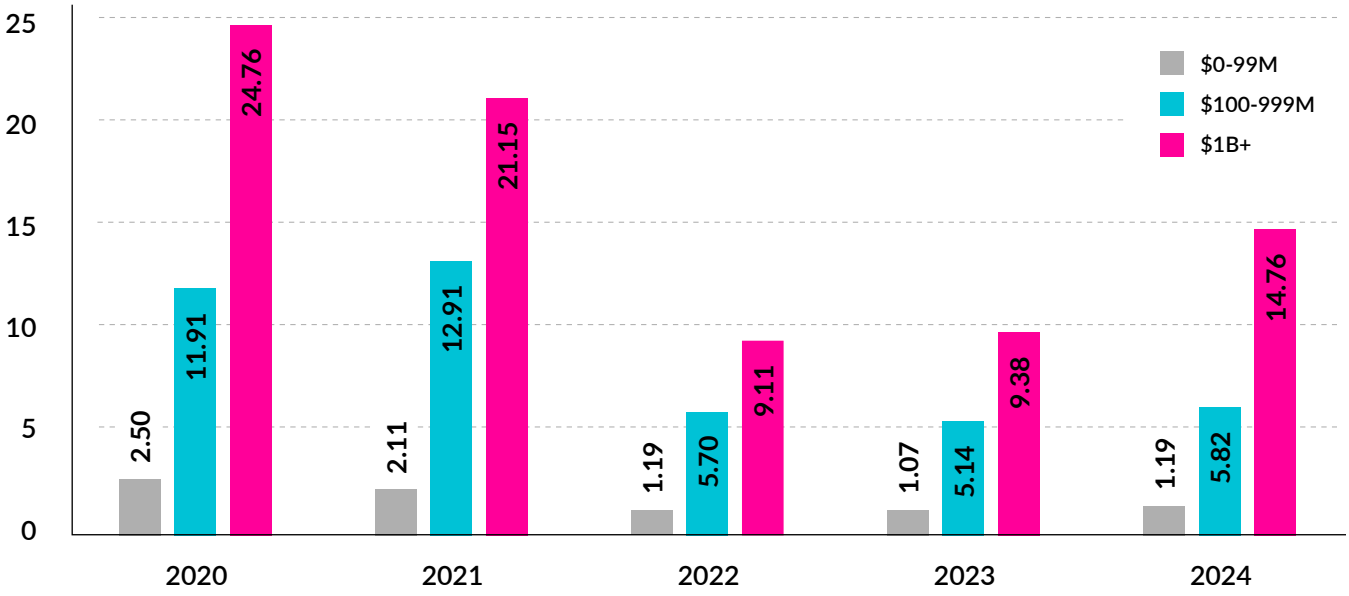
Percentage of Total Reported Cyber Claims in Calendar Year Due to Widespread Events





Our claims data tell the story: Despite falling from 2021 to 2023, the percentage of total reported claims from widespread events — which are single events that affect many companies at the same time — rose again in 2024 and continues to have an impact on overall frequency.

Frequency of Cyber Claims per 100 Cyber Policies Issued by Insured Revenue Band (U.S.)



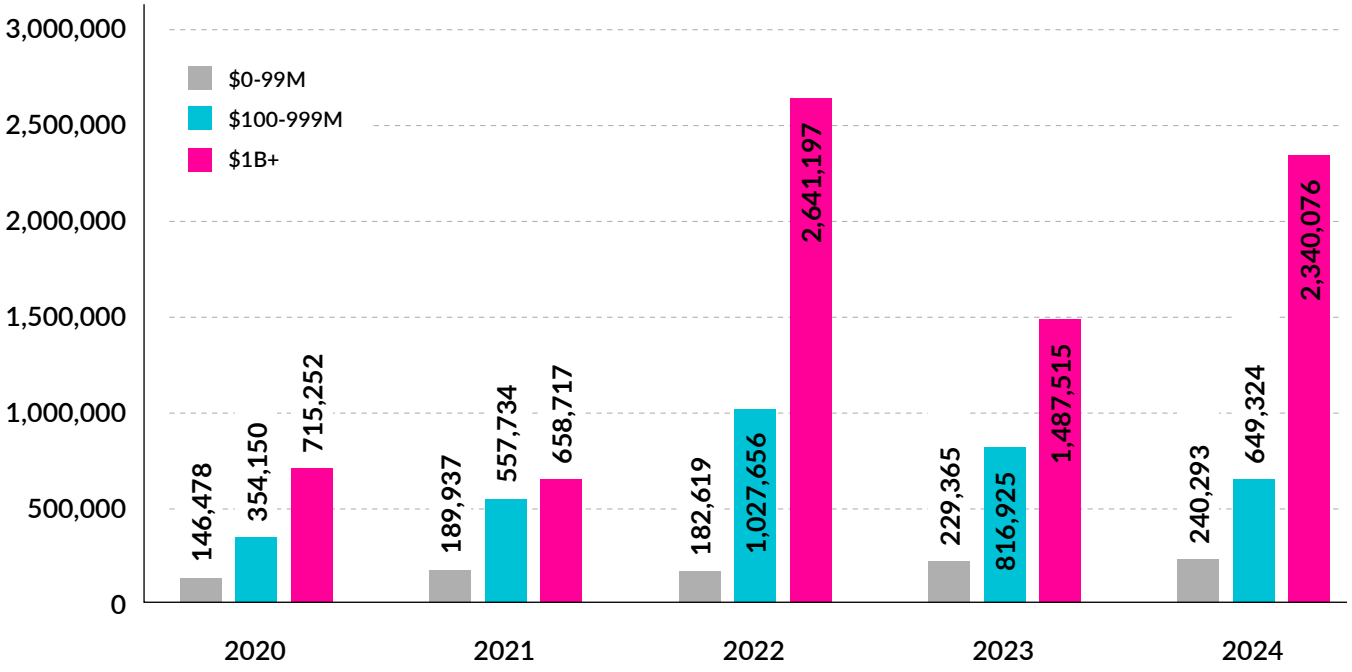
275%

Increase in Global Ransomware Attacks

Microsoft observed a 275% year-over-year increase in human-operated ransomware attacks between July 2023 and June 2024. This increase in ransomware attacks was partially offset by a sustained decrease in cyberattacks reaching the encryption stage, the report found.

Source: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

Severity of Cyber Claims by Insured Revenue Band (U.S.)



Cyber claim frequency for Chubb customers in the U.S. has increased over the past 3 years but remains lower than the peak of 2020-2021, while severity has increased from 2020 to 2024 with significant volatility in the past three years. Middle and large revenue accounts experienced a sharp increase in severity in 2022-2024, with several major companies incurring sizable claims that have been publicized widely in the media. While ransomware was ultimately a significant driver of this severity, it is notable that malicious actors have begun to employ new tactics. Some of the largest attacks were not caused by sophisticated malware that managed to evade the cybersecurity defenses of these highly controlled business, but were rather **social engineering attacks**[1] involving the manipulation of insured **IT help desks**[2] and **SIM swaps**.[3]

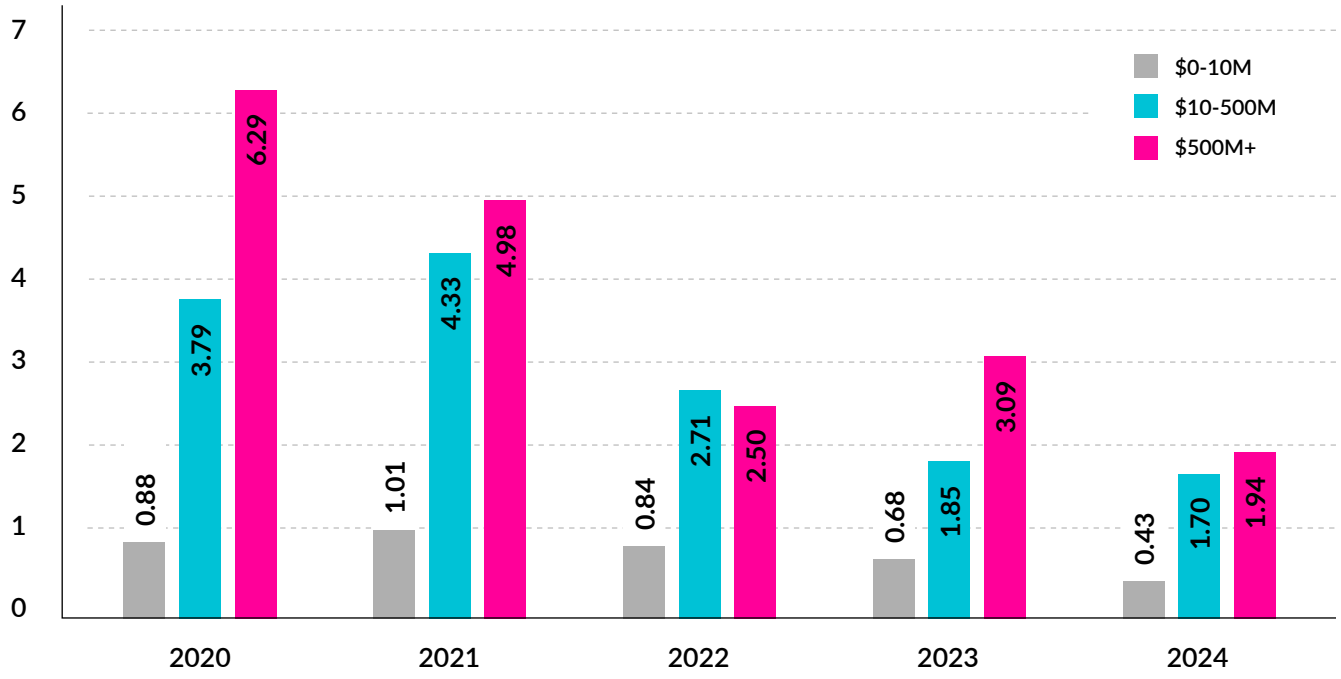
Currently, a larger share of subsequent third-party liability cyber claims in the U.S. – across all size risks – is related to ransomware incidents and privacy-related litigation than was the case in prior years.

1. Source: https://www.ibm.com/think/topics/social-engineering#:~:text=Social%20engineering%20attacks%20manipulate%20people,their%20personal%20or%20organizational%20security.
2. Source: https://www.obsidiansecurity.com/blog/understanding-social-engineering-attacks-on-helpdesk-agents/#:~:text=This%20technique%20typically%20begins%20with,to%20ensure%20their%20own%20persistence.
3. Source: https://www.incognia.com/the-authentication-reference/what-is-sim-swap-attack-and-why-fast-detection-is-important#:~:text=A%20SIM%20swap%20attack%20combines,to%20the%20fraudster's%20SIM%20Card.

By contrast, both frequency and severity outside of the U.S. have decreased among companies of all sizes.

Like their U.S. counterparts, Chubb's clients outside of the U.S. have invested in cybersecurity by increasing their awareness of cyber risk at the C-suite and board levels, building resilience in the form of improved **business continuity planning**[1] and the use of **incident response plans**,[2] and focusing on compliance with new regulatory structures (such as the EU's **Digital Operational Resilience Act**).[3] In addition, we have seen an increase in clients who are unwilling to pay ransoms. This combination of factors – alongside the fact that many of these countries are marked by less litigious business cultures – has driven these favorable trends for clients outside of the U.S.

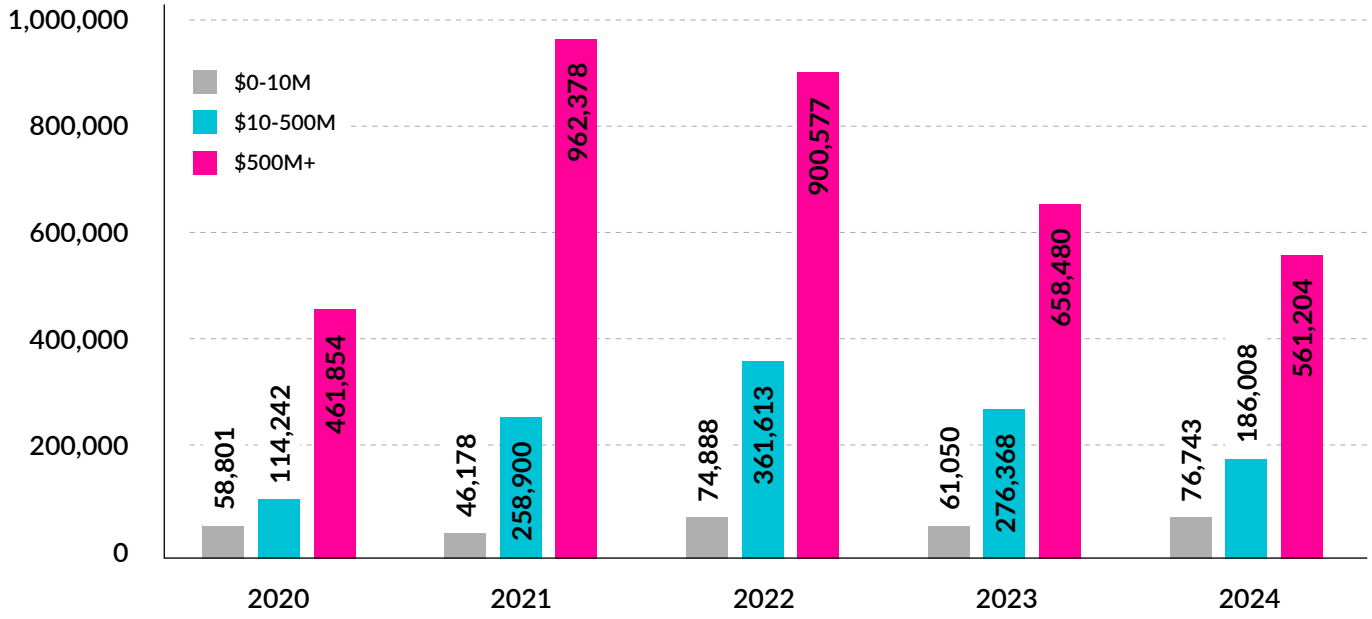
Frequency of Cyber Claims per 100 Cyber Policies Issued by Insured Revenue Band (Outside U.S.)



Frequency has declined across all sizes of insured.

1. Source: https://www.institutedata.com/us/blog/business-continuity-planning-in-cybersecurity/
2. Source: https://www.ibm.com/think/topics/incident-response
3. Source: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Severity of Cyber Claims by Insured Revenue Band (Outside U.S.)



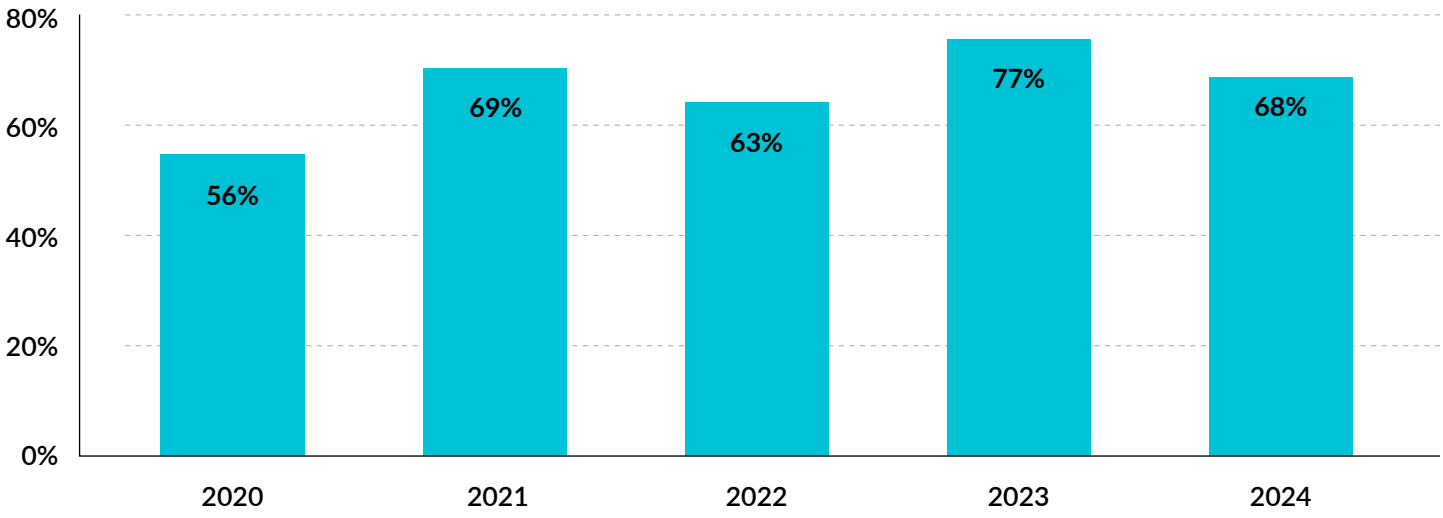
Severity has declined the past three years for medium and large revenue accounts, while small revenue accounts have experienced a modest increase in severity over the past few years.

The Ransomware Dilemma: To Pay or Not to Pay?

Ransomware encounters account for most incurred cyber losses globally, but clients react differently to an event depending on the strength of their resilience plan. Due to the inherent complexity and time sensitivity of ransomware claims, affected companies are confronted with the difficult decision of whether or not to pay a ransom. Threat actors recognize that these companies face a number of financial, ethical and legal issues; these actors may well use this stressful environment to their advantage, doubling down on their extortion efforts (demanding ransom both to restore systems and to prevent disclosure) or even tripling down on them (demanding additional ransom to prevent a threat to operations or to a third party). A company that pays a ransom might prevent further damage, but the costs associated with rebuilding its systems, recovering data and notifying customers may still be significant. Not paying a ransom, on the other hand, could subject a company to increased business interruption losses or additional legal liability. In an effort to stop ransomware activity, the U.S. Cybersecurity & Infrastructure Security Agency has convened a Joint Ransomware Task Force that has issued an informative guide, appropriately titled the **StopRansomware Guide**.

Source: https://www.cisa.gov/stopransomware/ransomware-guide

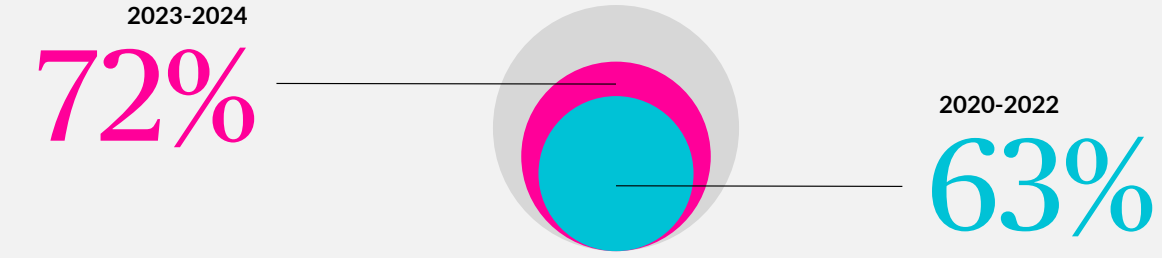
Percentage of Total Reported Cyber Losses in Calendar Year Due to Ransomware Incidents (U.S.)



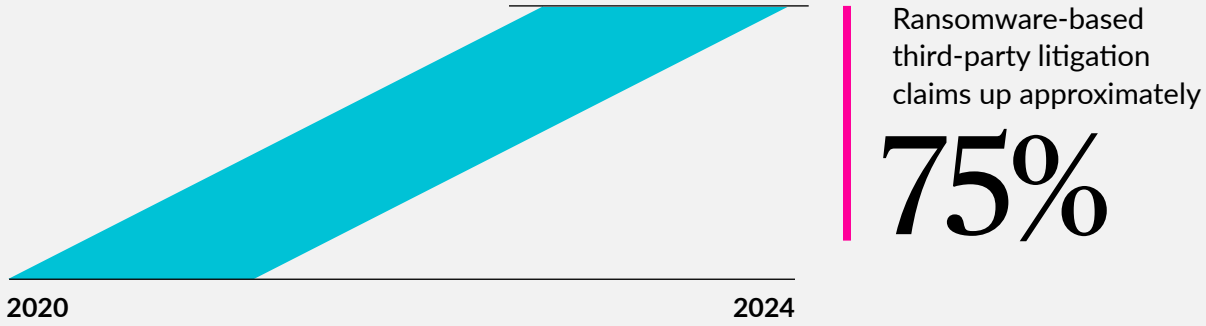
Ultimately, every company that finds itself in a ransomware situation must determine what is in its own best interests by considering multiple factors. **Resources are available**[1] for companies who are justifiably concerned about the risks they may encounter and who seek to **maximize their defense strategies**[2] in the face of attackers.

1. Source: https://securityandtechnology.org/ransomwaretaskforce/
2. Source: https://securityandtechnology.org/blog/prepare-dont-pay-a-quick-start-guide-to-defending-against-ransomware/

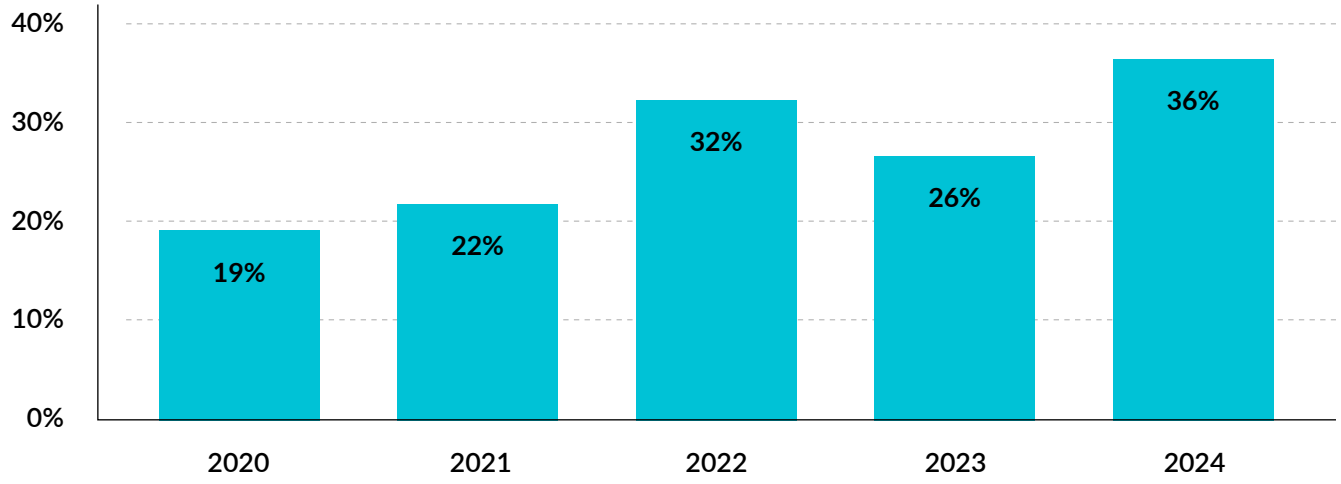
Ransomware-related losses in 2023 and 2024 accounted for nearly 72% of cyber claim dollars, compared to an average of 63% between 2020 and 2022.



Ransomware-related incidents should not be thought of as merely a disruption event for clients. Compromised data, whether stolen or inappropriately disseminated, can often lead to a lawsuit or class action, even when a client has conscientiously deployed security controls. The frequency of subsequent third-party litigation from ransomware incidents in 2024 is up approximately 75% over the 2020-2021 average.

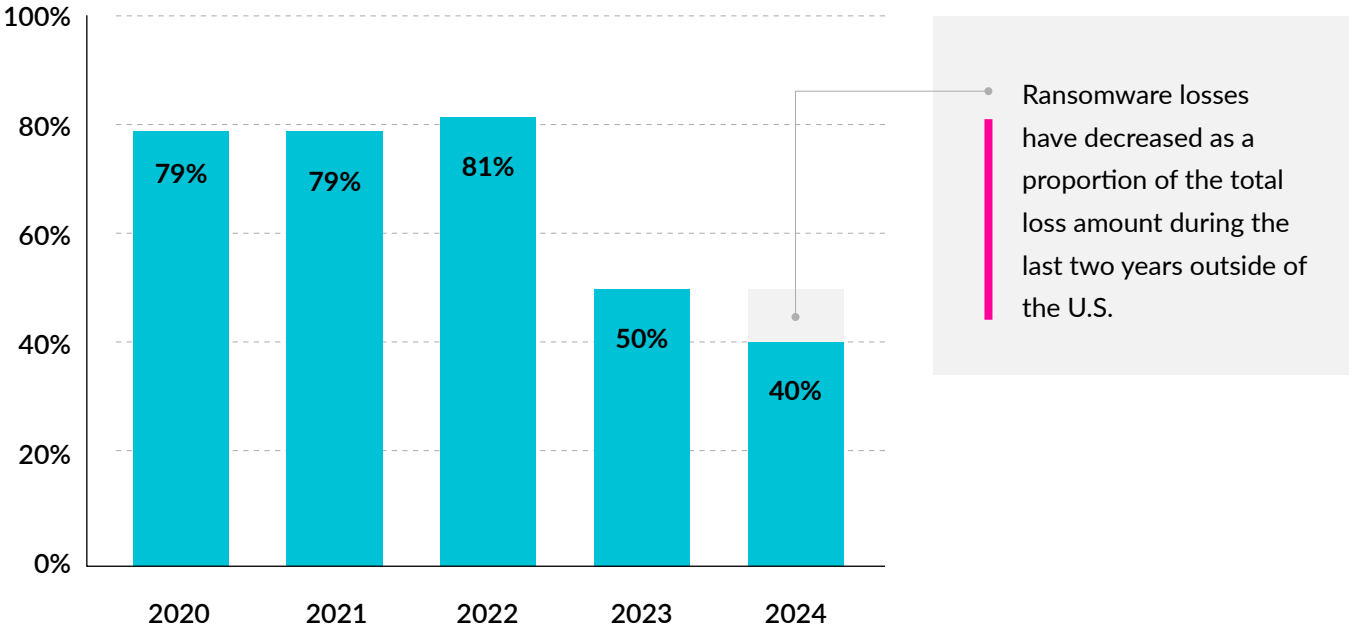


Proportion of Third-Party Cyber Claims Triggered by a Ransomware Encounter (U.S.)

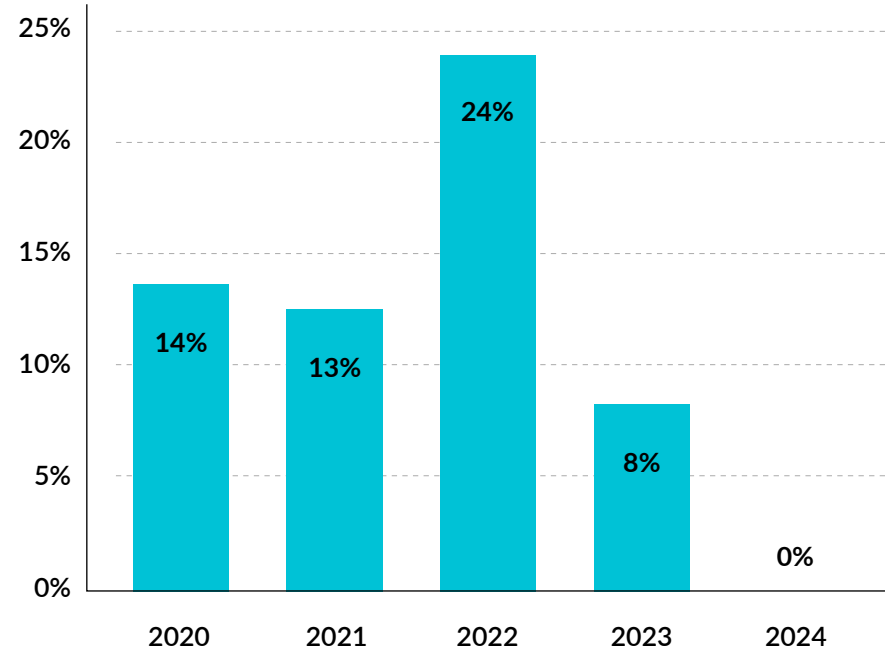


Outside of the U.S., however, the trends are different. Both the proportion of ransomware-related losses and the proportion of third-party claims related to ransomware incidents have declined over the past few years.

Percentage of Total Reported Cyber Losses in Calendar Year Due to Ransomware Incidents (Outside U.S.)

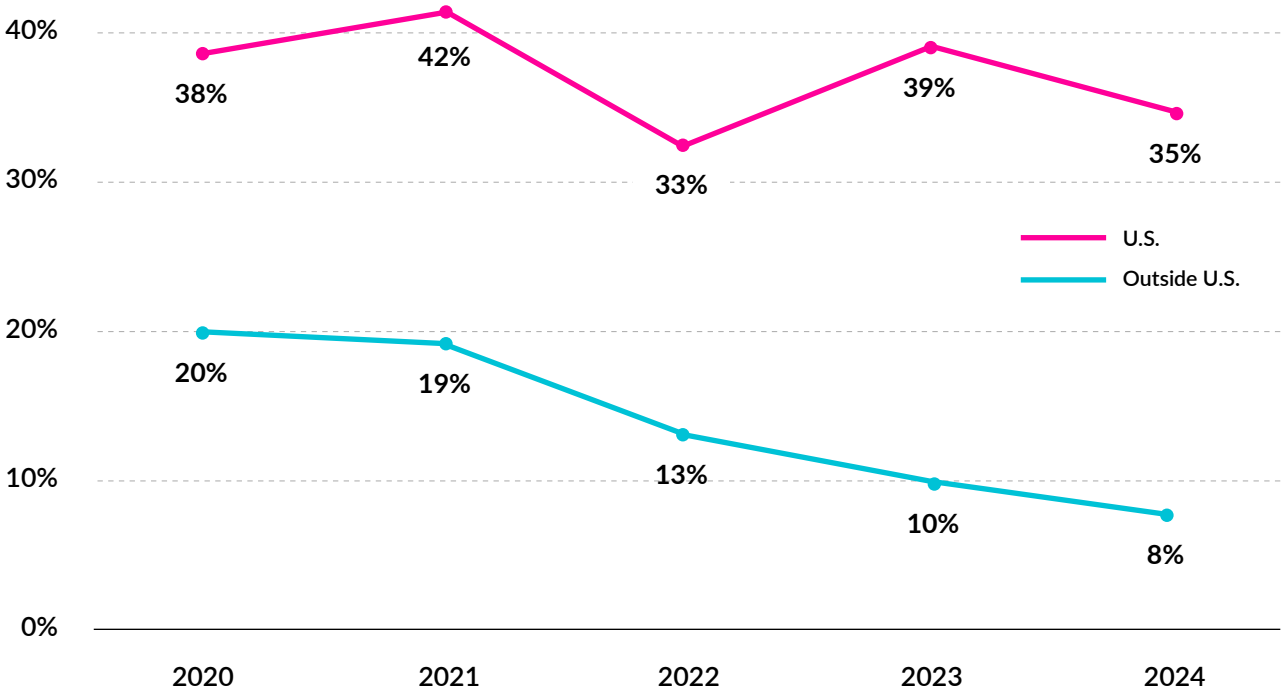


Proportion of Third-Party Cyber Claims Triggered by a Ransomware Encounter (Outside U.S.)



Our data indicate a noteworthy difference between policyholders in the U.S. and outside the U.S. with respect to the willingness to pay ransoms.

Pay to Encounter Rate



The pay to encounter rate in the U.S. is considerably higher than outside the U.S. and has remained so each of the last 5 years.

Why Policyholders May Consider Paying the Ransom

Economic Considerations

Sometimes the cost of paying the ransom is simply less than the potential financial losses that would result from downtime and data recovery efforts. This is a cold, hard calculation that many businesses are forced to make.

Lack of a Viable Recovery Environment

If a company's backups are compromised or inadequate, paying the ransom may be the only way to regain access to critical data and systems. This highlights the importance of robust backup and disaster recovery strategies.

Fear of Data Theft and Erasure

Ransomware gangs often threaten to leak or delete stolen data if the ransom is not paid. The potential consequences of this – including regulatory fines and lawsuits – can be a powerful motivator for payment.

Protecting Consumers and Partners

In some cases, a ransomware attack may disrupt services or compromise the data of customers or other businesses. Paying the ransom may be seen as a way to minimize the impact on these stakeholders and maintain critical relationships.

Highly Capable Threat Actor

If the attacker is known to be particularly sophisticated and persistent, there may be a fear that they will cause further damage or launch follow-up attacks if the ransom is not paid.

Life-or-Death Situations

In rare cases, ransomware attacks may target critical infrastructure or healthcare providers, potentially putting lives at risk. In such situations, paying the ransom may be seen as the only option to prevent a humanitarian crisis.

Why Policyholders May Consider Not Paying the Ransom

Sanctions and Legal Concerns

Paying ransoms to individuals or entities on the Office of Foreign Asset Control (OFAC) **sanctions list** is illegal. Additionally, there may be concerns about potential legal repercussions or reputational damage associated with funding criminal activity.

Availability of Effective Backups

If a company has robust and tested backups, it may be able to recover from a ransomware attack without paying the ransom. This underscores the critical importance of data backup and recovery planning.

Data Hasn't Been Compromised

If the attacker has not exfiltrated or encrypted sensitive data, there may be no need to pay the ransom. However, it is crucial to thoroughly investigate the extent of the attack to ensure that this is the case.

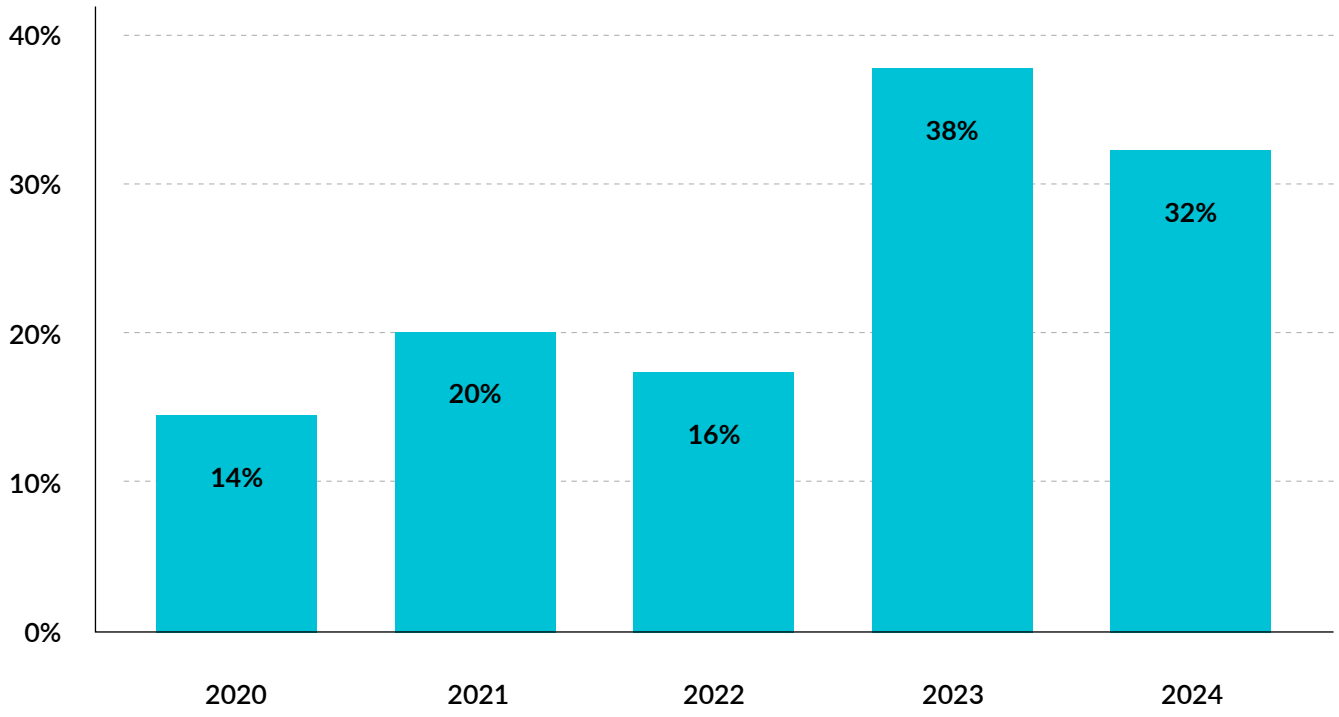
Principled Stance

Some organizations may simply refuse to negotiate with cybercriminals on principle, believing that paying ransoms only encourages further attacks.

The Primacy of Privacy

As cybersecurity and privacy concerns continue to intersect both within and outside of companies, claims are on the upswing.

Proportion of Third-Party Cyber Claims Triggered by a Privacy Incident (U.S.)



In the U.S., the proportion of third-party claims related to privacy liability has doubled in 2023-24 vs 2020-22.

Chubb's cyber insurance policies address privacy-related exposures more throughly than those of many other insurers, in large part because of our deep understanding of the ever-changing regulatory landscape.

Some U.S. laws that are currently having a considerable impact on privacy claims include:

Illinois Biometric Information Privacy Act (BIPA)

This law regulating the collection, use and handling of biometric identifiers and information by private entities resulted in a spike in claims that began in 2019 and persists even today, following adverse court decisions clarifying the statute of limitations and the accrual of claims.

Video Privacy Protection Act (VPPA)

This law directly addresses the manner in which companies use pixels, the tiny snippets of code embedded in a website that can track a multitude of events, including which items have been added to a cart or which products were reviewed during a visit. This information can then be sent to a third party for targeted advertisement or other commercial purposes. Since 2022, Chubb insureds have reported a wide range of claims alleging that websites have, through such activity, disclosed claimants' personal identifiable features and viewing histories without the claimants' consent, in violation of VPPA. The law allows for statutory damages of up to $2,500 per violation.

Wiretapping Laws

Wiretapping laws, such as the **California Invasion of Privacy Act** (CIPA), allow individuals to pursue a private right of action against businesses for violations of privacy, with statutory damages of up to $5,000 per violation. Other states such as Connecticut, Michigan, Pennsylvania and Washington also have statutes of this sort. Many recent claims are rooted in the part of the statute explicitly prohibiting the reading of any message, report or communication without consent. Plaintiff attorneys and courts have recently interpreted that a "message, report or communication" can include internet server session information, meaning that any attempt made by a party to read or learn the contents of information shared on the internet may legally constitute eavesdropping. The types of claims we are seeing under this statute frequently involve web session analytics and chat sessions.

In the U.S.

Privacy laws and regulations are being implemented with increased frequency and are having a measurable impact on claims, including cases involving mass arbitration of alleged violations of VPPA and wiretapping statutes, with arbitration fees becoming payable before the merits of the claim are even considered. Other state laws, such as Illinois's **Genetic Information Protection Act** (GIPA) and Washington's **My Health My Data Act**, should also be on the radar of any companies that are concerned about privacy liability.

> Unlike a number of our peers, Chubb has developed a specialty in managing the risk of unintentional privacy violations. Our cyber claims specialists can help companies avoid litigation by sharing our knowledge of the relevant legal and technological issues – issues that will only grow more complicated as factors like artificial intelligence come into play.

Outside the U.S.

Outside of the U.S., other frameworks such as the EU's **General Data Protection Regulation (GDPR)** regulate the lawful collection, processing, use, and retention and deletion of personal identifiable information. In recognition of increasing concerns over how personal data are being shared at a global level for commercial purposes, many countries have crafted or are now in the process of crafting laws that can create obligations and risk for all companies doing international business – not just media companies.

Controls Matter: Adopting a Zero Trust Approach to Cybersecurity

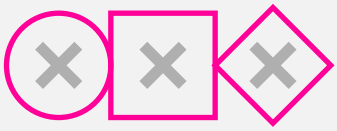
Widespread events do not always occur as a result of a malicious attack. In July 2024, **CrowdStrike**, an American cybersecurity company, sent a faulty software update to customers around the world that specifically impacted workstations and servers.

Thousands of businesses that used CrowdStrike were impacted, and thousands more were affected because their vendors or suppliers used CrowdStrike.

The result was global disruption.

8.5 million
systems crashed

Both direct clients of CrowdStrike and those with vendors that used CrowdStrike were impacted.



Airlines, hospitals, banks, stock markets, governments, retail establishments and many others that used the software found themselves unable to function.

$400M-$1.5B
in insured losses

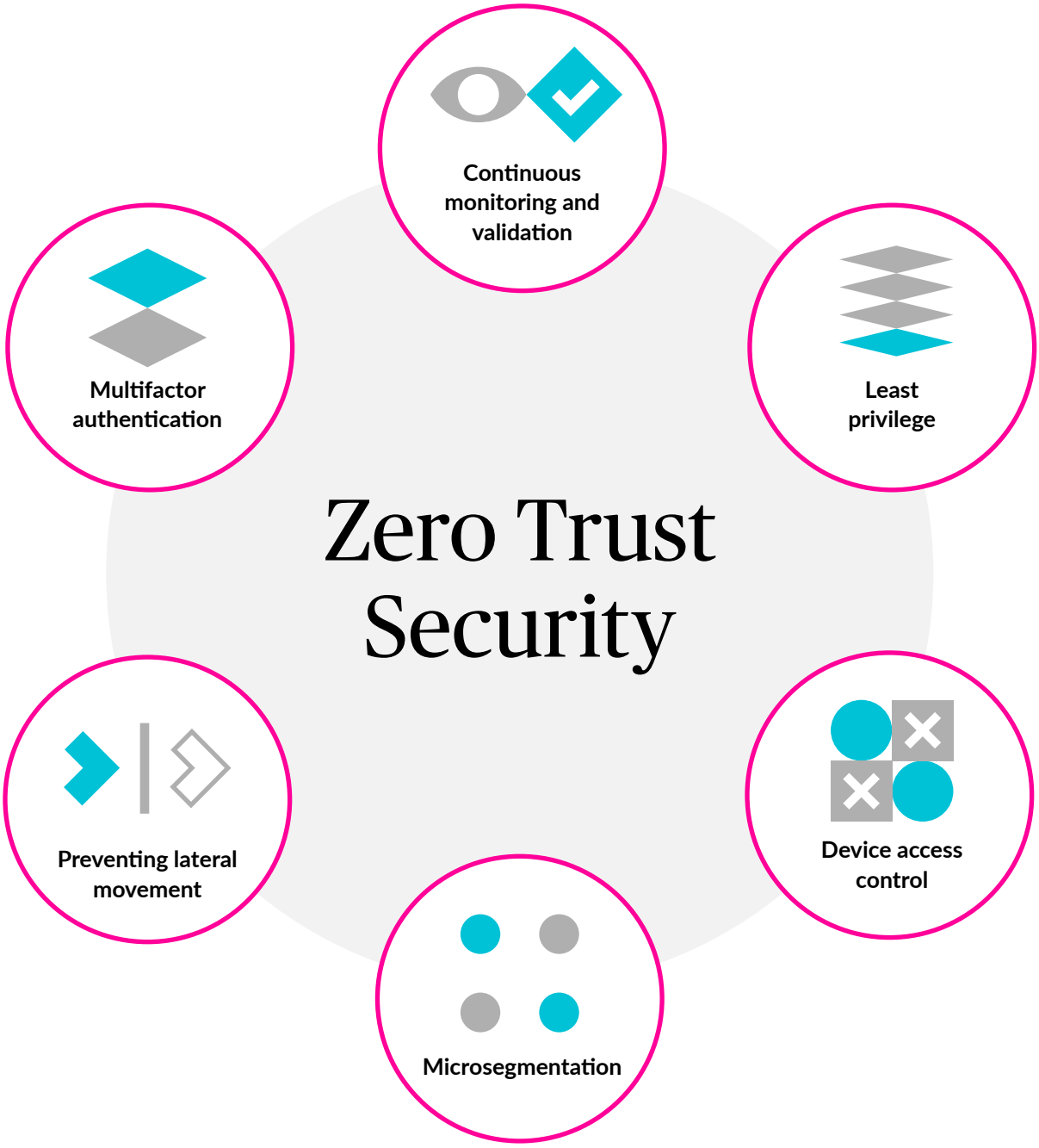
Customers with strong resiliency measures in place were less impacted.

Source: https://www.cybcube.com/news/cybercube-estimates-global-insured-losses-from-crowdstrike-event#:~:text=The%20faulty%20CrowdStrike%20Falcon%20Sensor,premiums%20of%20$15bn%20today

The CrowdStrike outage served as a reminder that non-malicious incidents can be as impactful as malicious cyber attacks. Practical lessons that can be gleaned from this unfortunate event include the importance of implementing and rehearsing incident response plans, as well as employing resilience measures to mitigate and quickly recover from unforeseen events that impact your business directly or via your supply chain.

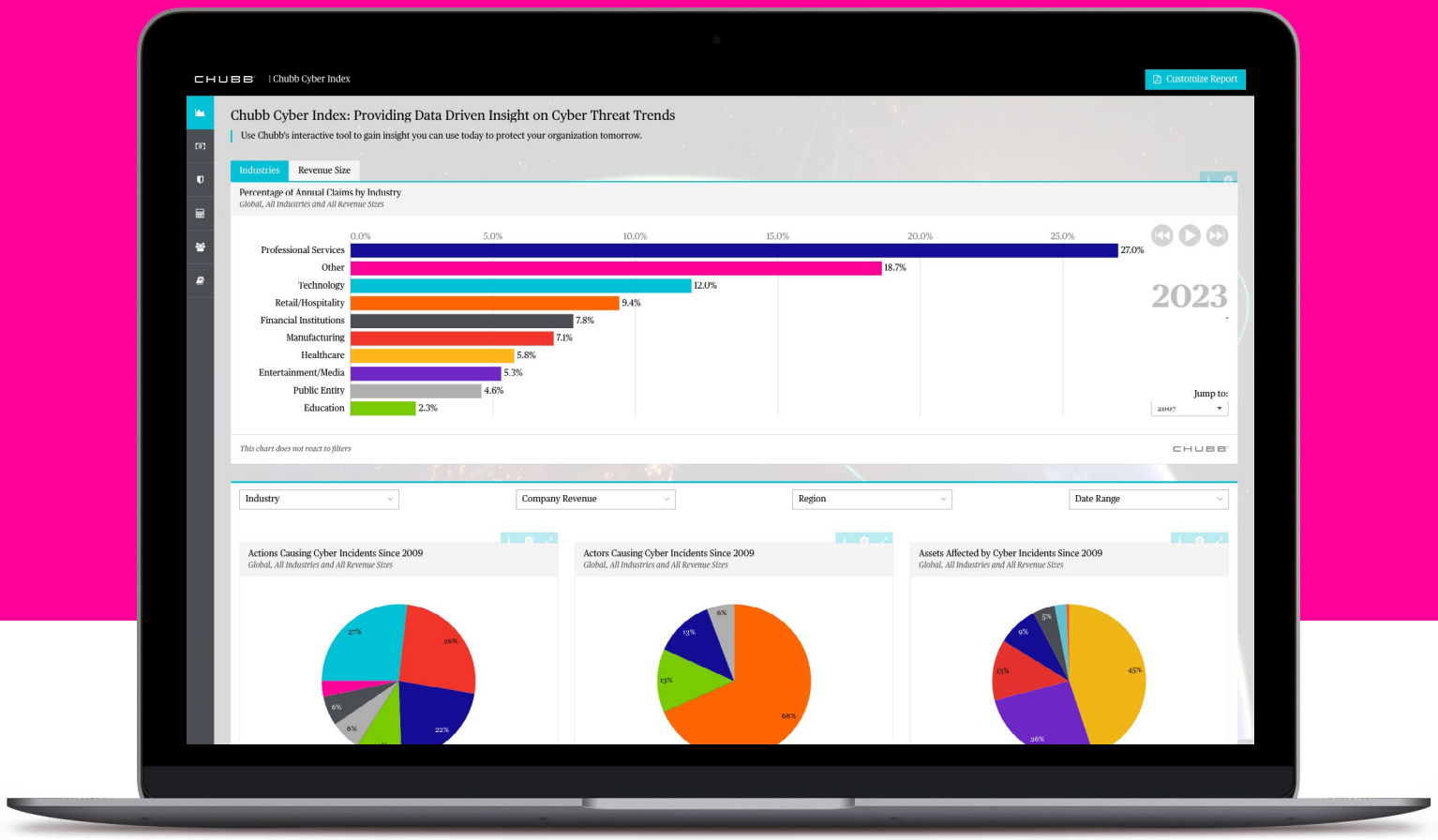
A **Zero Trust security model** is essential to maintaining controls.

This means employing and maintaining strict protocols that minimize the risk of breaches, disruptions, infections or errors by requiring the most stringent identity verifications for every single person attempting to access a private network – irrespective of their location or their status within the organization. Tools and policies might include **multifactor authentication**,[1] **least-privilege access**[2] and network **microsegmentation**,[3] among other solutions that have been shown to significantly reduce risk.



1. Source: https://www.cisa.gov/MFA
2. Source: https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP
3. Source: https://www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html

Chubb's Cyber Index: Empowering Companies With Data-Driven Insights



The **Chubb Cyber Index**, a digital tool that allows users to access our proprietary data regarding cyber threats and to craft strategies for protecting themselves, continues to grow and inform our brokers, providing valuable insights into industry-specific cyber risks and trends. The wealth of data that it contains fuels our underwriting decisions, enabling us to offer tailored solutions to our clients.

Consult Chubb's Cyber Index To Discover and Utilize:

Industry-specific insights

Detailed breakdowns of cyber attack trends and impacts across various industries and revenue sizes – which can be broken down further by date or region – allowing businesses to benchmark their risk profiles against their peers

Claims costs and paid incident response costs for cyber events

Sector-specific averages dating back to 2009

Ransomware "pulse check"

A specialized tool, in the form of a questionnaire, that allows businesses and organizations to identify their unique vulnerabilities to ransomware attacks and create the foundation for defensive strategies

Cyber risk calculator

Allows users to gain insight into the broader spectrum of cyber exposures and potential costs they may be facing

Peer purchasing insights

Allows users to examine cyber protection decisions made by other companies or organizations; capable of being broken down by industry, region and revenue size

Library and glossary

Links to videos and podcasts, plus other references to help companies and organizations further explore the ever-changing cybersecurity landscape

Helping Businesses Become More Secure

Businesses may not have the resources to fight against cyber events on all fronts by themselves.

Chubb offers many different **risk management services** and connects our customers directly to Chubb's team of **cyber advisors** who can help them craft the most effective management and response strategies.

Whatever your company size, Chubb can provide innovative cyber insurance solutions.

Chubb is the leading partner and go-to resource for businesses – of all sizes – that are seeking cyber protection. Work with our team of cyber advisors to protect your organization from cyber-related financial and reputational losses, and to gain access to essential mitigation tools and advisory resources that can help reduce your exposures 365 days a year. To learn more, click on the QR code below.

> These are just some of the tools that Chubb offers toward meeting our goal of helping clients safeguard against costly cyber events and continually strengthen their defences.

All cyber services are subject to change. Any changes to the service offerings will be reported on the local web form for cyber services. Policyholders are responsible for reviewing the specific conditions of each cyber service provider to ensure eligibility and to stay updated on any changes that may occur.

DISCOUNTED CYBER SERVICES OFFERED BY THIRD-PARTY PROVIDERS: External vulnerability monitoring. Secure password manager.

The above-described cyber services are offered by third-party providers at no additional cost to Chubb policyholders for the specified initial period, provided that the policyholder is a new subscriber/customer of the cyber services offered by the chosen third-party provider and meets the specific eligibility conditions. After the expiration of the specified initial period, policyholders may have the option to continue the cyber services at a discounted cost at the time of renewal. Please note that discounts may vary among specific products and services. Discounts on products and services offered by cyber service providers are available only to Chubb policyholders with active policies and are subject to applicable insurance laws. The products and services provided by third-party providers will be governed by the contractual terms that the policyholder will enter into with the third-party provider. Chubb will not be involved in the policyholder's decision to purchase services and has no liability for the products or services provided by any third-party provider.

This document is intended for information purposes only and does not constitute any kind of advice or recommendation for individuals or companies on any product or service. For more details on the terms and conditions of the product, please refer to the general terms of insurance.

Chubb European Group SE, Registered Office: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, France - Share capital €896.176.662 fully paid - General representation in Italy: Via Fabio Filzi n. 29 - 20124 Milan - Tel. 02 27095.1 - Fax 02 27095.333 - VAT identification number and Tax Code 04124720964 - Economic and Administrative Index No. 1728396 - Authorized to operate in Italy as an establishment registered with the IVASS (Italian insurance supervisory authority) under number I.00156. The activity in Italy is regulated by the IVASS, with regulatory regimes that could diverge from the French ones. Registered in the company's registry of Nanterre under number 450 327 374 by the Autorité de contrôle prudentiel et de résolution (ACPR) 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 RCS and subject to the rules of the French Insurance Code. info.italy@chubb.com - italy@pec.chubb.com - www.chubb.com/it.

We process the personal data provided by you or collected through authorized parties, such as insurance intermediaries, for purposes related to the underwriting and management of policies as well as for the assessment of any claims arising from the occurrence of an incident. The complete Privacy Notice regarding the processing of personal data is available on our website www.chubb.com/it-it/footer/privacy-statement.html.

IT-EN8785-HS 03/25

CHUBB®

chubb.com