Coalition®

2025 Cyber Claims Report

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

Table of Contents

Executive Summary

Cyber risk remains an unavoidable reality of doing business in a digitally connected world. Threat actors continue to demonstrate their relentlessness, evolving tactics to exploit new vulnerabilities and maximize financial gain.

In years past, Coalition witnessed this dynamic firsthand with cyber claims increasing in both frequency and severity across various industries and revenue segments. Yet in 2024, despite this ever-changing landscape, we observed remarkable year-over-year (YoY) stability, a clear testament to the power of Active Insurance.

What sets Active Insurance apart from others is our strategic underwriting, data-driven risk selection, real-time risk assessment, proactive policyholder engagement, rapid response times, human expertise, comprehensive coverage, and passion for going above and beyond the policy. **This unique combination is why Coalition policyholders experience 73% fewer claims than the industry average.**[1]

Having engaged policyholders that regard cyber risk as an ongoing priority rather than a one-time concern is not coincidental: It's a direct outcome from a novel approach. Businesses that recognize cyber insurance is more than just financial protection — but a true partnership in risk management — are proving to be more resilient in the face of evolving threats.

The most successful businesses are those that proactively invest in security controls, leverage access to real-time threat intelligence, and take action based on emerging risks rather than past events. The end result? Fewer attacks, less financial burden, and a stronger security posture.

Looking ahead, the path forward is clear: Prevention must be prioritized over reaction. The companies that embrace continuous cybersecurity improvements, strategic risk management, and early threat detection will be best positioned to withstand future attacks.

Meanwhile, Coalition recognizes that we must never be complacent. Instead, we continuously refine our own approach by leveraging predictive analytics, deepening our trust with policyholders and brokers, and introducing meaningful security solutions into every stage of the insurance lifecycle.

The future of cyber insurance will be shaped by the businesses, brokers, and insurance providers who choose to take action. Those who do will not only endure but emerge stronger.

About the 2025 Cyber Claims Report

This report features statistics, charts, and risk insights based on data from Coalition policyholders in the United States, Canada, the United Kingdom, and Australia. Cyber risk is a global matter, and the trends and risk mitigation strategies in this report are widely relevant and applicable across all geographic regions. Coalition is proud to share these insights to help businesses, brokers, and security professionals stay informed about the ever-changing cyber threat landscape.

1. *Industry average based on data reported by US insurers to the National Association of Insurance Commissioners (NAIC). Comparison performed using 2023 claims frequency data from Coalition and NAIC. Claims 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.*

Key Findings

GLOBAL HIGHLIGHTS

-7%
Decrease in claims frequency

$115K
Average loss amount

60%
Claims due to BEC and FTF

BUSINESS EMAIL COMPROMISE

+23%
Increase in claims severity

$35K
Average loss amount

29%
BEC events that resulted in FTF

FUNDS TRANSFER FRAUD

-46%
Decrease in claims severity

$185K
Average initial loss amount

$31M
Total recoveries via “clawback”

RANSOMWARE

-7%
Decease in claims severity

$292K
Average loss amount

60%
Ransom reduction via negotiation

THE POWER OF ACTIVE INSURANCE

73%
Fewer claims than industry average

56%
Reported matters handled at no added cost to policyholders

32K+
Security issues resolved by policyholders

Global Highlights

Claims frequency decreased as email-based attacks persisted

As cyber threats continue to evolve, businesses that take a proactive approach to managing and mitigating risk are experiencing the greatest successes. In fact, 56% of all matters reported to Coalition were handled without any out-of-pocket payments by the policyholder.

Global claims frequency decreased 7% YoY in 2024 to 1.48% with a notable dip in the latter half of the year (Figure 1.1). Claims frequency in the US was higher (1.54%) than the global average in 2024. Frequency in Canada was notably lower (1.13%), as was frequency in the UK (1.09%).

Global claims severity remained stable YoY in 2024 with an average loss amount of $115,000, a significant amount for organizations of all sizes (Figure 1.2). Claims severity in the US was lower ($108,000) than the global average in 2024. Severity in Canada was nearly double the global average ($226,000), while the UK was significantly lower ($35,000). Across all regions, severity continued to be driven by ransomware, the most costly and disruptive of all cyber attacks.

Frequency & Severity Explained

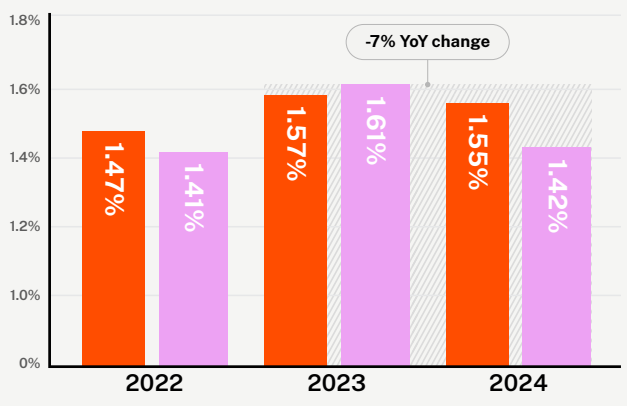
Claims frequency refers to how often insurance claims are filed over a period of time.

Claims severity refers to the average cost per insurance claim.

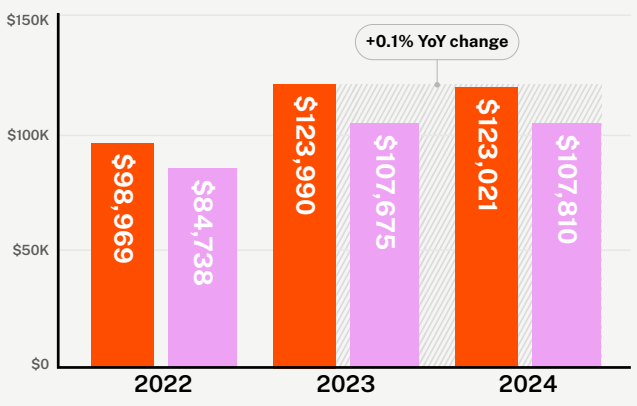
Frequency and severity data can help businesses, brokers, and insurance providers determine the likelihood and financial impact of cyber attacks, as they are strong indicators not only of threat actor behaviors but also the collective security posture of organizations.

56% Matters reported to Coalition that were handled without any out-of-pocket payments by the policyholder

Global Claims Frequency *(Figure 1.1)*

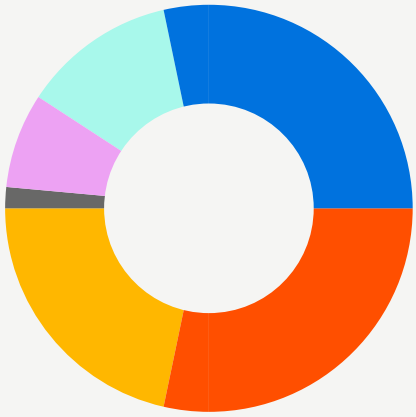


Global Claims Severity[2] *(Figure 1.2)*



2. *Global claims severity includes funds transfer fraud (FTF) events in which a recovery was made. For additional insight into initial FTF claims severity, see Page 13. For more information, please see Methodology.*

Claims by Event Type *(Figure 1.3)*



29.8%	FTF	**11.8%**	Misc. First-Party Loss
29.7%	BEC	**1.4%**	Third-Party Allegations
6.2%	Other	**21.1%**	Ransomware

Email-based attacks led the way

Email-based attacks were ever-present in 2024, as business email compromise (BEC) and funds transfer fraud (FTF) events accounted for 60% of all cyber insurance claims — a trend that has generally persisted for the past three years (Figure 1.3). Ransomware events continued to hover around 20% of all claims, though the devastating impact of these events were felt most in terms of severity.

The percentage of reported claims in the US were nearly identical to global averages, though other geographical regions saw noteworthy deviations. BEC (28.6%) and FTF (24.5%) events accounted for more than half of all claims in Canada, though ransomware events (29.6%) were more prevalent than in other geographies. In the UK, BEC (46.4%) was the leading event type by a considerable margin, with FTF (25%) and ransomware (17.9%) trailing behind.

Miscellaneous First-Party Loss & Third-Party Allegations

The 2025 Cyber Claims Report features two new event types: miscellaneous first-party loss and third-party allegations. Each of these categories encompasses a variety of event types. Miscellaneous first-party loss includes system failures, security failures, third-party breaches, and more; third-party allegations include copyright infringement, domain impersonation, privacy rights violations, and more. See pages 19-21 for additional details.

Claims by Industry

Sectors with less security awareness were more susceptible to attacks

Industries that handle sensitive financial data, personal health information, or intellectual property are often targeted by cyber criminals due to the high value of their data.

Industry plays a significant role in shaping a business' overall cyber risk, influencing both the frequency and severity of cyber insurance claims.

Industries that handle sensitive financial data, personal health information, or intellectual property are often targeted by cyber criminals due to the high value of their data. Industries tied to critical infrastructure may also face heightened risks from state-sponsored attacks and ransomware campaigns that can disrupt essential operations. Meanwhile, industries with lower cybersecurity awareness may be more susceptible to opportunistic attacks, like phishing and credential theft.

Understanding industry-specific risks can empower businesses to tailor their cybersecurity strategies to address the most pressing threats they face.

Consumer Discretionary

Businesses in the consumer discretionary industry (automotive, hotels, retail, etc.) experienced a 2% increase YoY in claims frequency in 2024 to 1.33%, consistent with the industry's average over the past three years. Claims severity for these businesses decreased 18% YoY to an average loss of $118,000. (See Figures 2.1 and 2.2 for all industries.)

Consumer Staples

Businesses in the consumer staples industry (agriculture, food and beverage, personal hygiene, etc.) experienced the highest claims frequency in 2024, increasing 17% YoY to 2.60% with an average of 2.29% over the past three years. Claims severity for these businesses plummeted 62% YoY to an average loss of $124,000, largely attributable to a sharp increase in the first half of 2023.

Energy

Businesses in the energy industry (electricity, oil and gas, renewables, etc.) saw a 6% YoY decrease in claims frequency in 2024 to 1.35%, part of a steady decline contributing to a three-year average of 1.44%. Due to volatility in the first half of 2024, claims severity for these businesses spiked more than 1,200% YoY to an average loss of $292,000, though historical severity sits around $108,000.

Financial Services

Businesses in the financial services industry (banks, investment firms, insurers, etc.) experienced a 17% YoY decrease in claims frequency in 2024 to 1.47% with an average of 1.53% over the past three years. Claims severity for these businesses decreased 2% YoY to an average loss of $95,000.

Healthcare

Businesses in the healthcare industry (hospitals, pharmacies, assisted care facilities, etc.) experienced a 19% YoY decrease in claims frequency in 2024 to 1.38% with an average of 1.45% over the past three years. Claims severity for these businesses increased 32% YoY to an average loss of $145,000.

Industrials

Businesses in the industrial industry (construction, manufacturing, engineering, etc.) saw a 4% YoY increase in claims frequency in 2024 to 1.64% with an average of 1.59% over the past three years. Claims severity for these businesses dipped 6% YoY to an average loss of $105,000, a figure that's commensurate with historical industry averages.

Information Technology

Businesses in the information technology industry (hardware, software, managed services, etc.) experienced a 13% YoY decrease in claims frequency in 202 to 1.36% with an average of 1.46% over the past three years. Claims severity for these businesses increased 11% YoY to an average loss of $131,000, primarily due to a notable spike in the first half of 2024.

Materials

Businesses in the materials industry (mining, chemicals, plastics, etc.) saw a 32% decrease in claims frequency in 2024 to 2.20%, contributing to stability after a significant spike in the second half of 2023, with an average of 2.63% over the past three years. Claims severity for these businesses increased 10% YoY to an average loss of $99,000.

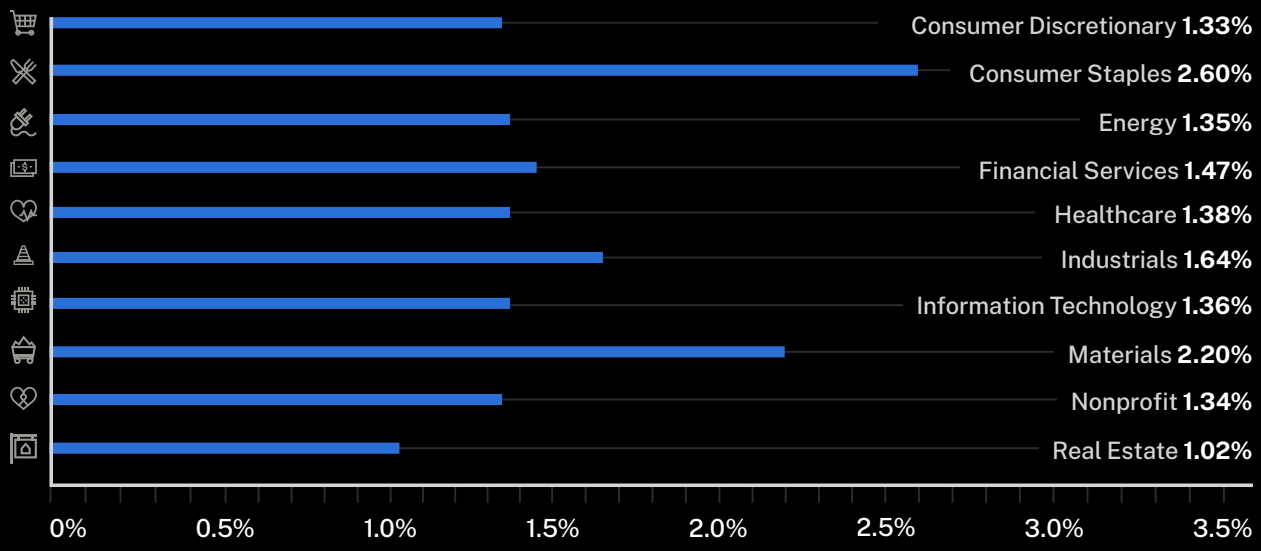
Nonprofit

Nonprofit organizations (charities, religious institutions, research facilities, etc.) saw a 1% YoY decrease in claims frequency in 2024 to 1.34% with a relatively steady average of 1.35% over the past three years. Claims severity for these organizations increased 12% YoY to an average loss of $73,000.

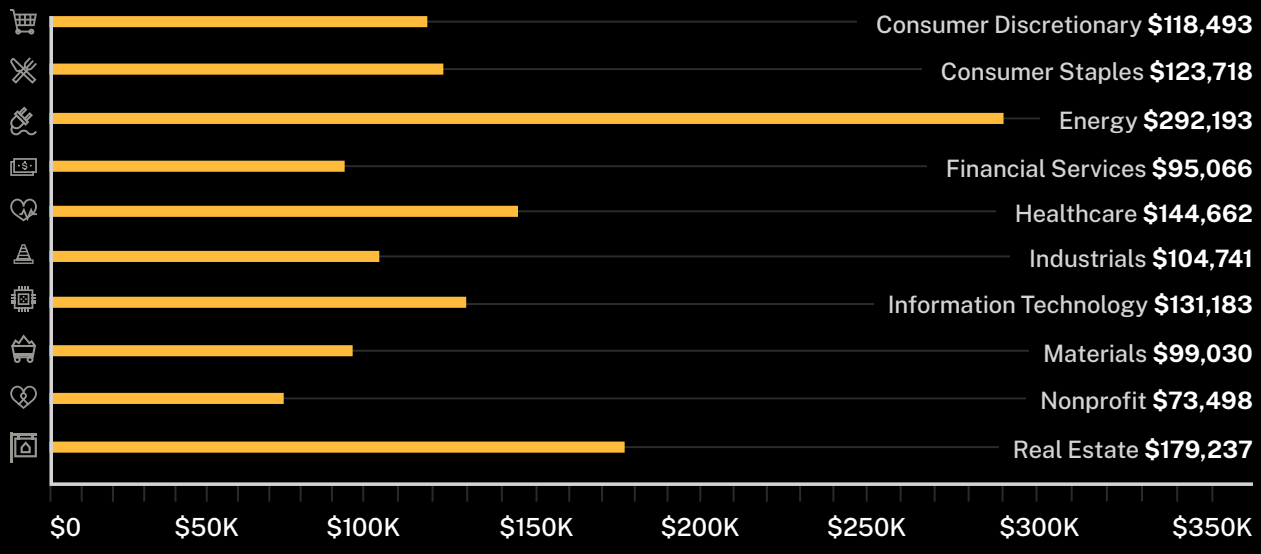
Real Estate

Businesses in the real estate industry (developers, property managers, brokerages, etc.) experienced a 24% decrease in claims frequency in 2024 to 1.02% with an average of 1.26% over the past three years. Claims severity for these organizations increased 58% YoY to an average loss of $179,000, largely driven by a spike in the first half of 2024.

Claims Frequency by Industry *(Figure 2.1)*



Claims Severity by Industry *(Figure 2.2)*



Claims by Revenue Amount

Frequency decreased year-over-year across all segments

Small and midsize businesses often face devastating financial consequences from cyber attacks due to limited resources and in-house security expertise.

Cyber risk impacts businesses differently based on their size, complexity, and resources. These factors have a direct influence on businesses' overall exposure, the types of threats they face, and their ability to recover after an incident.

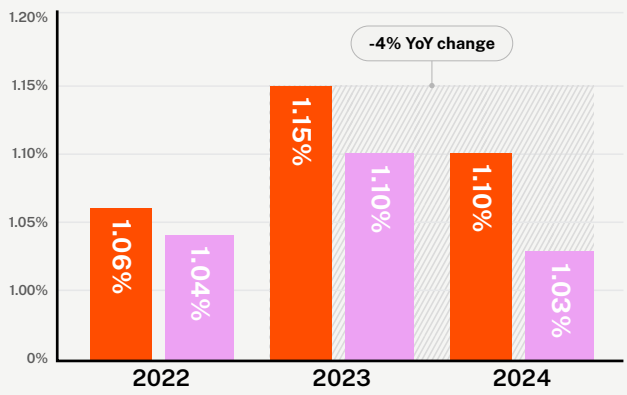
Small and midsize businesses (SMBs) often face devastating financial consequences from cyber attacks due to limited resources and in-house security expertise. Larger organizations, on the other hand, may have more sophisticated security programs but face highly targeted attacks due to their vast digital footprint and the volume of sensitive data they possess.

Cyber claims by revenue: Less than $25M

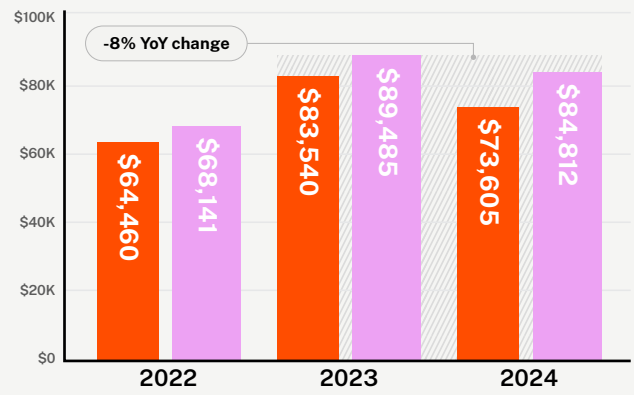
Claims frequency among businesses with less than $25 million in revenue (<$25M) decreased 4% YoY in 2024 to 1.07%, averaging out to 1.08% over the past three years (Figure 3.1). Although they experienced the lowest frequency of all revenue amounts, businesses <$25M in revenue represented 64% of total claims in 2024.

Businesses <$25M in revenue experienced an 8% YoY decrease in claims severity in 2024 to an average loss of $79,000 (Figure 3.2). The trend was primarily driven by a dip in the first half of the year, though the average loss amount remained stable over a three-year period.

Claims Frequency: <$25M *(Figure 3.1)*



Claims Severity: <$25M *(Figure 3.2)*



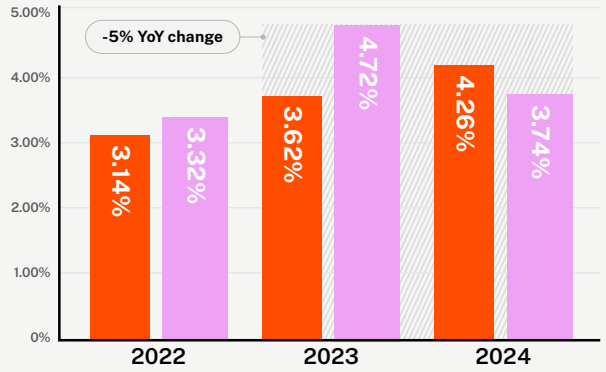
Cyber claims by revenue: $25M-$100M

Among businesses between $25 million and $100 million in revenue ($25M-$100M), claims frequency decreased 5% YoY in 2024 to 3.99% for a three-year average of 3.87% (Figure 3.3). This segment has seen greater volatility in frequency in recent years and represented 20% of total claims in 2024.

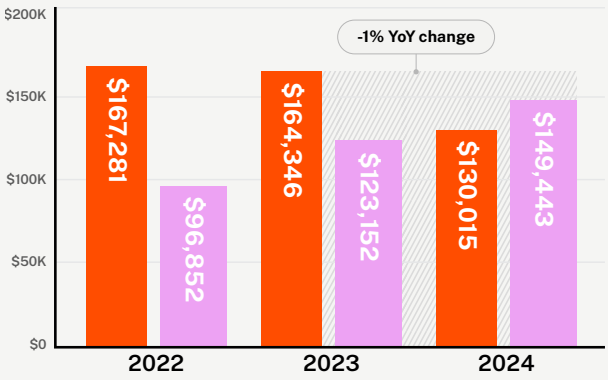
Claims severity among businesses $25M-$100M in revenue decreased 1% YoY in 2024 to an average loss of $139,000 (Figure 3.4). The slight decline was attributable to a higher-than-normal severity in the first half of 2023, though severity has been trending upward in recent months.

Claims Frequency: $25M-$100M

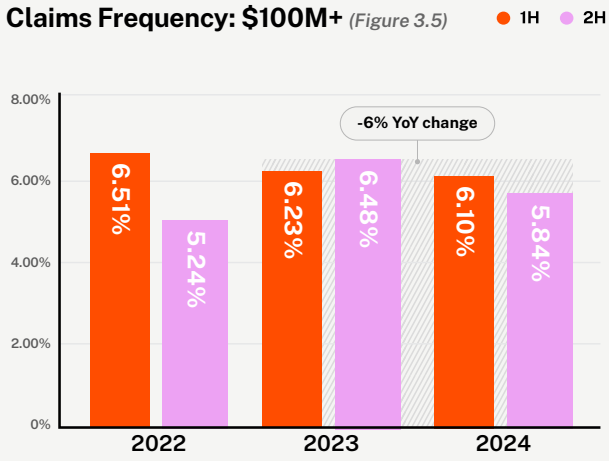
(Figure 3.3)



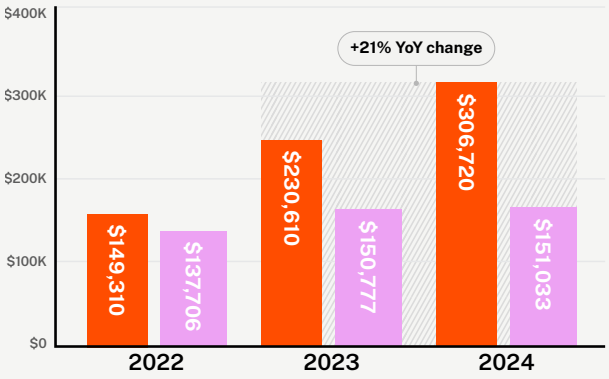
Claims Severity: $25M-$100M *(Figure 3.4)*



Claims Frequency: $100M+ *(Figure 3.5)*



Claims Severity: $100M+ *(Figure 3.6)*



Cyber claims by revenue: $100M+

Businesses with more than $100 million in revenue ($100M+) experienced a 6% YoY decrease in claims frequency in 2024 to 5.97% with an average of 6.06% over the past three years (Figure 3.5). Despite the dip in frequency, larger businesses experienced claims more often than their smaller counterparts.

Claims severity among businesses with $100M+ in revenue jumped 21% YoY in 2024 to an average loss of $228,000 (Figure 3.6). The increase was driven by a significant spike in the first half of the year and a considerable drop in the second half, a trend that's persisted over the past two years.

Business Email Compromise

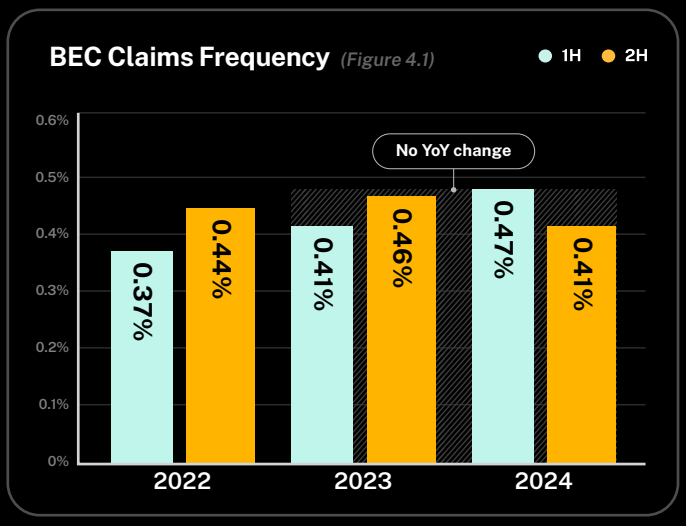
Spike in severity partly driven by prices related to mitigation & recovery

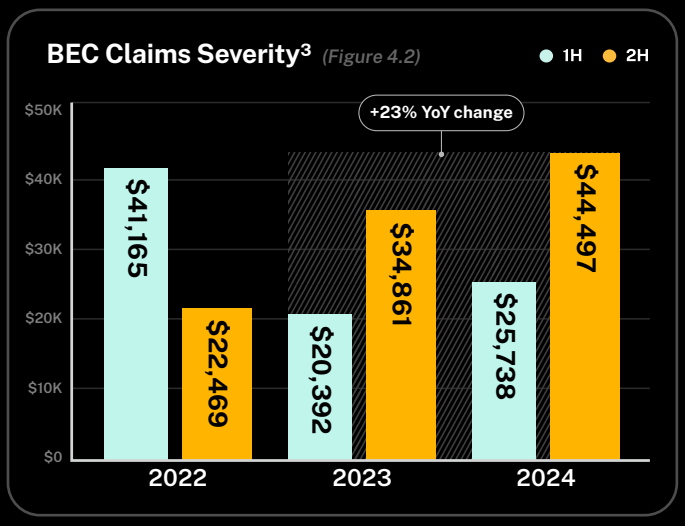
BEC claims severity increased 23% YoY to an average loss of $35,000, primarily driven by a spike in the latter half of 2024.

Business email compromise (BEC) is an event in which cyber criminals gain access to an organization's email account to execute a cyber attack. Attackers often leverage email access to find sensitive data, including login credentials, financials, and other private information. Once equipped with sensitive information, they can steal money, extract data for extortion, or compromise additional technologies.

BEC claims frequency remained stable in 2024 at 0.44%, seeing no YoY change, and has continued to hover at 0.43% over the past three years (Figure 4.1). BEC claims frequency in the US (0.44%) was on par with the global average in 2024. Frequency in Canada was lower (0.32%), while frequency in the UK was higher (0.51%).

BEC claims severity increased 23% YoY to an average loss of $35,000, primarily driven by a spike in the latter half of 2024 (Figure 4.2). BEC claims severity in the US was higher ($36,000) than the global average, while both Canada and the UK were notably lower ($22,000). The spike in BEC severity was, in part, driven by increased prices related to legal expenses, incident response firms, data mining, notifications, and other mitigation and recovery efforts.





3. *Business email compromise (BEC) events that resulted in funds transfer fraud (FTF) are classified as FTF events and, thus, not calculated into BEC severity. For more information, please see Methodology.*

Funds Transfer Fraud

Decrease in initial severity attributable to observed changes in behavior by threat actors & financial institutions

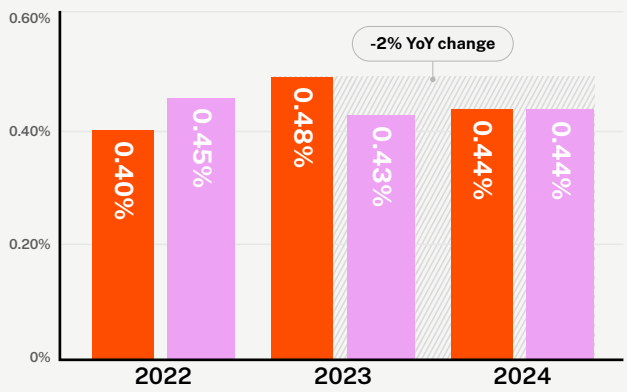
FTF events often occur through social engineering tactics or as a direct result of a BEC event.

The typical **funds transfer fraud** (FTF) is an event in which cyber criminals manipulate businesses into unknowingly sending money to fraudulent accounts controlled by cyber criminals. FTF events often occur through social engineering tactics or as a direct result of a BEC event: Attackers may pose as executives, vendors, or financial institutions to trick employees into initiating unauthorized wire transfers that can have devastating consequences for businesses.

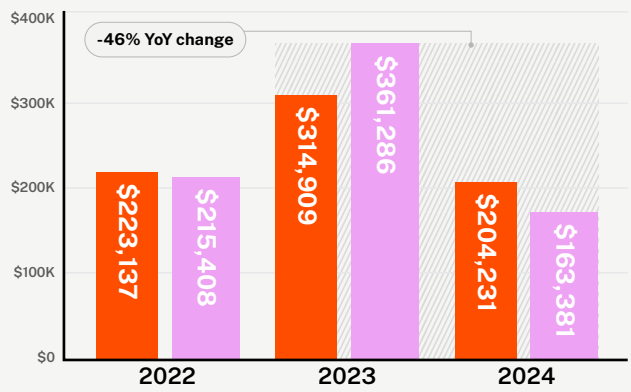
FTF claims frequency decreased 2% YoY in 2024 to 0.44% and has continued to hover at 0.44% over the past three years (Figure 5.1). FTF claims frequency in the US (0.47%) was higher than the global average in 2024. Frequency in Canada was lower (0.32%), as was frequency in the UK (0.27%).

FTF initial claims severity[4] decreased 46% YoY in 2024 to an average loss of $185,000 (Figure 5.2). The sharp decline followed an all-time high in 2023, when FTF initial severity for the entire year topped $340,000.

FTF Claims Frequency *(Figure 5.1)*



FTF Initial Claims Severity[5] *(Figure 5.2)*



4. *FTF initial claims severity excludes all financial recoveries ("clawbacks") to illustrate the true impact of FTF events prior to Coalition intervention.*
5. *Business email compromise (BEC) events that resulted in funds transfer fraud (FTF) are classified as FTF events and, thus, calculated into FTF severity. For more information, please see Methodology.*

Coalition has observed fewer FTF attempts with high six-figure and seven-figure dollar amounts.

The significant decrease in FTF initial severity may be explained by changes in behaviors by both threat actors and financial institutions. Coalition has observed fewer FTF attempts with high six-figure and seven-figure dollar amounts, possibly as a result of financial institutions flagging large transactions and holding them for an extended period of time.

However, FTF initial severity has been historically subject to volatility. It's not uncommon for the initial loss amount in an FTF event to exceed $1 million — in the back half of 2024, Coalition was alerted to a fraudulent transfer of $9.3 million that was ultimately recovered.

Business Email Compromise Led to Funds Transfer Fraud

Across all BEC events in 2024, 29% resulted in an FTF event with an average loss of $106,000.

29% of all BEC events in 2024 resulted in an FTF event

$106K average FTF severity for claims originating as BEC event

CASE STUDY

Coalition claws back $2.1M fraudulent wire transfer after threat actor spoofed email

A distributor of household and personal goods attempted to wire a $2.1 million payment to its landlord for a new lease, but unknowingly sent the funds to a threat actor.

Soon after wiring the money, the business realized the money had been sent to a fraudster and notified Coalition. In under one hour, Coalition made contact with the business and notified government contacts for assistance in freezing the assets. Less than 24 hours later, all but roughly $100 of the funds were frozen and held for return to the distributor.

Coalition Incident Response (CIR)[6] conducted a forensic investigation and determined no unauthorized access to the business' email account occurred: The fraudulent transfer was triggered by a spoofed email.

After the business paid its $100,000 self-insured retention, Breach Response coverage responded to $7,200 in CIR services and another $4,500 in breach counsel fees. Because nearly all of the stolen funds were recovered and returned to the business, Funds Transfer Fraud coverage wasn't triggered.

6. *Coalition Incident Response services provided through Coalition's wholly owned affiliate are offered to policyholders as an option via incident response firm panel.*

In 2024, Coalition's cooperative efforts with authorities and panel partners contributed to the successful clawback of $31 million with an average recovery of $278,000.

Coalition recovered $31 million on behalf of policyholders

When a policyholder reports an FTF event to Coalition, we take swift action based on the options available within the jurisdiction and do everything possible to "claw back" stolen money before it leaves the country of origin. These options include alerting government contacts, obtaining injunctions to freeze the stolen funds, or engaging panel firms to return money to the policyholder.

In 2024, Coalition's cooperative efforts with authorities and panel partners contributed to the successful clawback of $31 million with an average recovery of $278,000.

Clawbacks are a critical and time-sensitive process for Coalition. Policyholders that quickly report FTF events to Coalition have a greater likelihood of recovery. In 2024, Coalition policyholders made a partial recovery in 24% of all reported FTF events and a full recovery in 12% of reported events.

Coalition Clawbacks

$31M
Total FTF recovery in 2024

$278K
Average amount recovered per FTF event

24%
FTF events with at least partial recovery

12%
FTF events with a full recovery

$101M
Lifetime clawbacks

Ransomware

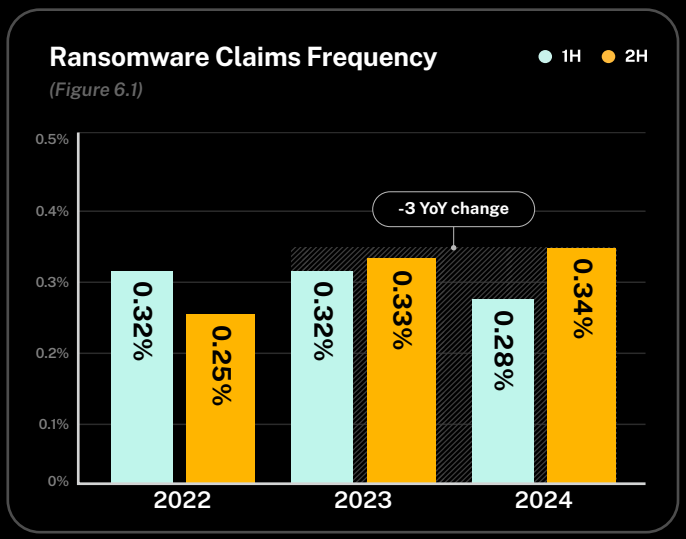
Frequency & severity decreased alongside dip in initial ransom demands

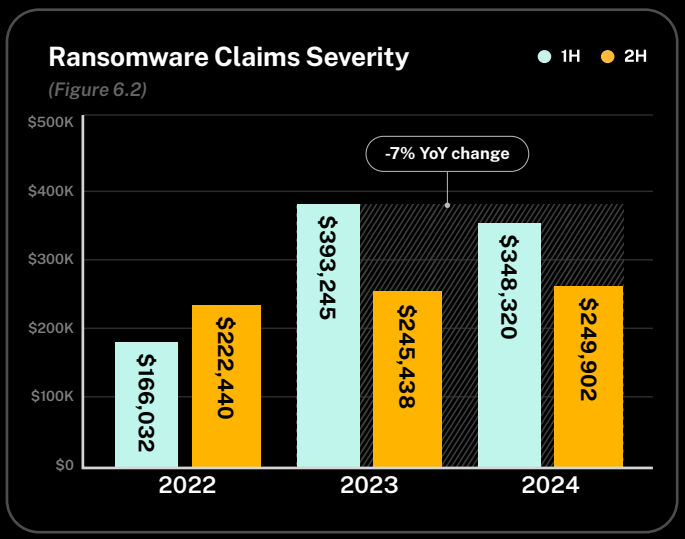
Ransomware claims severity decreased 7% YoY in 2024 to an average loss of $292,000.

Ransomware is a type of malicious software that encrypts a business' data or systems, rendering them inaccessible until a ransom is paid to obtain a decryption key. Ransomware events can result in significant operational disruption and financial loss, regardless if a business chooses to pay a ransom demand, with costs including business interruption, forensic investigation, and data recovery.

Ransomware claims frequency decreased 3% YoY in 2024 to 0.31%, consistent with a three-year average of 0.31% (Figure 6.1). Ransomware claims frequency in the US was only slightly higher (0.32%) than the global average in 2024. Frequency in Canada was faintly higher (0.33%), while the UK was considerably lower (0.19%).

Ransomware claims severity decreased 7% YoY in 2024 to an average loss of $292,000, well below the high point of $393,000 in 2023 (Figure 6.2). Ransomware claims severity in the US was lower ($249,000) than the global average in 2024. Severity in Canada was more than double the global average ($665,000), though the UK was significantly lower ($82,000).

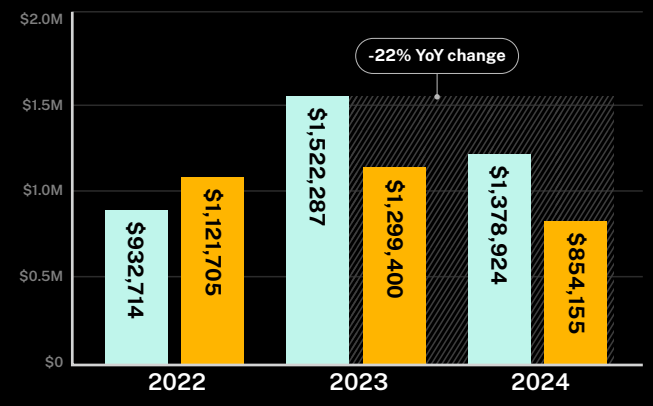




Ransom demands decreased 22%

Perhaps the biggest driver of the dip in ransomware claims severity was the decrease in initial ransom demands. Ransom demands fell 22% YoY in 2024 to an average of $1.1 million (Figure 6.3). Notably, the average demand in the latter half of 2024 fell below $1 million for the first time in more than two years.

Initial Ransom Demands
(Figure 6.3)



Drivers of Ransomware Loss

Ransom payments are often the largest contributor to ransomware claims severity but are only one aspect of the total loss amount. Costs related to business interruption, digital asset restoration, and forensic investigation are other key drivers.

$102K Average business interruption loss[7]

$18K Average digital asset restoration cost

$58K Average forensic vendor cost

CASE STUDY

Furniture manufacturer faces prolonged business interruption from ransomware attack

A furniture manufacturer learned it had been hit with a ransomware attack after discovering a ransom note on a company computer. Threat actors encrypted its data and rendered nearly all systems inoperable. The business contacted Coalition and quickly engaged Coalition Incident Response (CIR)[6] for forensic investigation.

After exfiltrating data, threat actors contacted current and former employees and pressured the manufacturer to pay the ransom. Because all onsite backups were corrupted, the manufacturer decided to pay to prevent the leak of private data. CIR successfully negotiated the ransom demand down from $682,500 to $400,000, but the decryptor provided by threat actors was ineffective. CIR and restoration vendors provided hands-on support for one month to get the manufacturer operational. Ultimately, CIR determined that initial access was gained through remote desktop software.

After the manufacturer paid its $25,000 self-insured retention, Business Interruption coverage responded with $609,000 to help cover the extended downtime. Additional costs were covered through a separate $1 million limit for Breach Response coverage for notifications, data mining, and legal and forensic vendors.

7. *Figures based on 2023 claims data due to the average amount of time required to fully develop business interruption losses.*

Ransomware Negotiations

44%

opted to pay ransom when deemed reasonable and necessary

60%

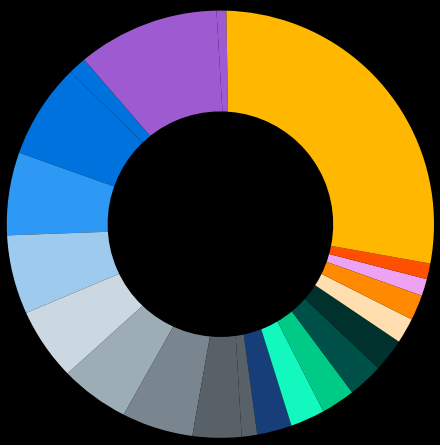
reduction in ransom payments negotiated by CIR

Coalition negotiated 60% reduction in ransom payments

Akira ransomware was the most prolific ransomware variant among Coalition policyholders, accounting for 13% of all ransomware claims in 2024 with an average demand of $692,000 (Figure 6.4). Play ransomware was another notable variant, accounting for 6% of all ransomware claims with an average demand of $2.6 million. The Black Basta variant accounted for just 3% of all ransomware claims, but was the highest in terms of demand with an average of $4 million.

When deemed reasonable and necessary, 44% of policyholders that experienced a ransomware event opted to pay the ransom. In these cases, Coalition Incident Response directly engaged threat actors and, on average, successfully negotiated a 60% reduction in payment based on the initial demand.[8]

Ransomware Events by Variant *(Figure 6.4)*



- **13.4%** Akira
- **6.2%** Play
- **5.7%** MedusaLocker
- **4.6%** RansomHub
- **4.6%** FOG
- **4.1%** Blacksuit
- **4.1%** Hunters International
- **3.1%** Lynx
- **2.6%** Black Basta
- **2.6%** Lockbit 2.0
- **2.6%** Rhysida
- **2.6%** BianLian
- **2.6%** Qilin
- **2.1%** Luna Moth
- **2.1%** Phobos
- **1.5%** Trigona
- **1.5%** 8Base
- **34%** Other

8. Ransomware negotiation data based on cases handled by Coalition Incident Response, an affiliate firm made available to all policyholders via panel selection.

Miscellaneous First-Party Loss

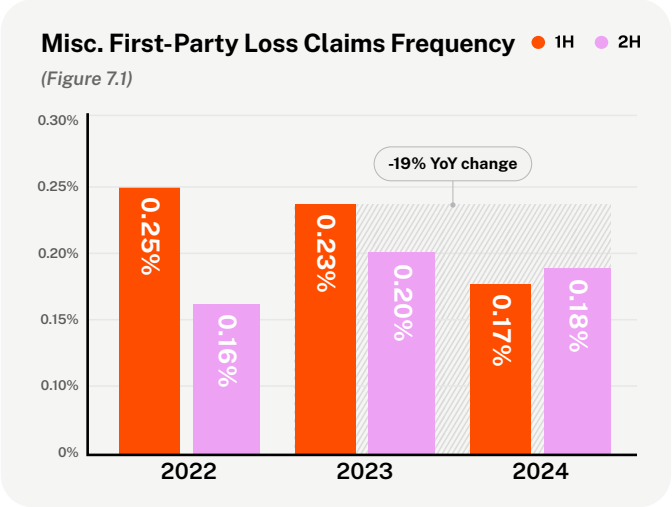
Third-party breaches accounted for more than half of all claims

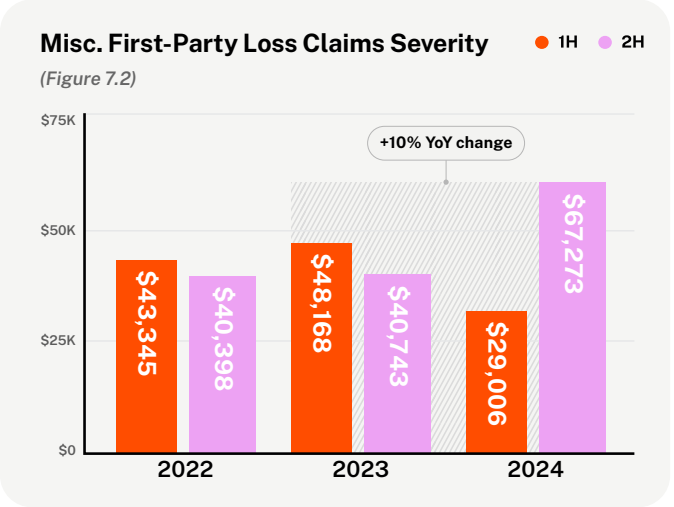
Miscellaneous first-party loss events include malware infections without data theft, insider threats, email or domain impersonation, invoice manipulation, and third-party breaches.

Miscellaneous first-party loss refers to direct financial and operational damages experienced by a business in a cyber event that was not BEC, FTF, or ransomware. These events — including malware infections without data theft, insider threats, email or domain impersonation, invoice manipulation, and third-party breaches, among others — can vary widely from one another but are similar in that they often manifest with gradual compounding costs.

Miscellaneous first-party loss claims frequency decreased 19% YoY in 2024 to 0.17%, just below the three-year average of 0.19% (Figure 7.1). First-party loss frequency in the US was slightly higher (0.20%) than the global average in 2024. Frequency in Canada was lower (0.13%), while the UK was notably higher (0.32%).

Miscellaneous first-party loss claims severity increased 10% YoY in 2024 to an average loss of $49,000 (Figure 7.2). First-party loss severity in the US was slightly higher ($51,000) than the global average in 2024. Severity in Canada was lower ($17,000), as was the UK ($25,000).





Third-Party Breaches

52%

of all miscellaneous first-party loss events due to third-party breach

$42K

Average severity of third-party breach

Risk Aggregation Event Severity

$63K

Average severity of CDK Global claim

$22K

Average severity of Change Healthcare claim

Third-party breaches led to widespread losses

Among all miscellaneous first-party loss claims in 2024, 52% were due to a third-party breach. In these cases, a policyholder's vendor or business partner was compromised, which often led to financial loss. In 2024, the average severity of a third-party breach was $42,000.

A subset of these third-party breaches constituted a **risk aggregation event**: a single cyber event that resulted in widespread loss to other organizations. Coalition observed two notable risk aggregation events in 2024 that stemmed from cyber attacks on Change Healthcare and CDK Global.

Change Healthcare

Change Healthcare, a technology company that processes transactions among healthcare providers, experienced a ransomware attack in February 2024 and was unable to provide critical services for more than a month. The disruption impacted more than 90% of pharmacies across the US, and the total cost of the attack was estimated at nearly $2.87 billion.[9] Among Coalition policyholders, the average severity for claims related to the Change Healthcare attack was $22,000.

CDK Global

CDK Global, a software vendor that facilitates vehicle sales, financing, and inventory management for car dealerships, suffered a ransomware attack in June 2024 that caused significant disruption across its network. Total direct losses to impacted car dealerships were estimated at $1 billion.[10] Among Coalition policyholders, the average severity for claims related to the CDK Global attack was $63,000.

CASE STUDY

Medical equipment supplier disrupted by Change Healthcare ransomware attack

When the Change Healthcare network went offline as a result of ransomware attack, a medical equipment supplier was unable to operate. The supplier could not access electronic medical records or bill its vendors. Without the cashflow, the supplier was also unable to purchase new inventory.

After the supplier reported the disruption, Coalition contacted a forensic accountant to determine the losses incurred from the breach. Within one month, Coalition issued the first of five payments to cover the ongoing business interruption losses and provided complimentary breach counsel. Over the span of eight months, the supplier's Business Interruption coverage responded to $297,000 in losses, including $9,000 in extra expenses.

9. *The HIPAA Journal, Change Healthcare Ransomware Attack Cost to Rise to $2.87bn in 2024*
10. *Anderson Economic Group, Dealer Losses Due to CDK Cyberattack Reach $1.02 Billion*

Third-Party Allegations

Frequency & severity decreased following spike in second half of 2023

Unlike first-party losses, third-party allegations arise when security failures, privacy violations, or intellectual property disputes lead to damages for others.

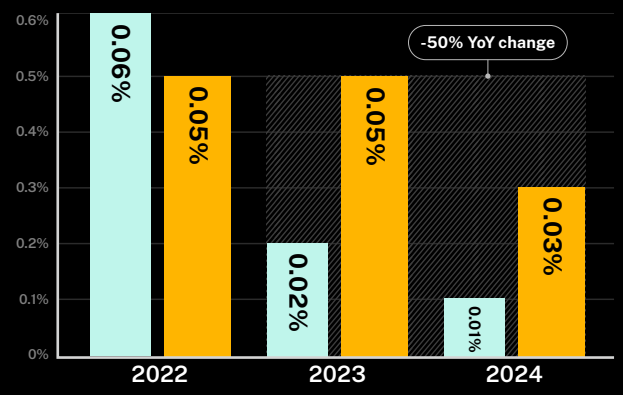
Third-party allegations refer to claims made against a business by external parties due to a cyber event, privacy breach, infringement, or error that caused harm or legal liability. These allegations are often made by customers, vendors, or regulatory bodies and can result in lawsuits, fines, contract disputes, and reputational harm.

Unlike first-party losses, third-party allegations arise when security failures, privacy violations, or intellectual property disputes lead to damages for others: The third party experiences a loss and seeks to hold a policyholder liable for the resulting damages. This can arise from data breaches, unauthorized disclosure of personal data, infringement, or copyright issues related to digital content.

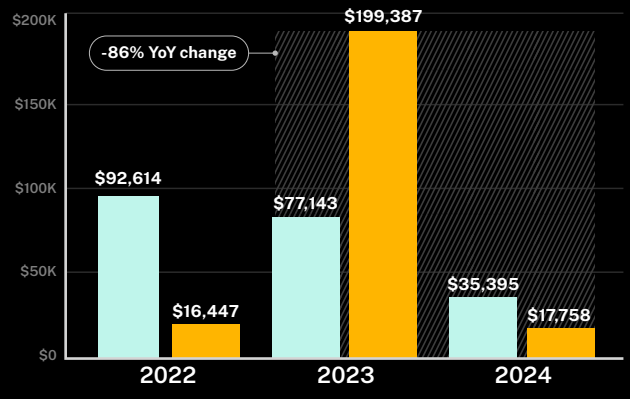
Third-party allegations frequency decreased 50% YoY in 2024 to 0.02%, a trend that reflects the fact that these events are far less common than others (Figure 8.1). The frequency of these events were consistent across the US and Canada, while the UK experienced none of these claims in 2024.

Third-party allegations severity decreased 86% YoY in 2024 to an average loss of $23,000, in part due to a substantial spike in the latter half of 2023 (Figure 8.2). Third-party allegations severity in the US mirrored the global average ($23,000), though Canada was slightly lower ($19,000.)

Third-Party Allegations Frequency
(Figure 8.1)



Third-Party Allegations Severity
(Figure 8.2)



The Power of Active Insurance

How Coalition protects against cyber threats before, during, and after an attack

Risks Avoided

614

Businesses that experienced an attack in 2024 after failing to address critical issues

$307M

Estimated losses among businesses that did not bind a Coalition policy

Security Alerts

85K+

Security alerts sent in 2024

32K+

Security issues resolved

Defense against cyber threats starts at the underwriting stage, well before an insurance policy is issued. Coalition is dedicated to smart, strategic underwriting and data-driven risk selection to help ensure every policyholder is set up for success. This often means prompting businesses to adopt new security tools or enhance specific controls that benefit all parties: strengthening the overall security posture of Coalition policyholders and, thereby, decreasing the likelihood of a cyber attack.

The power of Active Insurance is visible in 2024 with YoY decreases in claims frequency across all revenue segments. Businesses are recognizing the reality of our modern world and proactively addressing cyber risk before they become Coalition policyholders. Unfortunately, we also see what happens when businesses do not heed our recommendations.

In 2024, 614 businesses were notified of critical issues at the time of quoting a cyber insurance policy and opted not to resolve the issues or bind a Coalition policy, only to later experience a ransomware attack. Total losses among these businesses are estimated at $307 million.[11]

Of course, Active Insurance doesn't stop once coverage is bound — it continues throughout the life of every Coalition policy. Proactive engagement with policyholders is a critical aspect of reducing cyber risk.

Coalition security researchers work on the frontlines of the cyber threat landscape to gather intelligence and notify policyholders about new and emerging risks. Timely alerts about zero-day vulnerabilities and other critical vulnerabilities in widely used software give policyholders an opportunity to strengthen their defenses before attackers strike.

In 2024, we issued more than 85,000 security alerts to active policyholders via Coalition Control®, directly resulting in the mitigation of more than 32,000 security issues, ranging from time-sensitive software patching and zero-day vulnerabilities to ongoing maintenance and sunsetting of end-of-life software.

11. Estimate based on publicly available data, risk assessments at the time of quoting, and simulated claims based on comparable organizations.

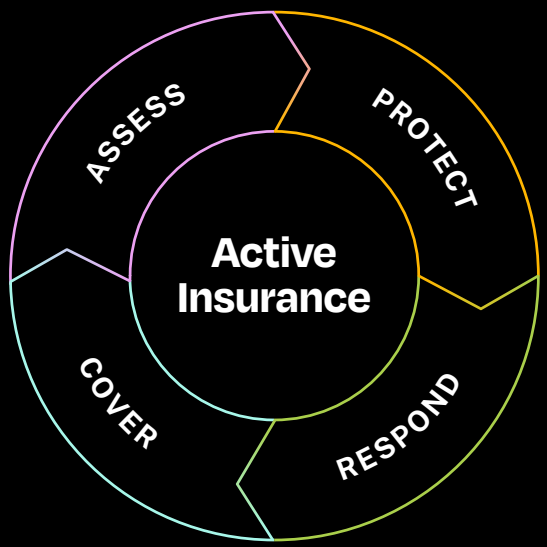
A Unified Approach to Help Protect Against Cyber Threats

Coalition policyholders experience 73% fewer claims than the industry average.

Our mission at Coalition is to help protect the unprotected. To meet cyber threat challenges in ways traditional insurance can't, we pioneered **Active Insurance**: the first cyber defense bringing together active cyber risk assessment, proactive protection, expert response, and comprehensive cyber coverage.

How Active Insurance Works

Active Insurance is purpose-built to help protect businesses in the digital age and mitigate risks throughout the life of the policy.



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

Benefits of Coalition Security

- Aligned incentives to help keep you secure
- Insights informed by real-world risks
- Access to deep cybersecurity experts
- Tools built and priced for SMBs

Maximizing Active Insurance with Coalition Security™

Coalition Security[12] complements cyber insurance at all phases of the policy period. Our products and services are informed by real-time risk and insurance insights from 90,000+ policyholders worldwide to help prioritize threats and remediation based on potential business impact.

- **Coalition Control®:** View unique cyber risk profiles, monitor security alerts, access security support, and explore enhanced security services
- **Coalition Managed Detection & Response:** Prevent and mitigate attacks with 24/7/365 protection for computing assets and monitoring by seasoned cybersecurity experts
- **Security Awareness Training:** Educate employees on threat actor tactics, learn how to spot and avoid cyber attacks with phishing simulations, and meet compliance requirements
- **Coalition Incident Response:** Respond to cyber attacks faster, recover with minimal business disruption, and receive hands-on support with incident response plans and tabletop exercises

Meet cyber risk head-on in 2025

Discover the true power of Active Insurance ›

Complement cyber insurance with Coalition Security ›

12. *Coalition Security services, Coalition Managed Detection & Response ("MDR") services, and Coalition Security Awareness Training ("SAT") are provided by Coalition Incident Response (d/b/a Coalition Security), a wholly owned affiliate of Coalition, Inc. Coalition Security does not provide insurance products. The purchase of a Coalition insurance policy is not required to purchase MDR, SAT or any other Coalition Security service.*

Methodology

The 2025 Cyber Claims Report features reported claims data from January 1 to December 31, 2024. Coalition defines a claim as an adverse cyber matter reported by a policyholder that incurred a gross loss.

To complete the analysis in this report, Coalition data scientists and actuaries used 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.

For the purposes of this report, every cyber insurance claim is categorized as a single event type. Although one cyber event can lead to another — BEC can lead to either ransomware or FTF — limiting each claim to a single event category is valuable when analyzing the totality of claims. As a result, certain event types are weighted more than others: FTF and ransomware both supersede BEC due to the severity and overall impact of those event types.

Regarding matters across different geographic regions, claims data from policyholders in Australia is included throughout this report, contributing to global claims frequency and claims severity figures, as well as those specific to event type. However, due to relative time in the market, Coalition is not publishing this data on a standalone basis.

Our methodology was first introduced in the 2023 Cyber Claims Report: Mid-year Update and has been retroactively applied to Coalition's historical data, allowing us to highlight claims trends impacting Coalition policyholders. In doing so, global claims frequency and severity data may have changed from prior reports. Please reference our most recent report when possible.

Coalition®

coalitioninc.com

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

Insurance products are offered in certain jurisdictions by the following wholly owned affiliates of Coalition, Inc.: In the U.S. Coalition Insurance Solutions, Inc. a licensed insurance producer and surplus lines broker (Cal. License #0L76155); in Canada Coalition Insurance Solutions Canada, Inc. a license insurance producer in all provinces with a principal place of business in Vancouver, British Columbia (#LIC-2020-0020925-R01) and in Quebec with a principal place of business in Montreal, Quebec (#608005); in Australia Coalition Insurance Solutions Pty Ltd (ABN 33 657 104 791, AFSL 539846) under a binding authority given by the insurers, Allianz Australia Insurance Limited (ABN 15 000 122 850, AFSL 234708) and Mitsui Sumitomo Insurance Company (ABN 49 000 525 637, AFSL 240816); in the U.K. by Coalition Risk Solutions Ltd., an appointed representative of Davies MGA Services Limited, a company authorized and regulated by the Financial Conduct Authority (FCA), registration number 597301, to carry on insurance distribution activities. Coalition Risk Solutions Ltd. is registered in England and Wales: company number 13036309. Registered office: 34-36 Lime Street, London, United Kingdom, EC3M 7AT. Coalition, Inc., a Delaware corporation, does not offer insurance products.

The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.

The foregoing review was completed using the carrier's base policy with endorsements made available to Coalition. 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 thereof. While Coalition endeavors to create the most accurate and complete review, the content is for informational purposes only and you should take steps necessary to ascertain that the information contained herein is correct and verified by your own review. Coalition makes no representations or warranties regarding the completeness, reliability, or accuracy of the reviews and does not assume any liability for any errors or omissions in the content. No coverage is provided by this coverage comparison, nor can it be construed to replace any policy provisions. Please refer to the policy for complete information on the coverages provided. Coverages and other features in an insurance policy vary based on customer profile and may not be available to all customers. Moreover, this information is not an insurance policy, does not refer to any specific insurance policy issued, and does not modify any terms and conditions expressly stated in any insurance policy issued. In order to fully understand the coverages and other features of a specific insurance policy offered by Coalition on behalf of unaffiliated insurance companies, and available on an admitted basis through Coalition Insurance Company, for a particular customer, you are encouraged to contact Coalition, Inc. at https://www.coalitioninc.com/contact. Copyright © 2025. All Rights Reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.