Coalition®

coalitioninc.com

2023 Cyber Claims Report

An in-depth analysis of cyber claims data from Coalition

Table of Contents

Executive Summary

Technology remains the most significant driver of change. Businesses rely on technology to power all aspects of their operations, from online ordering to managing payroll. New technologies, like generative artificial intelligence (AI), have also rapidly accelerated the changes in how we live and work that were ushered in by a global pandemic and a growing distributed workforce.

The digital economy has created a new class of digital risks that make organizations vulnerable to disruptive events, such as ransomware, and the interconnected nature of technology has even fueled concerns about the possibility of a widespread cyber catastrophe. However, we finally saw cyber claims stabilize in 2022, as Coalition demonstrated that cyber risk is insurable with the correct data and approach.

The past year highlighted the outsized impact that employees have on cybersecurity. Whether failing to patch vulnerable software, using outdated technology, or clicking on malicious links, employee actions were the greatest contributing factor to organizations that experienced a cyber insurance claim. Conversely, organizations that prioritized security controls and promoted good cyber hygiene saw the benefits of their investments.

Threat actors increasingly chose the path of least resistance. Tried-and-true social engineering techniques and legacy technologies turned organizations into easy targets. In response, the U.S. government unveiled new regulation strategies, and lawmakers began calling for the private sector to take proactive steps to reduce their risk.

The most important lesson from 2022 is that cyber risk is manageable. A majority of the incidents we observed could have been prevented with the right security controls and an active approach to cyber risk management, illustrating why we closely partner with each of our policyholders. Through personalized monitoring and dedicated incident response teams, Active Insurance helps mitigate risks and prevent attacks before they happen — and Coalition policyholders experienced 64% fewer claims than the industry average.

We're proud to share Coalition's 2023 Cyber Insurance Claims Report to help brokers and the entire cyber insurance industry keep pace with the ever-shifting cyber landscape. This report is our firsthand look at the events and trends that impacted our policyholders, along with our expert analysis of what it could mean for the future.

Cyber trends in 2022

- Cyber claims stabilized, but cyber risk did not disappear
- Unresolved vulnerabilities led to more frequent cyber attacks
- End-of-life (EOL) software made organizations an easy target
- Active Insurance continued to help protect organizations of all sizes

Key Findings

Whether failing to patch vulnerable software, using outdated technology, or clicking on malicious links, employee actions were the greatest contributing factor to organizations that experienced a cyber insurance claim.

Cyber risks stabilized in 2022 after organizations faced significant turmoil in the preceding years. Although cyber crime remains a persistent threat, overall claims frequency declined during the year. Most organizations experienced a decrease in the frequency and severity of cyber claims, while less-sophisticated crimes grew in popularity.

Due to this shift, overall claims frequency decreased by 22% year-over-year. Furthermore, Coalition policyholders experienced 64% fewer claims than the broader cyber market[1], with 47% of reported events handled with no cost to the policyholder (Figure 1.1).

A less-sophisticated crime, funds transfer fraud (FTF) unseated ransomware as the leading event type, accounting for nearly one-third of all claims. Notably, ransomware saw a sharp decline among all reported claims, while business email compromise (BEC) remained steady (Figures 1.2 and 1.3).

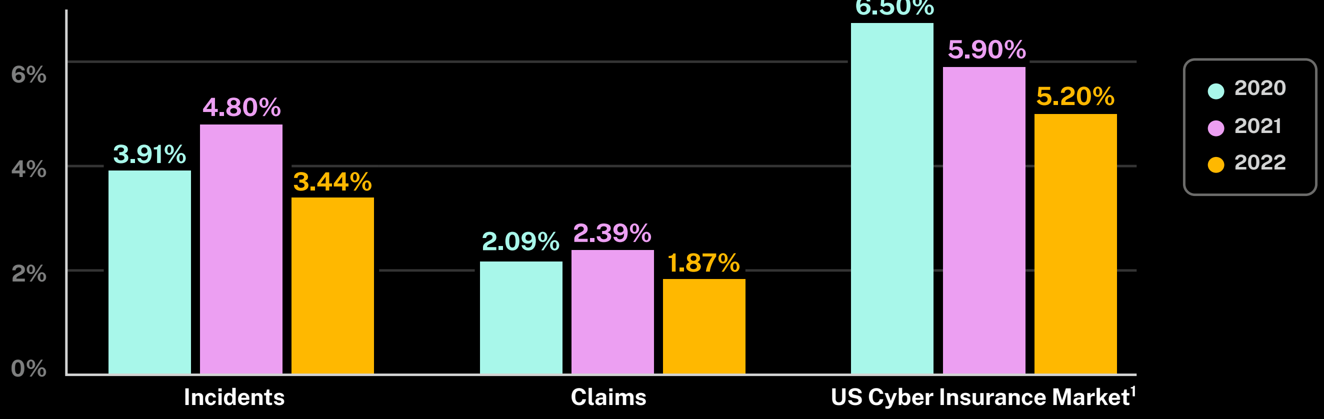
The greatest contributor to the decrease in overall claims frequency was ransomware, which dropped 54% year-over-year. Claims frequency for all other event types remained relatively flat (Figure 1.4).

As claims frequency dropped, claims severity increased by 7% to an average loss of nearly $169,000. The biggest contributor to the overall increase was Other[2] and BEC claims, which jumped 80% and 54%, respectively. Meanwhile, ransomware and FTF claims severity remained nearly the same, at $303,000 and $198,000, respectively (Figure 1.5).

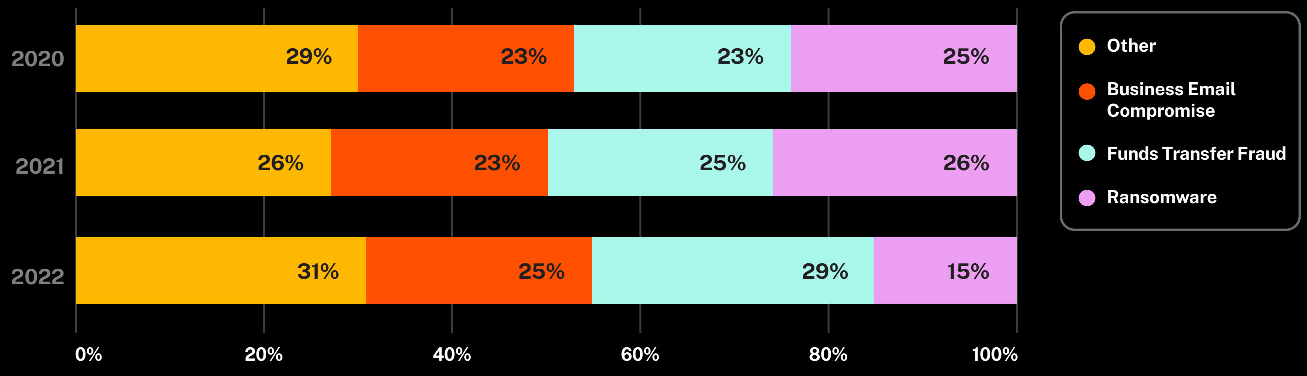
[1] *Market data is reported by US insurers to the National Association of Insurance Commissioners (NAIC). Frequency is calculated using the number of standalone cyber claims reported by the NAIC, divided by the average of standalone cyber policies in force at the current and prior year-ends.*

[2] *See Glossary section.*

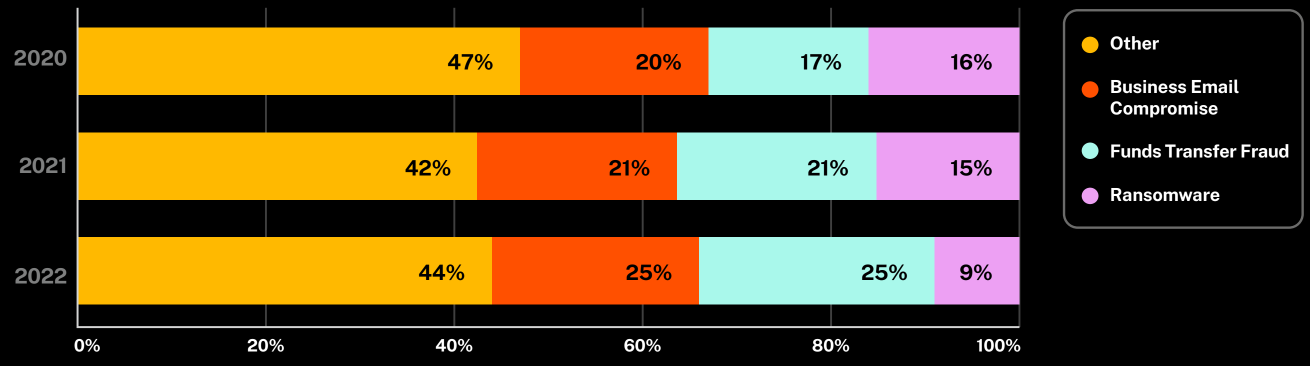
Claims frequency: US cyber insurance market and Coalition *(Figure 1.1)*



Percentage of reported claims by event type *(Figure 1.2)*

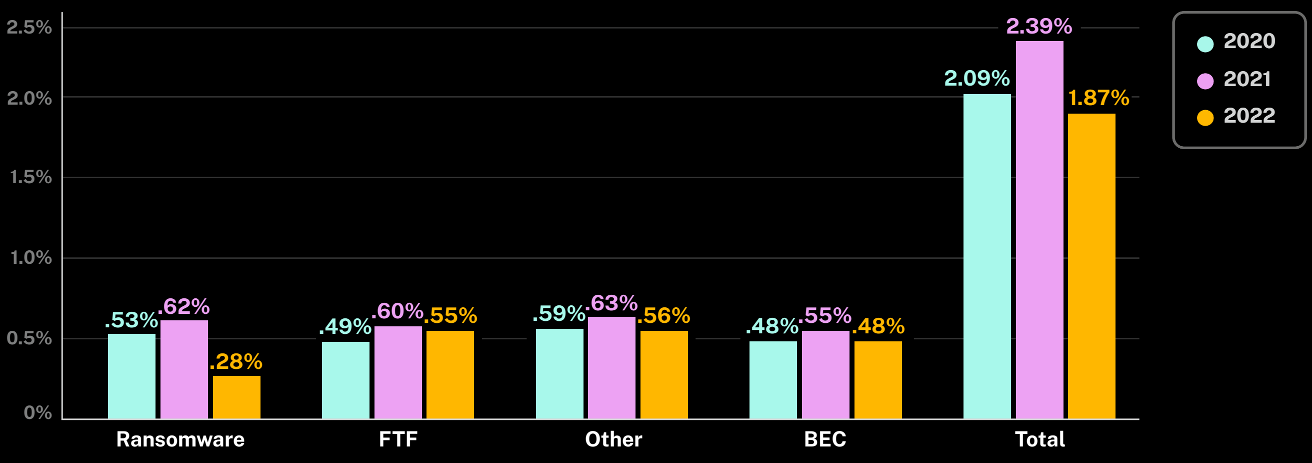


Percentage of reported incidents by event type *(Figure 1.3)*

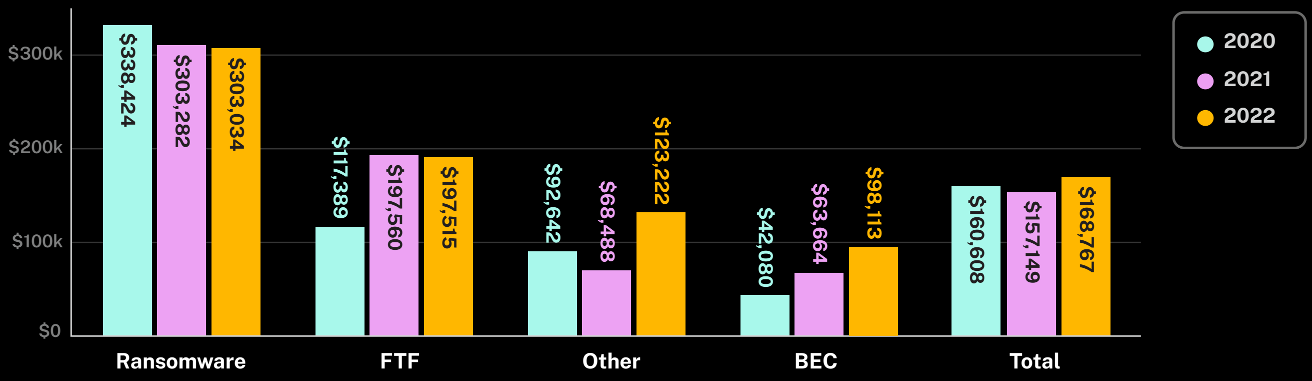


The "Other" event type among reported incidents includes pre-claims services for events that did not result in ransomware, FTF, or BEC. Coalition provides these services to all policyholders free of charge, and these events often do not result in the filing of a claim.

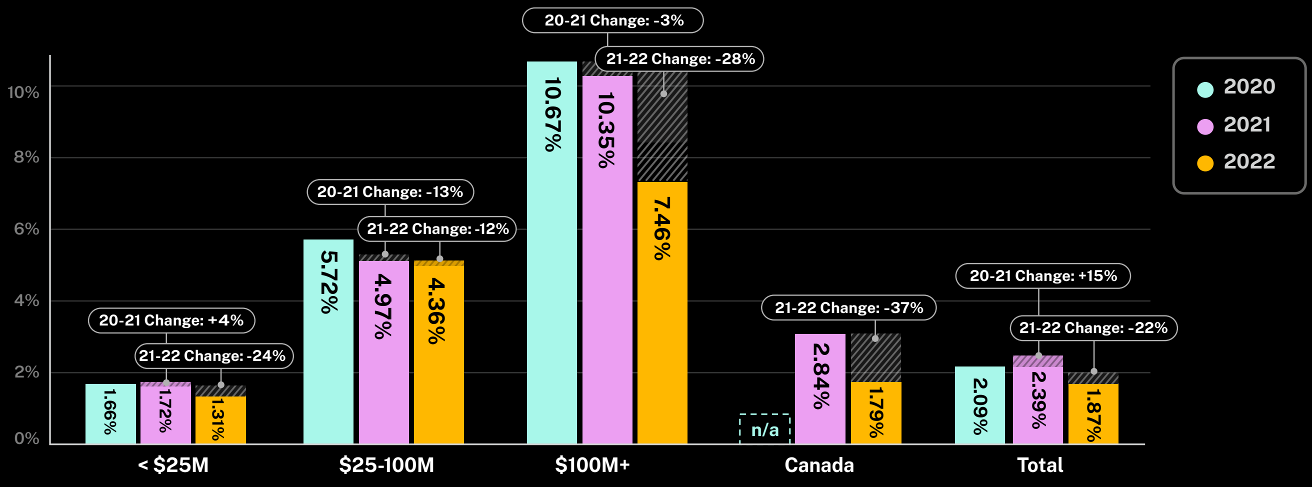
Claims frequency by event type *(Figure 1.4)*



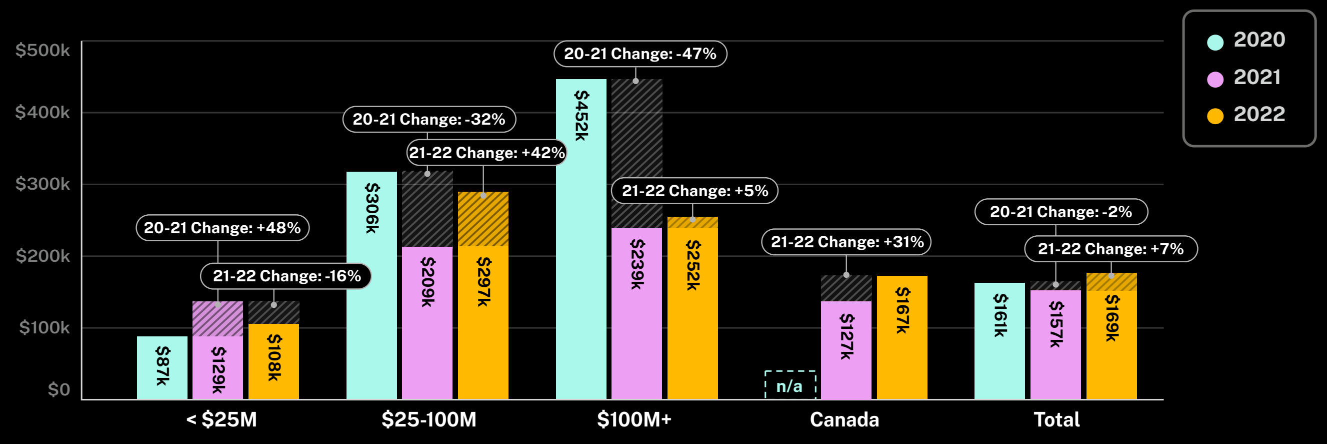
Claims severity by event type *(Figure 1.5)*



Claims frequency by revenue band: US and Canada *(Figure 1.6)*



Claims severity by revenue band: US and Canada *(Figure 1.7)*



Organizations that prioritized security controls and promoted good cyber hygiene saw the benefits of their investment.

Claims frequency for businesses with less than $25 million in revenue decreased 24% after a slight increase in the previous year. Claims frequency for businesses with more than $100 million in revenue also dropped 28%, while mid-market businesses decreased by 12% (Figure 1.6).

Similarly, businesses with less than $25 million in revenue had claims severity plummet 16% after seeing a 48% jump the year prior. Nonetheless, the average claim for businesses of this size was still more than $108,000, a substantial loss for small businesses and often the result of limited resources and funds to train employees, patch vulnerabilities, and retire outdated technology (Figure 1.7).

Incidents vs. Claims

Coalition uses two metrics to measure the impact of cyber risks: incidents and claims. Measuring these numbers separately tells us how many incidents impact policyholders and how our claims compare with the overall market.

- **Incidents** - any adverse cyber event reported by a policyholder
- **Claims** - any incident that incurred a loss[2]

Attackers Targeted Unresolved Critical Vulnerabilities

Coalition's Active Risk Platform continuously scans the internet to collect data and gather intelligence on potential vulnerabilities, then alerts policyholders to help them quickly resolve the risk.

Modern organizations are increasingly reliant on technology to operate, but critical vulnerabilities can turn essential technologies into significant cyber risks — especially if the vulnerabilities go unresolved. To bridge the gap that exists for many companies, Coalition Control, powered by Coalition's Active Risk Platform, continuously scans the internet to collect data and gather intelligence on potential vulnerabilities, then alerts policyholders to help them quickly resolve the risk.

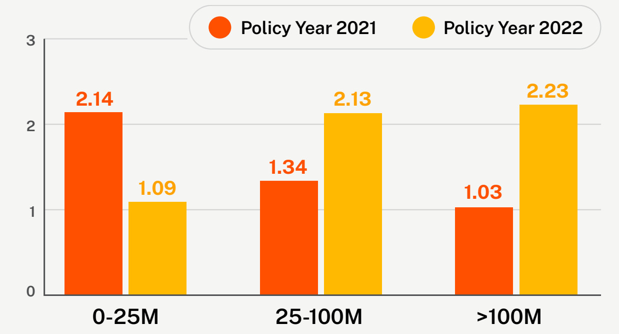
For example, after security vendor Fortinet announced several critical vulnerabilities, we promptly alerted policyholders and urged them to take remediation steps. Consequently, organizations with exposed Fortinet devices experienced **three times** as many claims as those with no Fortinet devices.

Businesses with more than $100 million in revenue using Fortinet devices were more than twice as likely to experience a claim in 2022 compared to 2021, while businesses with less than $25 million in revenue were two times *less* likely to experience a claim (Figure 2.1).

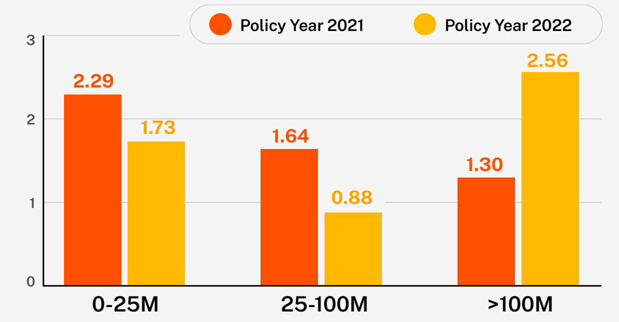
In fact, policyholders with one unresolved critical vulnerability of any kind were 33% more likely to experience a claim than those who resolved the vulnerability, according to analysis of our scanning, alerting, and forensics data.

Critical vulnerabilities associated with specific technology products continued to create risk, particularly with Microsoft Exchange. Both businesses with less than $25 million in revenue and businesses

Fortinet frequency multiplier *(Figure 2.1)*



On-premise Microsoft Exchange frequency multiplier *(Figure 2.2)*



The frequency multiplier in these charts is the relative likelihood of a claim tied to on-premise Microsoft Exchange.

Policyholders with one unresolved critical vulnerability of any kind were 33% more likely to experience a claim than those who resolved the vulnerability.

with more than $100 million in revenue running on-premise Microsoft Exchange had an increased risk of claims.

Businesses with less than $25 million in revenue with on-premise Exchange were nearly twice as likely to experience a claim than those without it, signifying the continued risk of running on-premise Exchange. Similarly, businesses with more than $100 million in revenue with on-premise Exchange were more than twice as likely to experience a loss than those without it — a 97% increase from 2021 (Figure 2.2).

Overall, organizations that did not resolve critical vulnerabilities in their technologies were more likely to experience a claim. As reported in our first-ever Cyber Threat Index, the majority of vulnerabilities in 2022 were exploited within the first 30 days of public disclosure, underscoring the importance of quick and consistent patching.

CASE STUDY

Unpatched vulnerability leads to $1M+ ransom

Coalition alerted a manufacturing business about its exposure to a Fortinet vulnerability. Despite our warning, the manufacturer did not remediate the issue. As a result, a threat actor gained network access and deployed ransomware, demanding over $1 million. After a painful eight days of disruption, the manufacturer was able to resume operations, but not before incurring significant financial losses.

End-of-Life Software Predicted Organizational Risk

Policyholders using EOL software were **three times more likely** to experience a claim than those not.

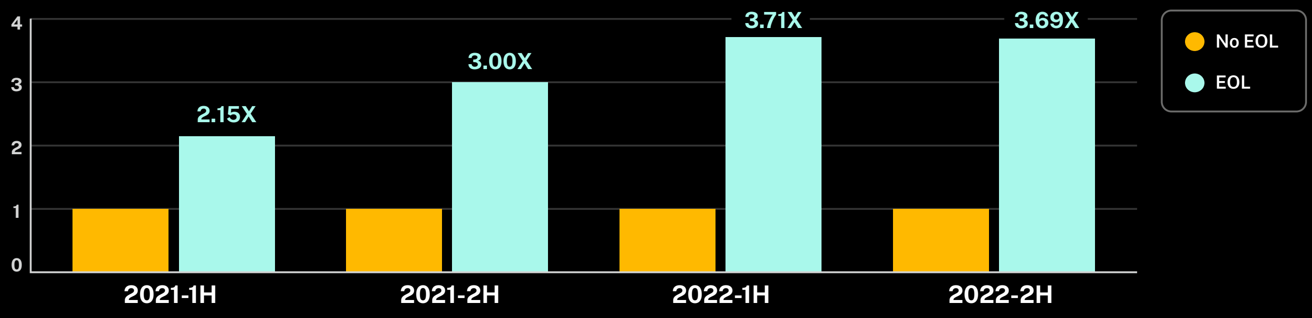
End-of-life (EOL) software are products no longer supported or updated by their original developers and, thus, highly vulnerable to cyber attacks. EOL software reveals targets of opportunity for threat actors; it signals weak security controls or unprotected infrastructure is likely in place, which creates risk for companies. Once a threat actor has targeted an organization, they can launch any number of attacks to gain unauthorized access.

Policyholders using EOL software were **three times more likely** to experience a claim than those not. Over the past two years, claims among policyholders using EOL software steadily increased, a trend that held true regardless of organization size (Figure 3.1).

Examples of EOL software used by policyholders who experienced a claim:

- Adobe Flash
- Microsoft Windows XP
- Microsoft Office 2003
- Microsoft IIS versions 6, 7, 7.5 (support for 8, 8.5 ending in 2023)

Relative likelihood of a claim: End-of-life software *(Figure 3.1)*

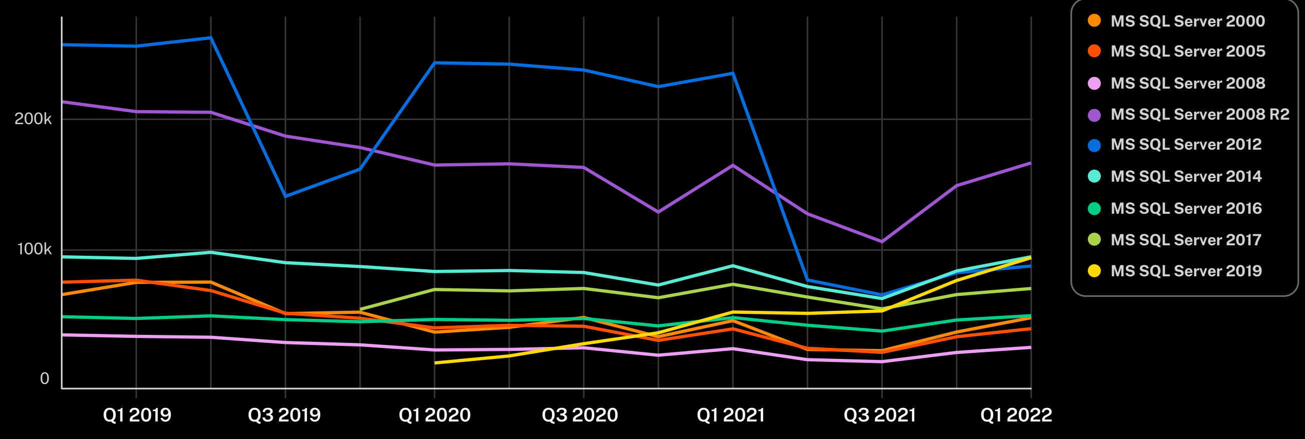


Continued use of EOL Microsoft SQL leaves organizations vulnerable to cyber attacks from any of the many documented critical vulnerabilities

Many EOL versions of the popular database platform Microsoft SQL are still in use, according to the Coalition Cyber Threat Index. Scanning data from Coalition's Active Risk Platform identified that the use of Microsoft SQL 2008 R2, which was officially deprecated in 2012, remains prevalent (Figure 3.2). Continued use of EOL Microsoft SQL leaves organizations vulnerable to cyber attacks from any of the many documented critical vulnerabilities, including two high-severity vulnerabilities that impact the 2008 R2 version.

Upgrading and patching all internet-facing software is critical, and organizations should implement a process to ensure they use the most up-to-date versions of these popular technologies.

Top Microsoft SQL server usage *(Figure 3.2)*



Phishing Gained Momentum as Top Attack Vector

Phishing was the initial attack vector for 76% of reported claims in H2 2022 — more than six times greater than the next-most popular attack technique.

Phishing became a fixture of everyday life as hackers attempted to trick employees to gain access to critical systems. The onslaught of emails, text messages, and voicemails was irritating, yet highly effective. In 2022, phishing was the **most common** attack vector to execute cyber attacks. Threat actors increasingly used the popular technique to target victims and gain access to sensitive information, often in service of other cybercrimes.

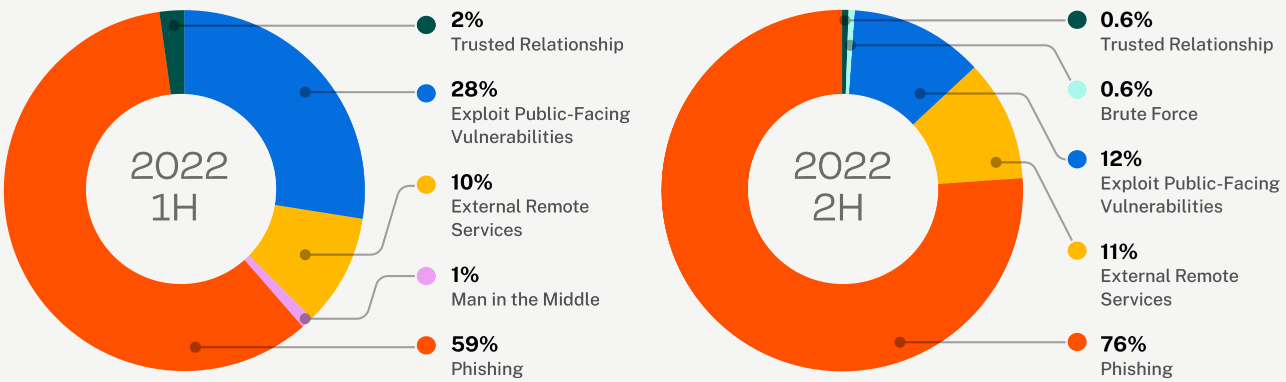
Phishing was the initial attack vector for 76% of reported claims in H2 2022 — more than six times greater than the next-most popular attack technique (Figure 4.1). This trend held true across the United States, as the FBI reported more than 300,000 incidents.[3]

Phishing-related claims have spiked over the course of the year — increasing 29% from H1 2022[4] — as the rise of new technologies has made these attacks easier to execute. Threat actors have started leveraging AI tools to write credible phishing emails and translate the scams across multiple languages, giving them more time and cover to gain access to a network.

[3] Federal Bureau of Investigation, Internet Crime Report, 2022.

[4] Data based on the determination of root cause, as reported by Coalition Incident Response, a forensic vendor engaged by certain Coalition policyholders.

Percentage of reported attacks by attack vector *(Figure 4.1)*



Note: attack vector data is not known in all cases. These charts reflect attack vectors for reported claims where the attack vector was known. Vectors are categorized according to the MITRE ATT&CK taxonomy of adversary tactics and techniques.

Threat actors increasingly used phishing to target victims and gain access to sensitive information, often in service of other cybercrimes.

As an attack vector, phishing often leads to FTF and BEC claims, both of which saw a slight uptick year-over-year in 2022. FTF events can result in organizations losing large sums of money, while BEC events can lead to the compromise or loss of various types of data and information, including intellectual property, critical business data, and personally identifiable information (PII).

CASE STUDY

Threat actor thwarted after phishing attempt

An accounting firm employee received an email with a seemingly innocuous message alert. After clicking the link, they were prompted to provide their username and password. After entering the information, nothing happened — the employee had just been phished. Coalition Incident Response was called in to investigate, and the team located the initial phishing email. It appeared the threat actor intended to launch another phishing campaign, but access was revoked and the policyholder incurred no additional loss.

Dwell Time Surged in Funds Transfer Fraud Events

When policyholders alerted us to an FTF event, we successfully recovered 66% of lost funds.

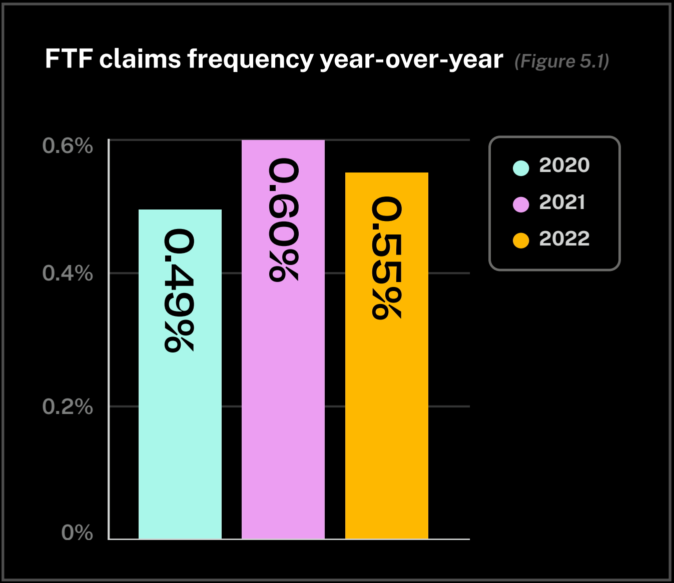
Funds transfer fraud (FTF) remains one of the easiest ways to monetize cyber crime. Often perpetuated via email phishing, FTF events allow threat actors to redirect or change payment information to steal funds. The average FTF loss amount (prior to recovering funds) in 2022 was $212,000, a 36% decrease from $331,000 in 2021.

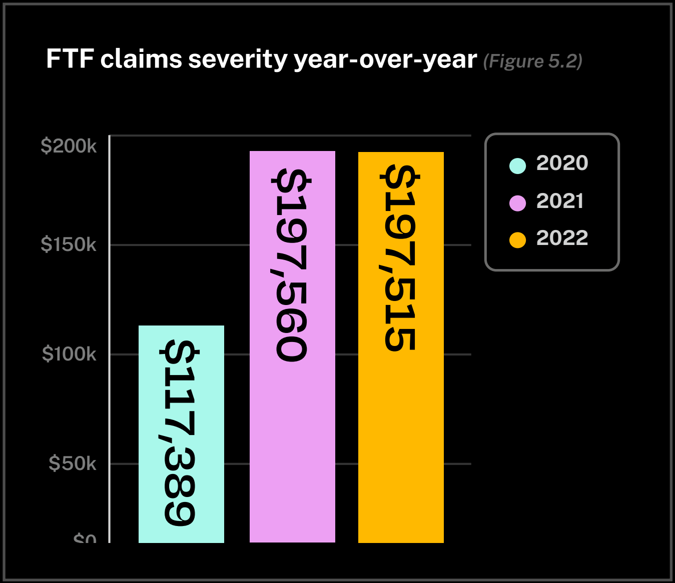
FTF frequency slightly decreased in 2022 after sharply rising 23% in 2021 (Figure 5.1). Similarly, FTF severity flattened in 2022 after a 68% surge in 2021 (Figure 5.2). Recovering funds has become more complex due to an increase in dwell time, the duration a threat actor remains in a network before executing an FTF event.

Dwell time gives threat actors more time to gather information, understand how an organization operates, and hide evidence of their crimes, which impacts the victim's ability to respond. In 2022, the average dwell time associated with FTF events was 42 days, an increase from 24 days in 2021.

When an FTF event occurs, Coalition works with policyholders to attempt to recover the funds. Fraudulent activity is usually detected when vendors inquire about missed payments or organizations notice unusual mailbox rules. The first 72 hours are critical in successfully stopping payments or reversing transfers, and Coalition works with our contacts in law enforcement and financial services to attempt to recover the funds.

When policyholders alerted us to an FTF event, we successfully recovered 66% of lost funds. However, as a result of the increased dwell time, our overall recovery numbers declined, falling to 36% in H1 2022 and 15% in H2 2022.





The first 72 hours are critical in successfully stopping payments or reversing transfers.

How to combat funds transfer fraud

- Turn on multi-factor authentication (MFA) for all online accounts, especially banking and email.
- Establish a procedure for requests to change payment information.
- Verify the authenticity of the request by calling a known phone number (not the number in an email).
- Require two-party review and approval for all funds transfers.
- Never confirm new or payment change requests via email.

Ransomware Dipped Amid Demand Downturn

Ransomware claims frequency dropped 55% year-over-year. This trend held true nationally, as the FBI reported a 36% decrease in reported ransomware incidents.

After serving as the attention-grabbing headline for years, ransomware subsided in 2022. Speculation continues to swirl around the reason for the year-over-year decrease: Russia's war in Ukraine is often cited as a significant contributor, though organizations are also increasingly utilizing secure offline backups to avoid paying steep demands.

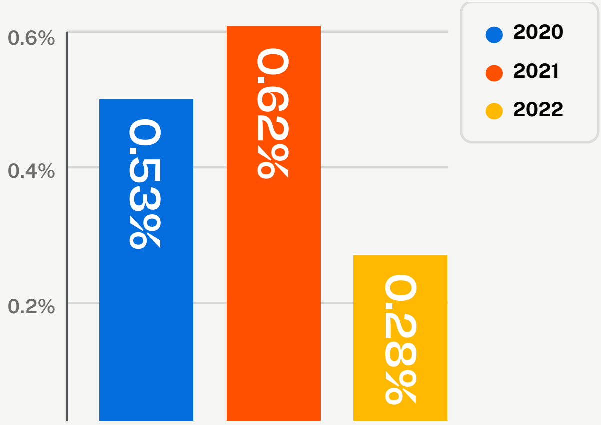
Ransomware claims frequency dropped 54% year-over-year (Figure 6.1). This trend held true nationally, as the FBI reported a 36% decrease in reported ransomware incidents, from 3,729 incidents in 2021 to 2,385 incidents in 2022[5]. In contrast, the severity of ransomware incidents flattened in 2022, remaining at $303,000 (Figure 6.2).

Ransomware demands also decreased year-over-year. The average ransomware demand in 2021 was $1.2 million compared to $1 million in 2022 — a 17.5% drop. Businesses with less than $25 million in revenue experienced the sharpest decline (53%) in demand amounts, shrinking from $1.1 million in 2021 to $400,000 in 2022.

[5] *Federal Bureau of Investigation, Internet Crime Report, 2022.*

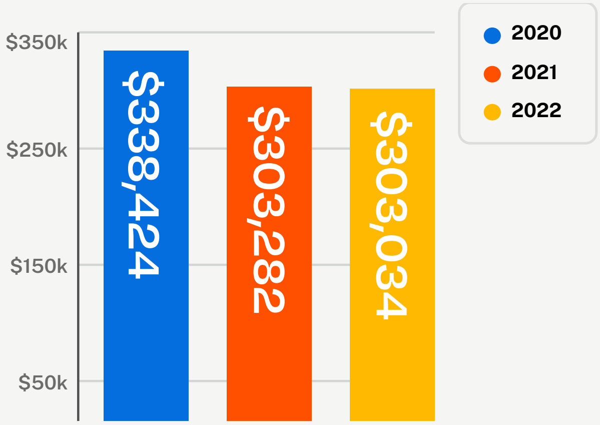
Ransomware claims frequency year-over-year

(Figure 6.1)



Ransomware claims severity year-over-year

(Figure 6.2)



Coalition successfully negotiated the payments down to an average of 27% of the initial demand in 2022.

Coalition observed ransom demands in the millions of dollars for three variants, including Black Basta ($8 million), Karakurt ($5 million), and Lorenz ($5 million). While ransomware demands can seem insurmountable for businesses that choose to pay, **Coalition successfully negotiated the payments down to an average of 27% of the initial demand in 2022.**

CASE STUDY

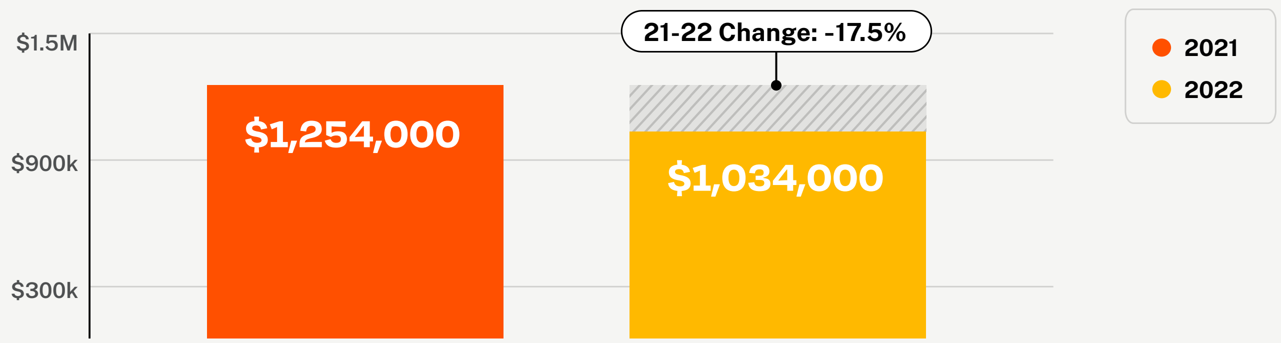
After ignoring alerts, business hit with $750K ransomware demand

Coalition notified a healthcare organization about its exposure to a critical vulnerability related to Remote Desktop Protocol. After failing to remediate the issue, they experienced a ransomware event directly tied to the vulnerability. With no viable data backups, the organization had to pursue buying a decryption key from the threat actor demanding a $750,000 ransom.

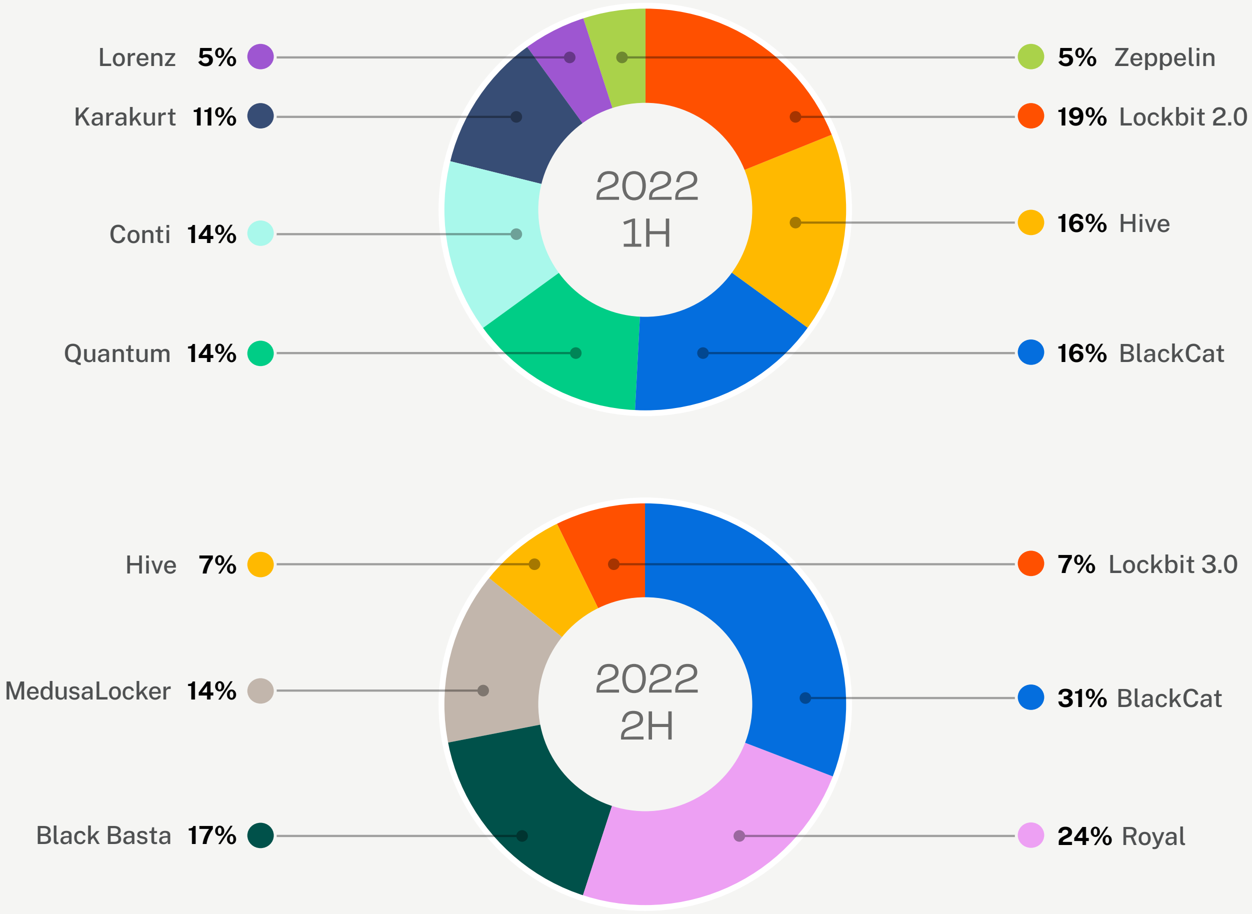
Ransomware variant trends

While the frequency and severity of ransomware decreased, one thing is clear: the malware variants that result in losses from ransomware claims are highly dynamic and have shifted year-over-year in our claims data (Figure 6.4). Given the highly-dynamic nature of ransomware, we anticipate both variant trends and frequency to shift again.

Average ransom demand year-over-year *(Figure 6.3)*



Top ransomware variants by incidents reported *(Figure 6.4)*



Predictions

FTF remains one of the easiest cyber crimes to monetize and we anticipate surges in 2023, likely aided by the increased ease of phishing and AI advancements.

At Coalition, we have unique insight into the cyber threat landscape and its impact on our policyholders. We expect that the market will continue to evolve. Our claims, incident response, and insurance teams shared the following predictions for the upcoming year.

Ransomware will return.

From what we've seen in cyber attack trends, ransomware gangs will continuously evolve their tactics. We anticipate another rise in ransom demands as long as global socioeconomic conditions remain volatile. And analysts agree — a recent poll of the Washington Post's Cybersecurity 202 Network of cybersecurity experts showed the majority of survey respondents say they expected ransomware to "take off" in 2023.

FTF will remain an easy, and frequent, cyber crime.

Threat actors will continue to seek the immediate monetization of their crimes. FTF remains one of the easiest cyber crimes to monetize and we anticipate surges in 2023, likely aided by the increased ease of phishing and AI advancements. Companies and individuals should follow simple and consistent methods to prevent this type of loss.

All organizations across all industries should implement best practices like MFA, data backups, restricting access to critical information, and segmenting sensitive data, not only critical infrastructure providers.

Phishing attacks will become more personalized and persuasive.

Employees will continue to fall for phishing ploys, as technology makes it easier to execute more personalized scams. Threat actors will continue to leverage these broad phishing attacks permitting easy access to unprotected corporate systems leading to large payouts through FTF or extortion via ransomware. New AI technology will make personalized phishing scams through targeted emails and voice impersonation even more persuasive, requiring employees to think critically before responding.

Threat actors will optimize for the most impactful targets.

We expect the trend of threat actors focusing their attack efforts on the most impactful targets, like critical infrastructure (manufacturing, materials, and energy, for example), to continue into 2023. Sophisticated attackers will persist in their efforts to maximize damage, especially amidst the ongoing geopolitical conflict. The National Cybersecurity Strategy underscores this, delineating critical infrastructure as the sector most at risk. But all organizations across all industries should implement best practices like MFA, data backups, restricting access to critical information, and segmenting sensitive data, not only critical infrastructure providers.

Cyber insurers will play an important role in national cybersecurity.

The new National Cybersecurity Strategy calls for a shift in the balance of cyber responsibility "away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks." Coalition has a unique view of the conditions that result in incidents, and our incentives are aligned with our policyholders to actively reduce risk. We believe the cyber insurance industry will play a bigger role in the year ahead by promoting good security hygiene by recommending best practices and vendors who can help keep organizations safe.

The shifts we observed across the cyber risk landscape in 2022 were meaningful but not entirely surprising. Threat actors will always alter their tactics, identify legacy technologies, and target critical vulnerabilities, all of which contribute to the dynamic nature of cyber risk.

Active Insurance is the solution to changing cyber risk conditions. Designed to prevent digital risk before it strikes, Active Insurance combines technology and traditional coverage to provide continual risk assessment, protection, and response to address dynamic risks. This is why Coalition policyholders experienced 64% fewer claims than the industry average.

Our Active Risk Platform provides a comprehensive, near real-time cyber risk assessment for every new policyholder, which allows us to help improve their risk profiles and strengthen their security controls. We then continuously monitor policyholders and send personalized alerts through Coalition Control, our risk management platform, to notify them of new threats. By providing actionable recommendations on how to mitigate their exposure, we successfully handled 47% of reported events with no cost to the policyholder.

The Power of Active Insurance

The findings in this report illustrate the power of Active Insurance. Our commitment to policyholder security gives us an edge in assessing cyber risks and understanding the overall cyber risk landscape. With the backing of a powerful cybersecurity research team, we are able to help policyholders mitigate new risks and prevent attacks before they happen. Our in-house claims team is available 24/7, and our in-house incident response team, Coalition Incident Response (CIR), provides pre-claim services to help policyholders get back to business faster.

Our mission at Coalition is to protect the unprotected. We share these cyber insights to help our broker partners advise clients on new and emerging risks, empower policyholders to prioritize their cybersecurity posture, and bring more stability to the entire cyber insurance industry.

- To learn more about becoming an appointed Coalition broker, visit signup.coalitioninc.com.
- To receive a free Coalition Risk Assessment for your organization, visit control.coalitioninc.com.

Methodology

Regardless of whether or not an incident becomes a claim, what affects our policyholders matters to us because it causes them harm.

Cyber incidents are highly disruptive to businesses. Regardless of whether or not an incident becomes a claim, what affects our policyholders matters to us because it causes them harm. That's why we report cyber events in two ways when analyzing frequency and severity:

- **Incidents**
  Any adverse cyber event reported by a policyholder
- **Claims**
  Any incident that incurred a loss

The sample size of reported incidents and claims is limited in strict statistical terms; we'll continue to regularly update and share our analysis to identify changing trends. Our underwriting and risk engineering capabilities are unique among cyber insurance providers, and our claims frequency reflects this. As a result, we may see different types of claims than others.

The 2023 Coalition Claims Report includes reported incident data through December 31, 2022. To prepare our dataset for this report, we utilized our own internal claims data as well as that of our carrier partners. Our team of data scientists and actuaries used this data to complete the analysis.

Our underwriting and risk engineering capabilities are unique among cyber insurance providers, and our claims frequency reflects this.

As part of the analysis, our actuaries used historical trends to calculate ultimate losses, or fully developed claims, on open cyber claims and incidents. This means Coalition does not under-report our losses even though some of these events have not fully matured. The severity and frequency calculations in this report are based on this analysis.

While these calculations reflect the actuary's best estimates at the time of the report, deviations may naturally occur from one report to the next due to actual loss experience observed during that period. Accordingly, the actuarial analysis is updated for each report to reflect both new incidents and loss development on previous incidents. The 2023 Cyber Claims Report presents an annualized look at our claims and incident data to reflect on fully developed trends across a complete calendar year.

Coalition's root cause analysis methodology

In partnership with the forensics vendors we engage, we work to identify and attribute the root cause of every possible policyholder cyber incident. This allows us to better understand which root causes and attack vectors result in loss.

We aggregate and ingest root cause data in our Active Risk Platform, the data collection and analytics platform that powers our underwriting, continuous monitoring, and alerting capabilities. This enables us to more accurately and quickly identify future incidents and claims.

Glossary

Cyber attack: A deliberate attempt to breach the security of a computer system, network, or device in order to gain unauthorized access, steal data, disrupt services, or cause damage.

Cyber event: A broader term that encompasses any occurrence or incident involving or affecting computer networks, information technology systems, or electronic data.

Cyber claim: Unless otherwise noted, a claim is an incident that incurred a gross loss.

Cyber crime: Criminal activity involving a computer, a computer network, or networked devices. Individuals, businesses, groups, and governments can be targets of cyber crime.

Cyber incident: An incident is an adverse cyber event reported to Coalition by a policyholder.

Frequency: Frequency is the average number of claims per earned insurance policy, without reflecting policy limits and/or retention, with development to ultimate selected by the reserving actuary based on historical experience and ongoing trends.

Gross loss: Gross loss, or ground-up loss, is the loss to the policyholder before insurance.

Net loss: Net loss is the amount of loss sustained by an insurer after reflecting the self-insured retention, sub-limit(s) by coverage, and policy limit.

“Other” claims: Includes, but is not limited to: web application compromises not resulting in one of the other three claim event types (BEC, FTF ransomware), legal/regulatory proceedings, theft/misconduct/error - IP/data.

Severity: Severity is the average monetary loss of an insurance claim without reflecting policy limits and/or retention, with development to ultimate selected by the reserving actuary based on historical experience and ongoing trends.

Ultimate loss: The total gross or net loss for a fully developed claim, which includes paid losses, outstanding reported losses, and incurred but not reported (IBNR) losses.

Coalition®

coalitioninc.com

55 2ND STREET, SUITE 2500
SAN FRANCISCO, CA 94105

You are advised to read this disclosure carefully before reading or making any other use of this report and related material. The content of this report is (i) not all-encompassing or comprehensive; (ii) solely for informational purposes; (iii) not be construed as advice of any kind or the rendering of consulting, financial, legal, or other professional services from Coalition; and (iv) not in any way intended to create or establish a contractual relationship. Any action you take upon the information contained herein is strictly at your own risk and Coalition will not be liable for any losses and damages in connection with your use or reliance upon the information. The content of this report may not apply directly to specific circumstances and professional advice should be sought before any action is taken in relation to the information disseminated herewith. Coalition makes no representation or warranties about the accuracy or suitability of information provided in the report or related materials. The report may include links to other resources or websites which are provided for your convenience only and do not signify that Coalition endorses, approves or makes any representation or claim regarding the accuracy of copyright compliance, legality, or any other aspects of the resources or websites cited. Copyright © 2023. All Rights Reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.