Coalition®

2024 Cyber Claims Report

An in-depth look at cyber claims data and the state of Active Insurance

Table of Contents

Executive Summary

Technology has become ingrained in modern business and so has cyber risk. Cyber risk is now the most significant concern for business leaders globally.[1] As a result, businesses of all sizes and industries must take steps to safeguard their critical information from opportunistic threat actors.

For the better part of a decade, cyber insurance providers have been promoting good cyber hygiene and advocating for better risk management decisions — and policyholders are listening. Despite critical vulnerabilities reaching an all-time high and global ransom payments surpassing $1 billion in 2023,[2] businesses that reinforced their security controls and embraced partnership with cyber insurance providers were generally more secure.

Claims activity in 2023 has validated a belief long-held by Coalition: Volatility across the cyber threat landscape persists (and likely always will), but an active approach to cyber risk management can help reduce claims for businesses and insurance providers. The findings in this report highlight the value and impact of Active Insurance experienced by Coalition policyholders.

Key takeaways of 2023

- **Cyber claims increased year over year (YoY).** Overall frequency continued to trend upward. Although overall severity decreased in the latter half of the year, it was not enough to offset the first-half spike primarily driven by increased ransomware claims.
- **Cyber claims originated in the inbox.** More than half of all claims were business email compromise (BEC) or funds transfer fraud (FTF), highlighting the importance of email security as a key aspect of cyber risk management.
- **As ransomware payments hit $1 billion globally, Coalition ransomware severity dropped 54%.** Ransomware frequency, severity, and demands dropped in the second half of the year after a surge in the first half, though severity is still up year over year.
- **Businesses using select boundary devices were at greater risk.** Firewalls, virtual private networks, and other devices can help reduce cyber risk. However, boundary devices with known vulnerabilities increased the likelihood of a business experiencing a cyber claim.

Coalition's 2024 Cyber Claims Report features data and case studies from organizations across the United States. Cyber risk is global, and we believe this report's trends and risk mitigation strategies are applicable regardless of location. As an active partner in protecting organizations from digital risk, we're proud to share these insights to help policyholders, brokers, and others in our industry stay informed about the ever-changing threat landscape.

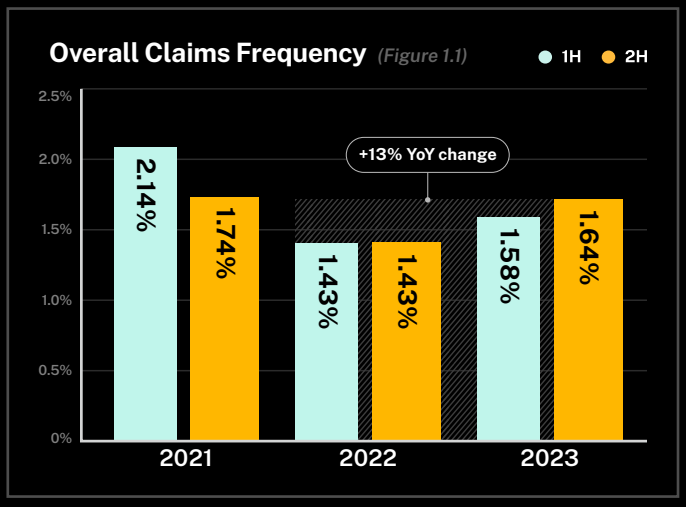
1. *Allianz, Allianz Risk Barometer 2024*
2. *Chainalysis, Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline*

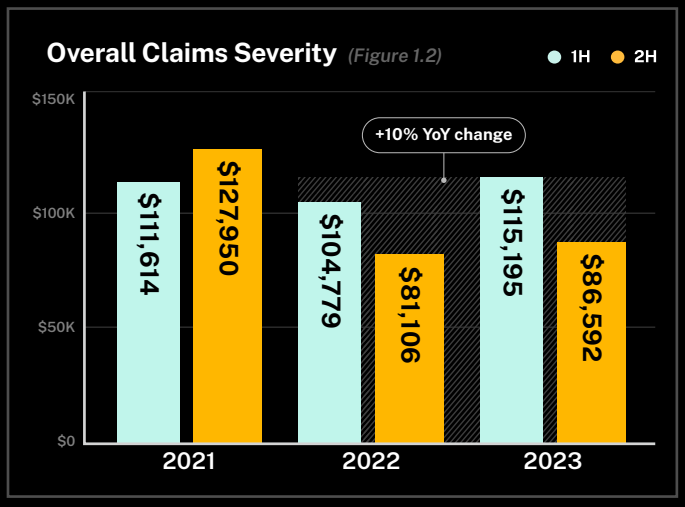
Cybercrime Put All Businesses at Risk

52% of all reported matters were handled without any out-of-pocket payments by the policyholder.

Cybercrime is a thriving business that adversely impacts the global economy. In 2023, the Federal Bureau of Investigation (FBI) received more than 880,000 complaints of cybercrime with reported losses of $12.5 billion.[3]

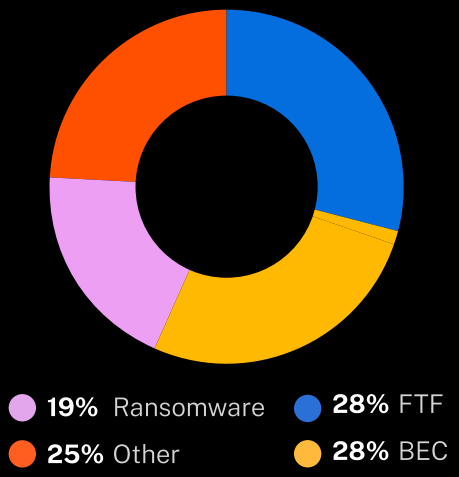
Overall claims frequency increased 13% YoY but remained below the historic high of 2021 (Figure 1.1). Overall claims severity increased 10% YoY to an average loss amount of $100,000, primarily due to a surge of ransomware claims in the first half of the year (Figure 1.2). However, 52% of all reported matters were handled without any out-of-pocket payments by the policyholder.





3. *Federal Bureau of Investigation, Internet Crime Report 2023*

Gross Reported Claims by Event Type
(Figure 1.3)



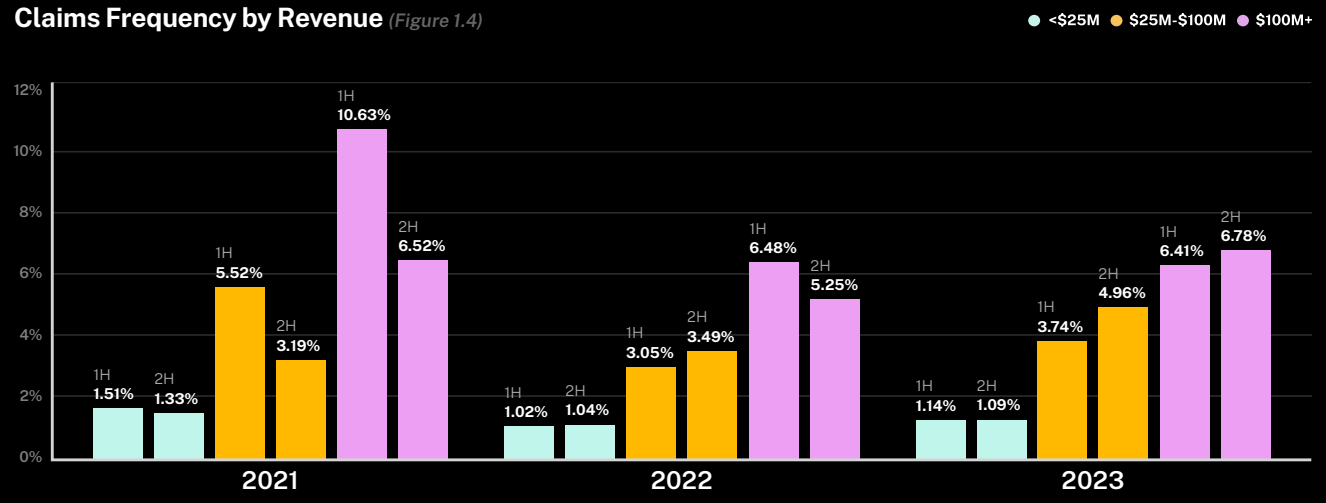
Ransomware accounted for just 19% of reported claims, although historically it is the largest source of claims severity (Figure 1.3). Funds transfer fraud (FTF) and "Other" events increased YoY by 2% and 7%, respectively, while claims related to business email compromise (BEC) decreased by 8% YoY.

Other events include: Errors, Misuse, and Theft; Legal, Privacy, and Media; Non-encryption System Compromise; and Third-party Compromise.

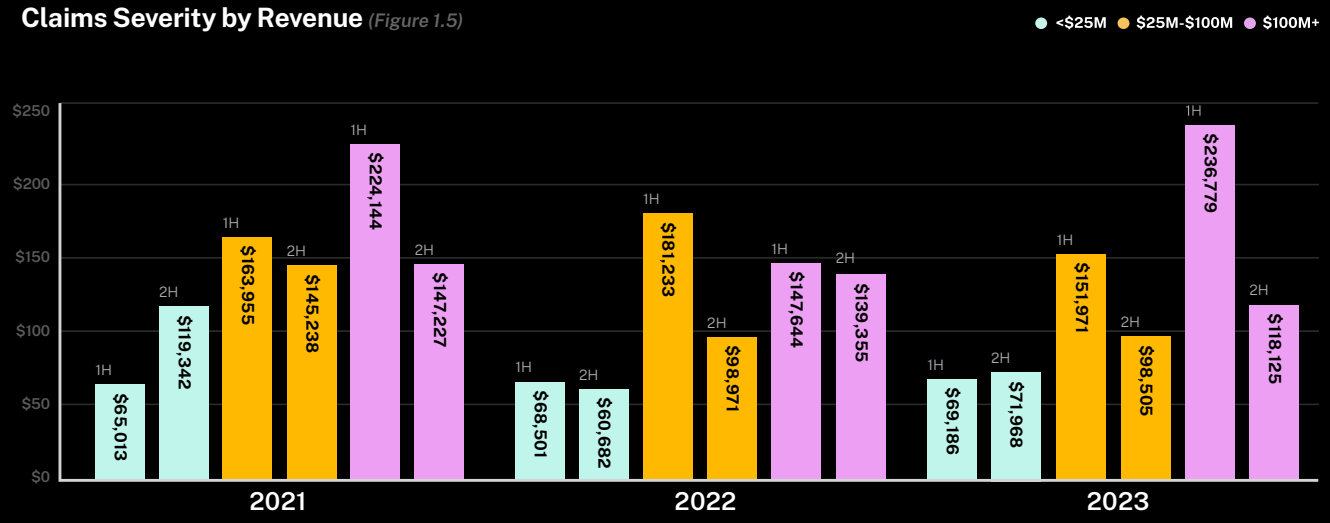
Claims frequency increased across businesses of all revenue amounts. Businesses between $25 million and $100 million in revenue saw the sharpest spike, with a 32% increase YoY (Figure 1.4). Businesses with more than $100 million in revenue saw a 14% increase in frequency, while businesses with less than $25 million in revenue experienced an 8% increase.

Businesses with more than $100 million in revenue saw a 14% increase in frequency, while businesses with less than $25 million in revenue experienced an 8% increase.

Claims Frequency by Revenue *(Figure 1.4)*



Claims Severity by Revenue *(Figure 1.5)*



The uptick in overall claims frequency and severity among Coalition policyholders is indicative of industry-wide trends, though far less volatile than the pandemic-era ransomware boom in 2021.

Claims severity stabilized in the latter half of the year after a volatile start. After spiking to an average loss amount of more than $236,000 in 1H 2023, businesses with more than $100 million in revenue saw severity nearly cut in half — though still a 21% increase YoY (Figure 1.5). The significant changes in severity among this cohort are attributable to spikes in ransomware severity in the first half of the year. Severity among businesses with under $25 million in revenue increased 10% YoY, while businesses between $25 million and $100 million saw severity increase by 9%.

The uptick in overall claims frequency and severity among Coalition policyholders[4] is indicative of industry-wide trends, though far less volatile than the pandemic-era ransomware boom in 2021. Our rigorous security and underwriting standards provide us with a holistic outlook on cyber risk. We use our claims data to continuously refine our outlook on risk and support businesses as they address cyber risks prior to binding a policy and throughout the policy period.

4. *Insurance products in the United States are offered through Coalition Insurance Solutions, Inc., a licensed insurance producer with its principal place of business in San Francisco, CA (Cal. license #0L76155), acting on behalf of a number of insurance companies and an affiliate of Coalition, Inc.*

Boundary Devices Targeted by Threat Actors

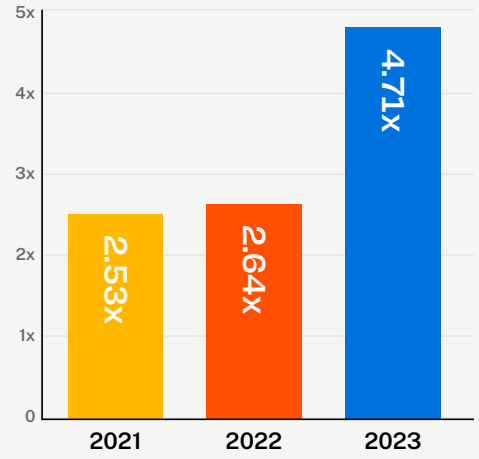
When businesses use a boundary device to protect their network and adhere to best practices to update firmware and monitor all endpoints, they can react quickly if the boundary device has been compromised.

The technologies critical to business operations are often prime targets for threat actors. This is especially true of boundary devices, such as routers, firewalls, and virtual private networks (VPNs), that sit between a business and the public internet.

However, boundary devices are also critical tools in reducing a business' attack surface and protecting other types of risky technology. This is the case with Remote Desktop Protocol (RDP), a protocol used for hosts to communicate. When a boundary device does not secure remote access, it can increase the risk of a business experiencing a cyber attack.

When businesses use a boundary device to protect their network and adhere to best practices to update firmware and monitor all endpoints, they can react quickly if the boundary device has been compromised.

Cisco ASA Relative Claims Frequency
(Figure 2.1)



Cisco Adaptive Security Appliance

Cisco Adaptive Security Appliance (ASA) devices facilitate remote access and protect networks through a combination of firewall, antivirus, intrusion prevention, and VPN capabilities. Due to the risk associated with these devices, Coalition routinely scans policyholders for exposed Cisco ASA web panels.

The relative claims frequency for policyholders using Cisco ASA surged in 2023. **Businesses with internet-exposed Cisco ASA devices were nearly five times more likely to experience a claim in 2023** (Figure 2.1).

Several critical vulnerabilities impacting Cisco ASA devices were discovered in 2023, likely contributing to the increased relative frequency. Security researchers discovered that the ransomware gang Akira was actively exploiting a Cisco ASA vulnerability from 2020, which posed a significant risk for businesses that has continued into 2024.[5]

CASE STUDY

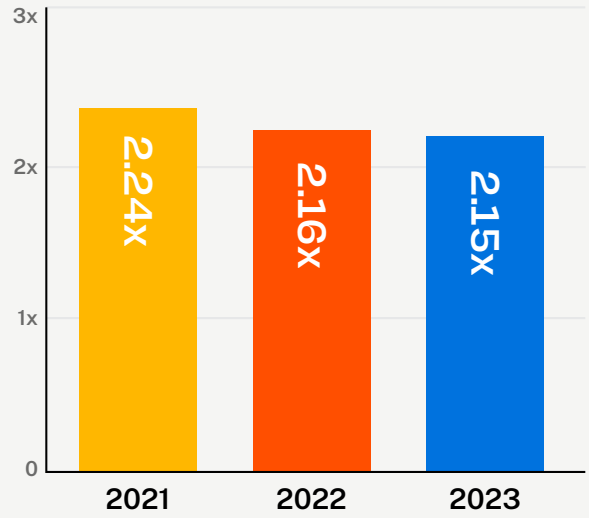
Coalition Helps Firm Locate Vulnerable Boundary Device Exploited in Ransomware Attack

A financial firm using a Cisco ASA device called Coalition to report a ransomware event. Coalition Incident Response[6] (CIR) investigated the matter but was unable to determine the root cause because the firm did not have good logging in place. Around the same time, Coalition learned the Akira ransomware gang was using an old vulnerability to compromise Cisco ASA devices, so we began rapidly scanning the internet for vulnerable businesses.

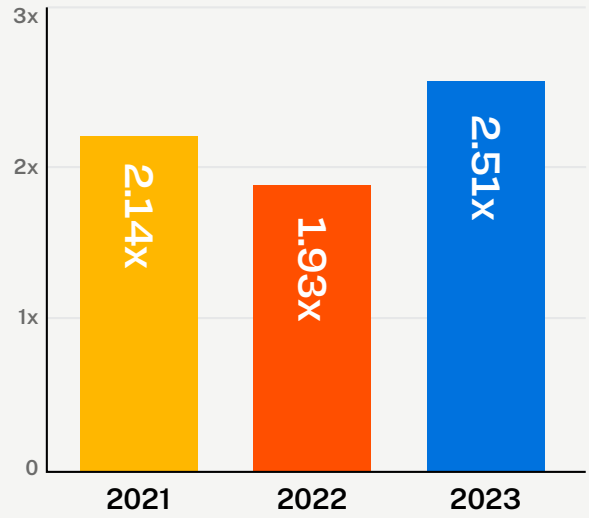
Coalition Security Labs, our in-house team of security researchers, used proprietary scanning technology to successfully locate the SSL VPN login for the financial firm's vulnerable boundary device. This device was determined to be the likely source of compromise, which led to the ransomware attack. Armed with the new information, CIR continued its forensic investigation and remediation efforts, then worked with our claims team and breach counsel to help the firm evaluate its exposures and the ransom demand. Ultimately, the financial firm decided it was necessary to obtain a decryption key, and CIR engaged with the threat actor to negotiate a ransom payment.*

5. *Truesec, Akira Ransomware and Exploitation of Cisco Anyconnect Vulnerability CVE-2020-3259*
6. *Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.*

Fortinet Relative Claims Frequency *(Figure 2.2)*



RDP Relative Claims Frequency *(Figure 2.3)*



Businesses with internet-exposed Fortinet devices were twice as likely to experience a claim in 2023.

Fortinet

Fortinet offers a variety of boundary devices that are often targeted and exploited by threat actors due to the level of privileged access that can be gained by compromising them. **Businesses with internet-exposed Fortinet devices were twice as likely to experience a claim in 2023** (Figure 2.2).

The relative claims frequency associated with Fortinet devices has remained a stable, persistent risk YoY. Several critical vulnerabilities in Fortinet devices were discovered in 2023 and in early 2024, and the likelihood of policyholders experiencing a claim may increase throughout the year.[7]

Remote Desktop Protocol

RDP is a remote access solution built into Windows. Given its ubiquity, RDP is frequently targeted by threat actors who scan the internet looking for exposed instances to exploit. After a decrease in 2022, the risk associated with RDP surged in 2023. **Policyholders using internet-exposed RDP were 2.5 times more likely to experience a claim in 2023** (Figure 2.3).

Traffic from threat actors scanning for RDP grew in 2023. Coalition honeypots detected a 59% increase in unique IP addresses scanning for RDP between January and October 2023.[8]

7. *Coalition, FortiOS SSL VPN Vulnerability Actively Exploited in the Wild*
8. *Coalition, Cyber Threat Index 2024*

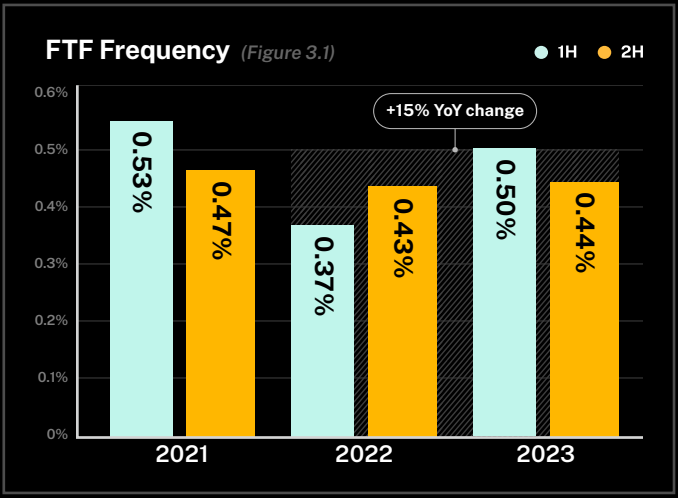
Funds Transfer Fraud Counteracted by Clawbacks

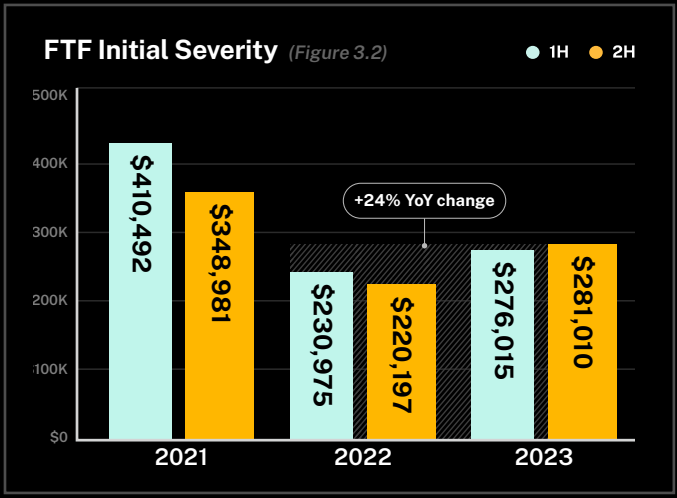
"Consumers reported losing more money to bank transfers and cryptocurrency than all other methods combined."

-FEDERAL TRADE COMMISSION

FTF is a low-effort, high-reward way to monetize cybercrime. According to the Federal Trade Commission (FTC), $10 billion was lost to fraud in 2023, with reports of imposter fraud soaring: "Consumers reported losing more money to bank transfers and cryptocurrency than all other methods combined."[9]

FTF frequency increased 15% YoY (Figure 3.1). Despite the increase, FTF frequency remains relatively flat over time, as the spike in 1H 2023 neared a historic high. Given the ease with which threat actors execute these attacks, we expect FTF to continue hovering at its current frequency.





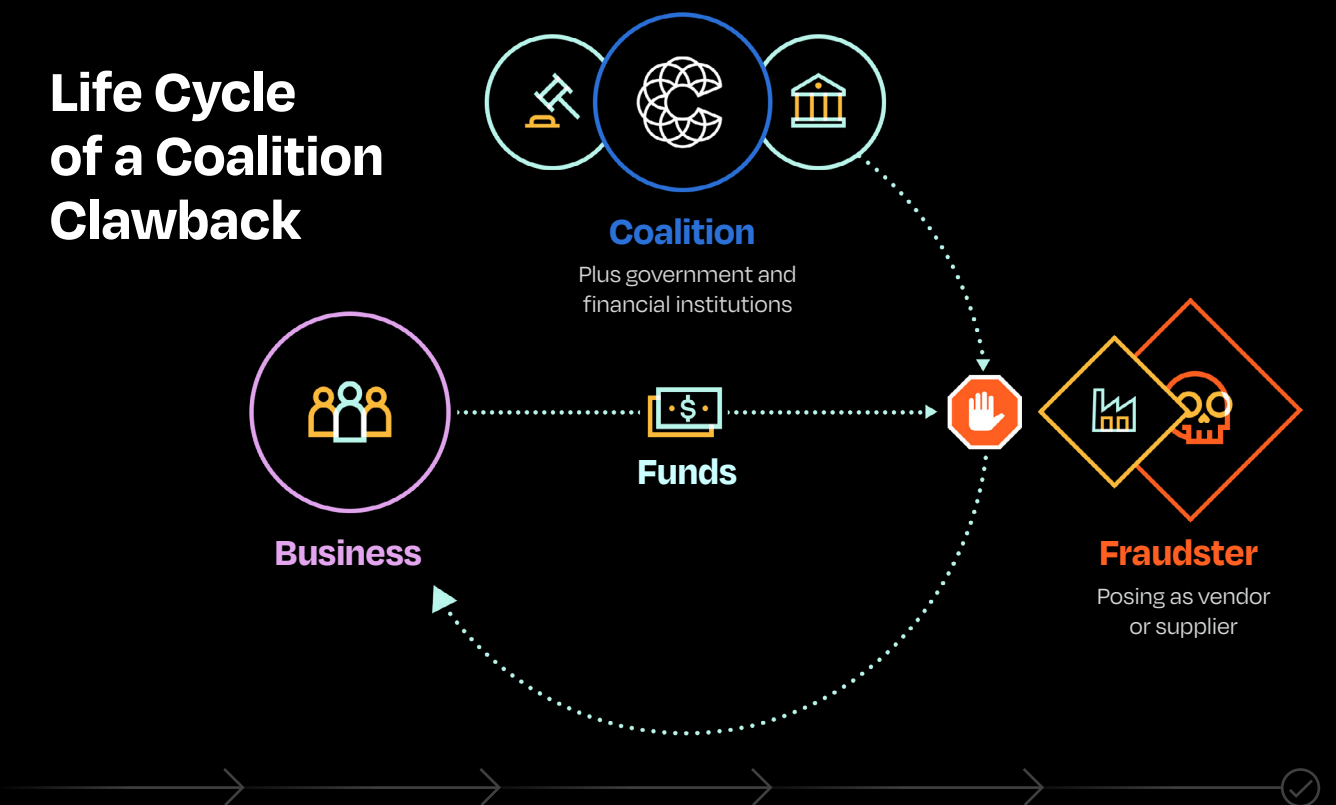
9. *Federal Trade Commission, As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public*

FTF initial severity increased 24% YoY to an average loss of more than $278,000.

Cybersecurity trends point to threat actors using generative artificial intelligence (AI) tools to launch more sophisticated attacks. Phishing emails are becoming more credible and harder to detect, and threat actors are believed to be using AI to parse information faster, communicate more efficiently, and generate campaigns targeted toward specific companies — all of which may contribute to increases in FTF claims.

FTF initial severity increased 24% YoY to an average loss of more than $278,000 (Figure 3.2). FTF initial severity is calculated prior to recovery activities. For businesses that have unwittingly transferred large sums of money to a threat actor, recovery is their primary concern. Policyholders that report the loss quickly to Coalition have a greater likelihood of recovery.

Life Cycle of a Coalition Clawback



Over the years, Coalition has clawed back more than $80 million for policyholders.

Coalition Clawbacks

Coalition helps businesses recover funds lost to FTF through relationships with U.S. government entities and financial institutions to stop payments and "claw back" stolen funds. This is a critical and time-sensitive process, as threat actors routinely transfer funds between multiple banks and across jurisdictions to cover their tracks.

Coalition successfully clawed back more than $38 million in fraudulent transfers in 2023. In instances where recovery was successful, we recovered an average amount of $470,000 per FTF claim in 2023. Over the years, Coalition has clawed back more than $80 million for policyholders.

Clawbacks in 2023

$38M
Total FTF recovery

$470K
Average amount recovered per FTF claim when recovery was successful

46%
FTF events with a full recovery when recovery was successful

102%
Increase in total FTF recovery amount since 2022

CASE STUDY

Coalition Claws Back $4.9M From Overseas Transfer

A real estate firm contacted Coalition after paying a fraudulent invoice. The firm's vendor had been compromised by a threat actor who emailed instructions to wire a $4.9 million payment to a bank account they controlled in Hong Kong. Within days of the initial transfer, Coalition helped the firm file a report with the FBI, and law enforcement agencies froze the funds before the threat actor could transfer the money to another account. Thanks to the firm's timely reporting and our experienced claims team, Coalition successfully clawed back all $4.9 million of the stolen money.*

Ransomware Severity Increased Amid Volatile Year

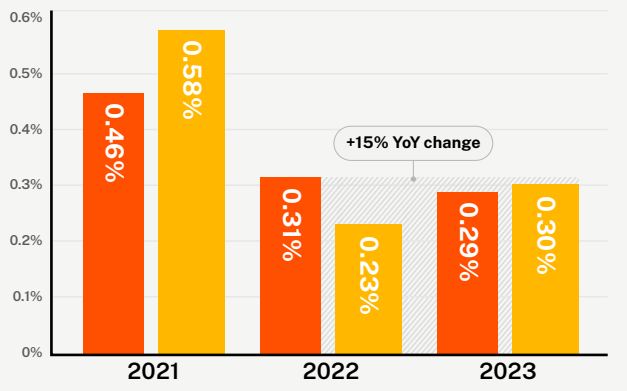
As ransomware payments hit $1 billion globally, Coalition's ransomware severity dropped 54% in the latter half of the year to an average of nearly $170,000.

Ransomware remains a pain point for businesses and governments alike. Over the past few years, threat actors have turned to ransomware as a lucrative method for monetizing their crimes, and in 2023, ransomware payments hit historic highs.

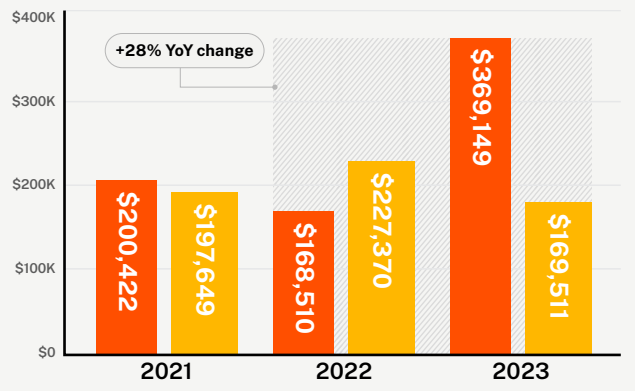
Ransomware frequency increased by 15% YoY, largely due to a sharp uptick in frequency in the first half of the year (Figure 4.1). The uptick in frequency follows historic lows from the previous year, especially 2H 2022. Ransomware frequency has seen sharp peaks and valleys over time, which may be attributable to law enforcement efforts to takedown individual ransomware gangs.

Ransomware severity increased 28% YoY for an average loss of more than $263,000 — but 2023 was truly a tale of two halves (Figure 4.2). Following historic lows in 2022, ransomware severity spiked in 1H 2023 to more than $369,000. However, as ransomware payments hit $1 billion globally, Coalition's ransomware severity dropped 54% in the latter half of the year to an average of nearly $170,000.

Ransomware Frequency *(Figure 4.1)*



Ransomware Severity *(Figure 4.2)*



The average ransom demand increased 36% YoY to an average of nearly $1.4 million (Figure 4.3). Among policyholders that experienced a ransomware incident, 40% opted to pay a ransom, deeming it reasonable and necessary. Among ransomware claims that resulted in a payment, Coalition successfully negotiated the amount down by an average of 64% of the original demand.[10]

Ransom payments factor into the costs that underpin ransomware claims severity but are only a portion of the total expense. Other costs associated with the incident response for ransomware claims include: forensic investigation and related data mining, recovery and remediation, notifications, breach counsel, business interruption, exposure to legal action, litigation, regulatory activity, and public relations impact.

DISPELLING MYTHS ABOUT RANSOMWARE PAYMENTS

Paying a ransom is a complex decision for any business. While paying every ransom is not the answer, a blanket ban is impractical. Proponents of a ransomware payment ban often say cyber insurers are part of the problem, suggesting they pay ransoms as an easy way out or view insurance as a substitute for security investments. These myths can undermine collaboration between insurers and policymakers and drive responses that exacerbate the problem.

Myth 1: Cyber insurers pay ransoms to save money

Critics say cyber insurers pay ransoms because it's cheaper than incurring the other business disruption costs. However, insurers often incur higher incident costs than the initial ransom demand, spending more on crisis response and recovery expenses.[11] Data shows that a fraction of claims costs go toward ransom payments because insurance providers prioritize and fund strategies to avoid paying.

Myth 2: Cyber insurers are undermining resilience

A ransom payment ban might make sense if businesses were at a reasonable level of cybersecurity maturity, especially if cyber insurance providers were making businesses more likely to pay the ransom. Yet, the number of businesses that opted to pay declined from 80% in 2019 to a record low of 31% in 2023.[12]

Myth 3: Cyber insurers have encouraged the ransomware epidemic

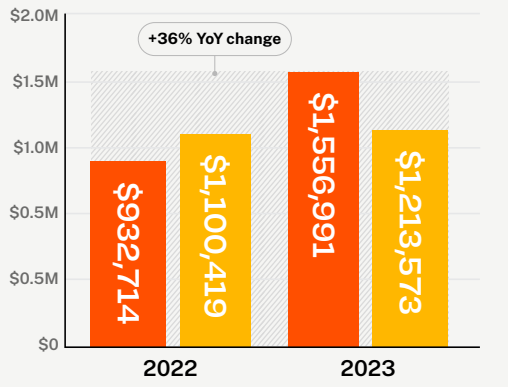
Naysayers focus on how cyber insurance providers shape negotiation strategies, but studies show the industry had a neutral impact.[13] If anything, insurers have been actively reducing the rate of compromise to prevent infections that force the payment decision.

A ransomware payment ban is not the answer

Complex problems are rarely solved with binary solutions; ransomware is no different. A payment ban would limit options available to victims with little evidence that doing so will end the ransomware problem. The government already has a policy lever to ban payments to ransomware gangs, which Coalition supports and enforces. In all other cases, we support policyholders in making the decision for themselves based on their situations.

10. Decrease in ransom amount paid only includes negotiations handled by Coalition Incident Response, an affiliate firm made available to all policyholders via panel selection.
11. NetDiligence, Cyber Claims Study 2023 Report
12. Coveware, New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying
13. Royal United Services Institute, Cyber Insurance and the Ransomware Challenge

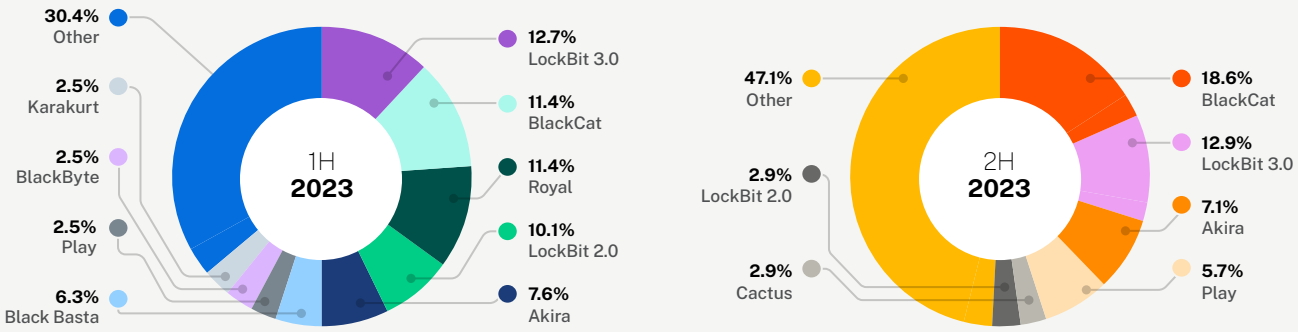
Ransom Demands *(Figure 4.3)*



Ransomware Variants

Expectedly, the ransomware variants that drove losses shifted. LockBit ransomware had two variants that appeared in the second half of the year (Figure 4.4). Among Coalition policyholders, LockBit 3.0 accounted for 12.9% of all ransomware claims and LockBit 2.0 accounted for 2.09% of claims. Notably, the LockBit ransomware gang was briefly taken offline by law enforcement in early 2024 before reappearing three days later.[14]

Ransomware Variants *(Figure 4.4)*



CASE STUDY

Business Merger Leads to Costly Ransomware Attack

A construction business fell victim to a ransomware attack despite having endpoint detection and response (EDR) to alert on anomalous activity in its network. The business had recently acquired a subsidiary and failed to perform sufficient due diligence on the subsidiary's security controls during the merger. A salesperson clicked on a phishing link that enabled a threat actor to breach the subsidiary and move laterally to compromise the construction business. The threat actor demanded a ransom of nearly $1 million, for which CIR helped negotiate a reduced payment.*

14. *The Record, LockBit ransomware gang attempts to relaunch its services following takedown*

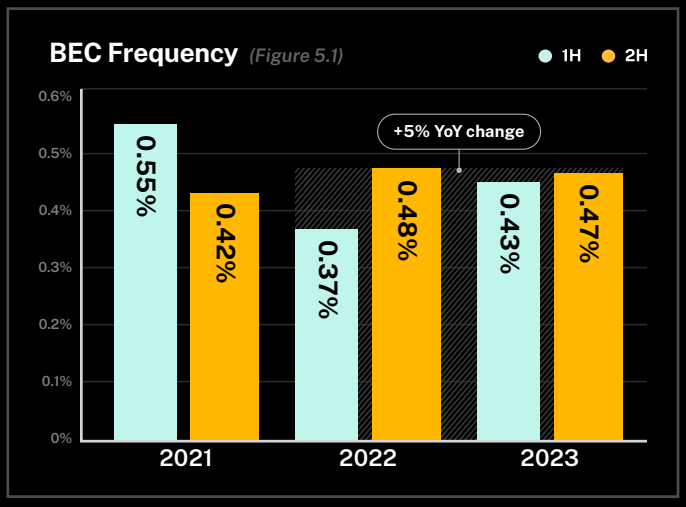
Business Email Compromise Remained Stable

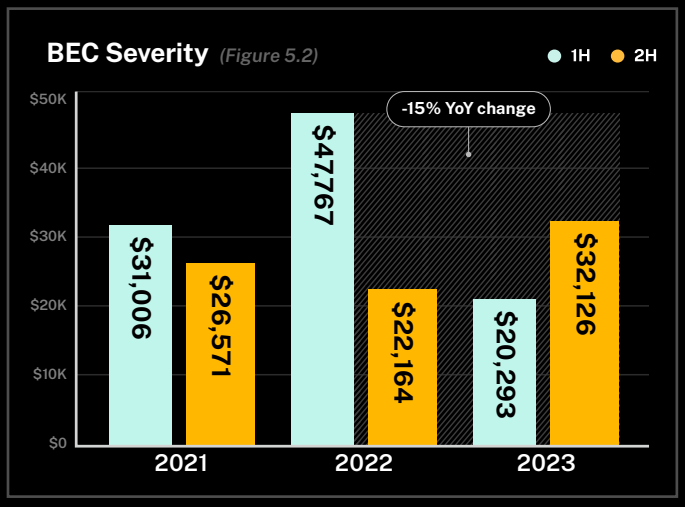
With the exception of 1H 2022, BEC severity has remained stable over time, a trend we anticipate continuing.

Threat actors want to get paid. When compromising an email inbox,they often search for terms that will help uncover vendor or payment information. If the compromise results in a fraudulent wire transfer, the event is classified as FTF rather than BEC. However, threat actors may gain access to the inbox of a user who lacks access to financial systems, in which case they typically wait inside the network and send phishing emails to compromise a user with direct access to money.

BEC frequency has been relatively stable over time and is likely to remain as such, despite a 5% YoY increase (Figure 5.1). However, some variance is inevitable because many BEC attacks evolve into FTF claims.

BEC severity decreased 15% YoY to an average loss of more than $26,000 (Figure 5.2). With the exception of 1H 2022, BEC severity has remained stable over time, a trend we anticipate continuing.





MOVEit Persisted as Third-Party Risk

'OTHER' EVENTS DEFINED

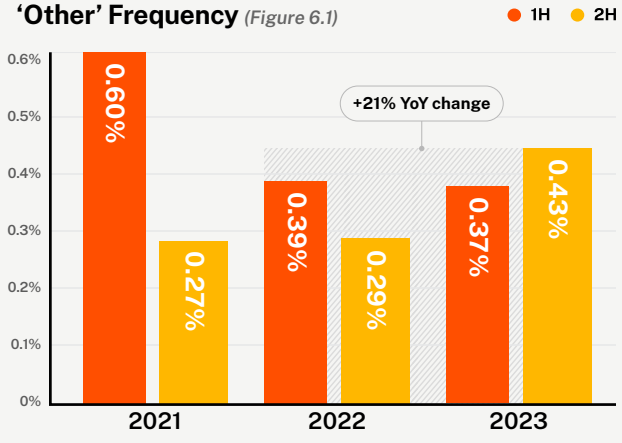
- **Errors, Misuse, and Theft:** Misuse of business assets, inappropriate handling of information, and physical theft of assets
- **Legal, Privacy, and Media:** Intentional or unintentional violations of privacy policies or other legal proceedings
- **Non-encryption System Compromise:** A system compromise that is neither ransomware nor BEC
- **Third-party Compromise:** A vendor, supplier, or other organization is compromised

Cybercrime is a diverse ecosystem. While claims like ransomware and FTF can have devastating consequences, threat actors have other ways to adversely impact businesses. Coalition categorizes claims events that did not result in ransomware, FTF, or BEC as "Other."

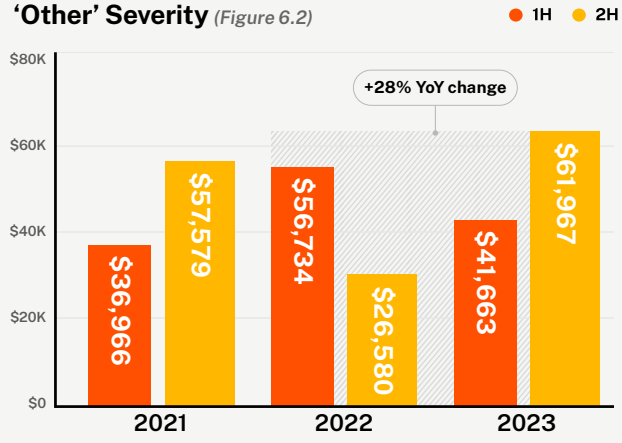
Claims frequency for Other events increased by 21% YoY (Figure 6.1). Claims severity for Other events increased by 28% to an average loss of more than $53,000 (Figure 6.2).

Most of these events were Non-encryption System Compromise claims, which are similar to other cybercrimes that start with stolen or purchased credentials. Threat actors attempt to use these credentials to gain authenticated access to a network. The divergence occurs when threat actors find and exfiltrate sensitive information to sell on the dark web or attempt to ransom the business, as opposed to encrypting the network or looking for financial data.

'Other' Frequency *(Figure 6.1)*



'Other' Severity *(Figure 6.2)*



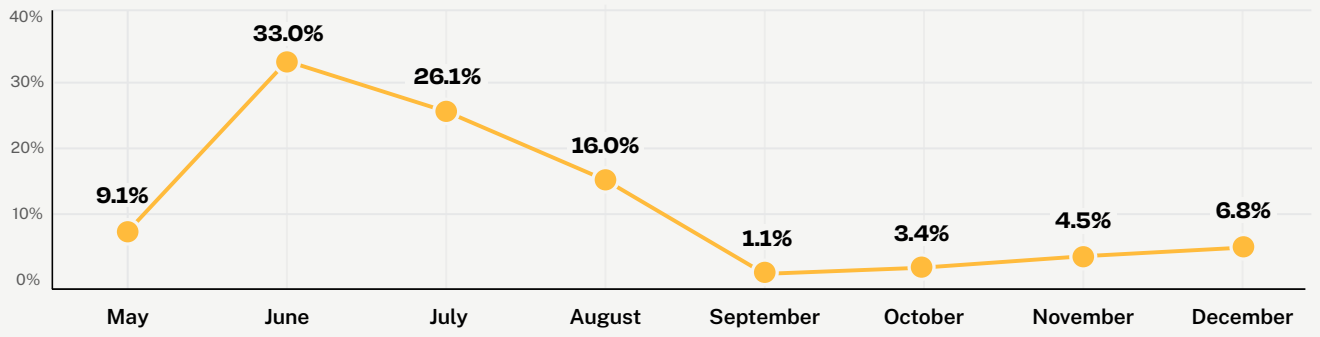
Despite the initial disclosure taking place in mid-2023, Coalition policyholders continued to experience cyber incidents related to MOVEit well into the latter half of the year.

The most notable third-party compromise event pertains to MOVEit.[16] Progress Software disclosed a critical vulnerability in the file transfer program in May. The Cl0p ransomware gang likely exploited the vulnerability prior to disclosure and used it to compromise hundreds of organizations, publishing their data through the Cl0p ransomware leak site.[17]

Despite the initial disclosure taking place in mid-2023, Coalition policyholders continued to experience cyber incidents related to MOVEit well into the latter half of the year (Figure 6.3).

Incidents related to MOVEit contributed to the increase in severity among Other events.[18] Many of the incidents were due to third-party compromise, in which the vendors or suppliers of our policyholders were directly compromised.

MOVEit Incidents in 2023 *(Figure 6.3)*



16. *Progress Software, MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*
17. *Kroll, Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*
18. *Incident defined as an adverse cyber event reported to Coalition by a policyholder that may or may not evolve into a cyber claim. Unless otherwise noted, a claim is an incident that incurred a gross loss.*

Mitigating Cyber Risk with an Active Partner

Good cyber hygiene and strong security controls remain the strongest tools to protect against these familiar cyber attacks.

The volatility of the cyber threat landscape is inevitable. The frequency and severity of cyber claims continued to trend upward in 2023, yet Coalition found success in minimizing the impact through data-driven risk selection and active engagement with policyholders.

Ransomware may have declined in the latter half of the year, but we cannot herald its defeat. We believe threat actors will pivot their tactics and remain persistent, as the financial incentive of these attacks is too strong to abandon. Similarly, the easy-to-execute nature of FTF and BEC makes these attacks mainstays of the cybercrime economy.

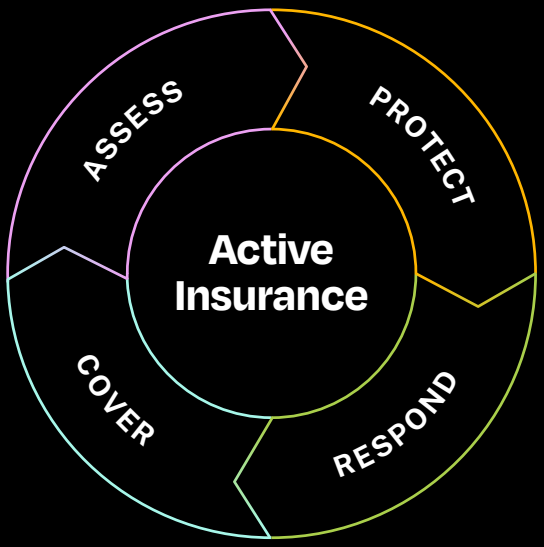
Good cyber hygiene and strong security controls remain the strongest tools to protect against these familiar cyber attacks. We continue to see a direct correlation between the technologies businesses use and the risks associated with cyber insurance claims. Security controls and services, like multi-factor authentication (MFA) and managed detection and response (MDR), can help businesses stay one step ahead of threat actors.

Coalition sits at the intersection of security and insurance. Our robust data on cyber threats and claims allow us to create a comprehensive picture of real-time risk, which is continuously refined with proprietary claims and underwriting data. The depth and breadth of this data gives us a unique vantage point on cyber risk, while proactive alerts help businesses prioritize and respond to the cyber threats that pose the greatest risk to their operations.

Why Modern Businesses Choose Coalition

Our mission at Coalition is to help protect the unprotected. As the world continues to digitize, we actively partner with businesses to help them stay one step ahead of digital risk. Coalition's Active Insurance is the first cyber defense bringing together active cyber risk assessment, proactive protection, expert response, and comprehensive cyber coverage. We share the insights in this report to help empower others in the face of growing cyber risks.

Hundreds of thousands of businesses protect their businesses with Active Insurance. While other cyber insurance providers wait for a claim to engage, we use data and security insights to partner with businesses and help mitigate digital risks. Our comprehensive cyber coverage, innovative security tools, and world-class claims handling allows policyholders to focus on growing their business with protection and greater peace of mind.



Prevent risk before it strikes with Active Insurance

ASSESS
Real-time, external view of cyber risk with customized recommendations

PROTECT
Identify and prevent new threats with tailored remediation guidance and support

COVER
Comprehensive coverage to give peace of mind following an attack

RESPOND
Immediate expert support to minimize impact and speed up recovery

Want to work with us?
Become an appointed broker

Looking for help?
Get matched with a broker

Curious about your risk?
Get a free risk assessment

Methodology

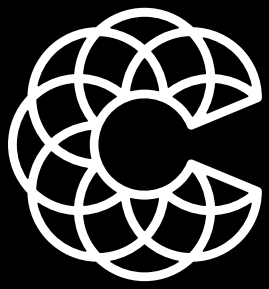
The 2024 Cyber Claims Report is based on reported claims data from January 1 to December 31, 2023. A claim is defined as an adverse cyber event reported by a Coalition policyholder that incurred a gross loss. Our team of data scientists and actuaries used our own internal claims data to complete the analysis.

Coalition uses the reported experience as of six months of age rather than ultimate loss projections. Ultimate loss is the total sum paid by the policyholder and its insurers. As a projection, ultimate loss can change over time due to future loss development. By comparing reported experience evaluated at the same age, we assume the same ultimate development between all periods, allowing for a direct comparison without the bias of future trends skewing the ultimate projections.

Our methodology was first introduced in the 2023 Cyber Claims Report: Mid-year Update and has been retroactively applied to Coalition's historical data. This allows us to highlight the trends in cyber claims impacting Coalition policyholders. In doing so, overall claims frequency and severity data from prior reports, as well as data for specific event types, may have changed. For example, we updated our reporting on cyber incidents related to MOVEit as activity continued throughout the second half of 2023.

Correlational risk related to the use of specific technologies or products is calculated as relative claims frequency. The relative claims frequency for a given segment of policies represents the risk multiple of claims frequency for that segment relative to the claims frequency across all policies. For example, a 1.5 relative claims frequency for all policies with a given risk characteristic suggests said risk characteristic leads to a claim frequency 1.5 times higher than average.

The purpose of this report is to share timely data with brokers, policyholders, and others in our industry. Shifts in the cyber threat landscape pose a real risk to all businesses. Our methodology allows us to gather and publish cyber claims data faster. As a general practice, please reference our most recent reports when possible, as the current methodology is our standard for reporting cyber claims trends moving forward.



Coalition®

coalitioninc.com

548 MARKET STREET, #94729
SAN FRANCISCO, CA 94104