Coalition®

2026 Cyber Claims Report

Table of Contents

THE CHALLENGE

Confronting the Cyber Protection Paradox

More tools & more spending aren't making businesses safer

Brokers, business leaders, and insurance professionals may not agree on everything, but on this the consensus is clear: Cybersecurity incidents are the single-greatest risk facing modern businesses.[1] No longer a quiet IT concern, cyber risk is now a boardroom priority; 86% of companies reported cybersecurity as a skill, or desired skill, on their boards of directors,[2] an acknowledgment that digital resilience is synonymous with business survival.

Global cybersecurity spending projections have increased 24% over the past two years, rising from $193 billion in 2024 to $240 billion in 2026.[3] Yet, organizations are being confronted by the **Cyber Protection Paradox: More tools and more spending aren't making businesses safer.** Despite record investments and an explosion of vendors, businesses are now two times more likely to experience a cyber incident than they were five years ago.[4]

Instead, the abundance of cybersecurity tools has fueled complexity: 76% of security leaders say they feel overwhelmed by alert fatigue, while 96% of organizations report critical visibility blind spots because their platforms fail to correlate data.[5] This fragmentation is an obsolete strategy in an era where attackers move at machine speed.

While our past reports documented third-party fragility and hard-won stability, the economic reality of 2026 has shifted. This year's report illuminates why the solution to this paradox isn't "more stuff," but a smarter, holistic approach. While the cyber insurance industry at large struggles with rising loss frequency and severity, Coalition claims data demonstrates the impact of proactive risk management in stabilizing loss trends.

This success is a result of Active Insurance. We believe cybersecurity and cyber insurance are inseparable; true resilience can't be achieved with one but not the other. By bridging these domains, Coalition helps businesses break the cycle of ineffective overspending, prioritize fixes based on financial impact, and resolve incidents before they escalate.

The path to operational resilience requires shifting from a disconnected collection of tools to a coordinated engagement. Active Insurance helps businesses overcome the Cyber Protection Paradox: stopping threats earlier with personalized risk insights and guidance, responding to incidents quickly to help minimize impact and accelerate recovery, providing comprehensive coverage to help give peace of mind following an attack, and offering robust security solutions that are integrated with insurance and proven to protect.

About the 2026 Cyber Claims Report

This report features statistics, charts, and risk insights based on data from 100,000+ Coalition policyholders across the United States, Canada, the United Kingdom, Australia, and Germany. Cyber risk is a global matter, and the trends and risk mitigation strategies discussed 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. Allianz, Allianz Risk Barometer 2026 2. EY Center for Board Matters, Cyber and AI Oversight Disclosures 3. Gartner, Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025 4. Check Point Research, Global Cyber Attacks Surge 21% in Q2 2025 5. Gurucul, 2025 Pulse of the AI SOC Report

AT A GLANCE

Key Findings

Insights from the front lines of cyber risk

Email-Based Attacks

58% of claims were business email compromise (BEC) or funds transfer fraud (FTF)

52% of FTF claims originated as a BEC with an average loss of **$112K**

71% of FTF claims resulted from social engineering

Ransomware

70% of ransomware claims involved both encryption and data exfiltration

47% surge in ransomware demands to an average of more than **$1M**

86% of ransomware victims refused to pay the demand

The Power Of Active Insurance

64% of closed claims resulted in no out-of-pocket loss for policyholders

$21.8M in stolen funds recovered with an average of **$202K** per incident

65% average reduction in ransom payment via negotiation

THE BIG PICTURE

Global Overview

Shifting dynamics in claims frequency, severity & event types

The global cyber risk landscape is perpetually in flux. The relationship between how often attacks occur and the financial damage they inflict underwent a significant shift in 2025. While the volume of incidents continued to place pressure on organizations, the average financial impact per event decreased, a trend that reflects a maturing cybersecurity posture among Coalition policyholders.

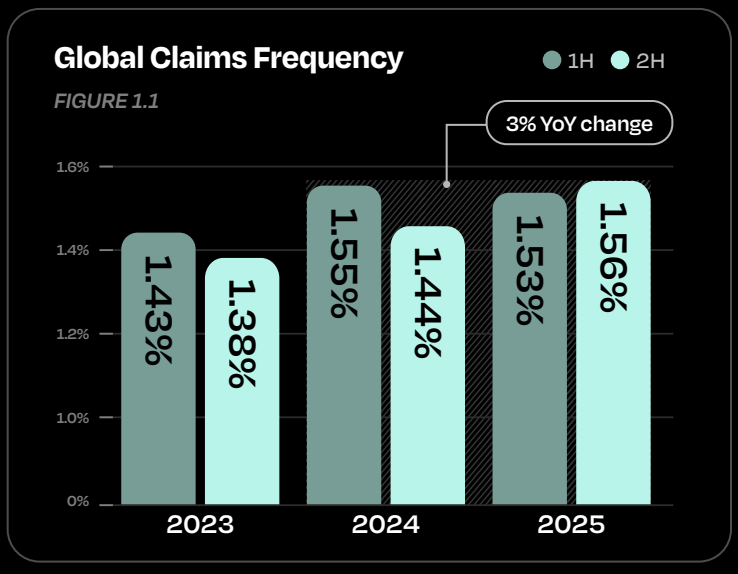
Claims frequency refers to how often claims are filed over a period of time.

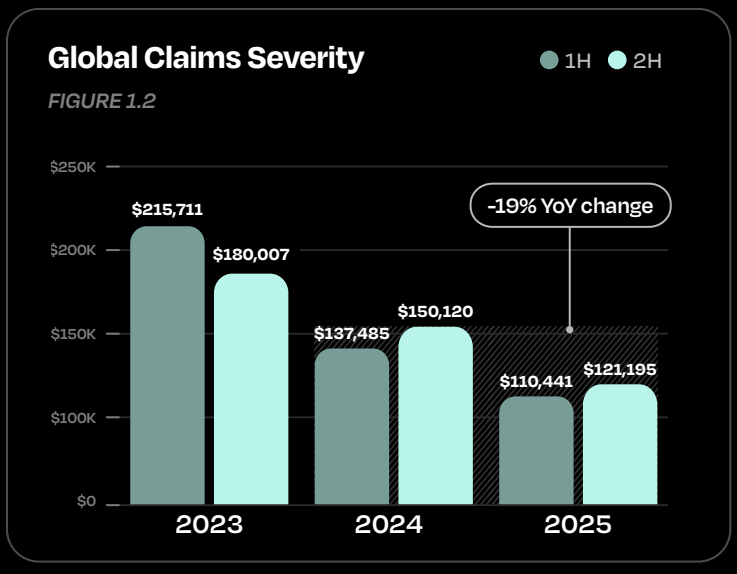
Claims severity refers to the average loss amount per claim.

Frequency & Severity: An Inverse Trend

Claims data in 2025 highlights an inverse relationship between how often attacks occur and how much they cost. While the frequency of claims is rising, the average cost of those attacks is beginning to stabilize.

Global claims frequency rose 3% year over year (YoY) to 1.54%, peaking in the second half of the year as attackers became more persistent (Figure 1.1). However, this increased volume was met with a more robust defensive posture: Global claims severity decreased 19% YoY to an average loss of $116,000 (Figure 1.2). This suggests that while attackers are knocking on the door more often, businesses are becoming more effective at limiting the damage once a breach occurs.





Evolving Threat Landscape

Business Email Compromise

BEC remained the leading event type, accounting for 31% of claims, as attackers increasingly used sophisticated social engineering to exploit the human element (Figure 1.3). While some may view it as a simple email issue, BEC has evolved into a primary staging ground for more complex downstream cyber attacks.

Funds Transfer Fraud

FTF closely trailed BEC as the second-most common event type, representing 27% of claims. As banks and businesses tightened access controls, attackers shifted toward bank impersonation tactics to bypass traditional approval loops. Together, BEC and FTF comprised a strong 58% of claims.

Ransomware

Accounting for 21% of claims, extortion-based attacks remained a prominent threat. Once a straightforward threat of encryption, ransomware has transitioned into a multifaceted crisis, as ransomware severity was largely dictated by exfiltration, making data theft more costly than encryption alone.

Miscellaneous First-Party Loss

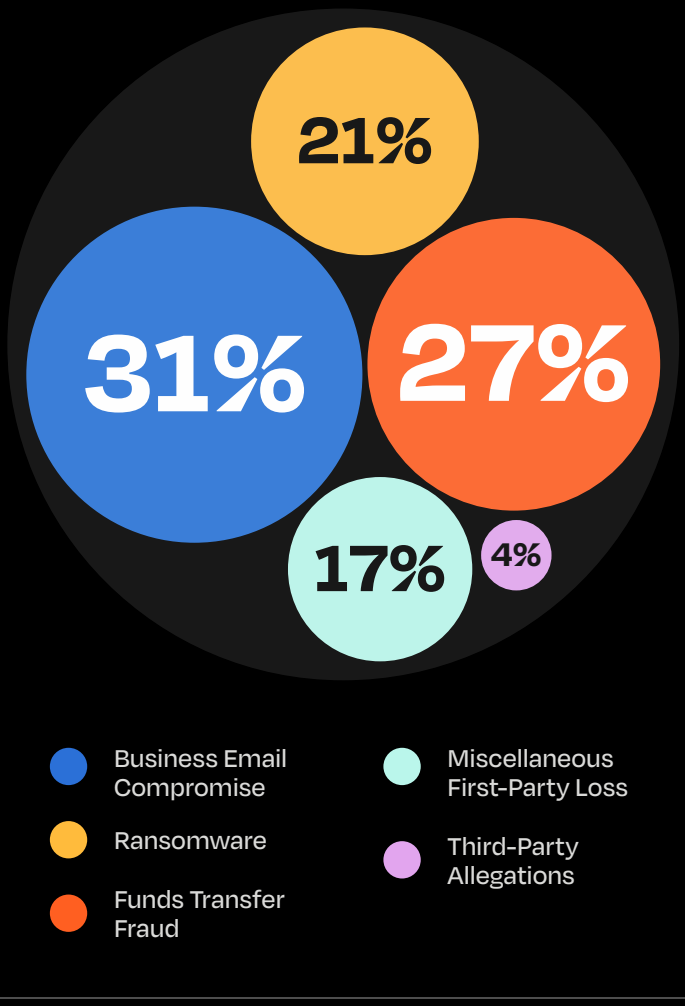
Miscellaneous first-party loss events encompassed a broad range of claims, including instances of unauthorized access, email or domain impersonation, security failures, and third-party breaches. These claims highlight that not all cyber events are malicious; internal errors and technical instabilities can be just as damaging to business continuity.

Third-Party Allegations

Third-party allegations represented the growing legal and regulatory tail that followed an incident, as external parties sought accountability for data privacy or security failures. In particular, 2025 saw a notable rise in class-action activity and regulatory scrutiny surrounding the use of web-tracking technologies.

2025 Claims by Event Type

FIGURE 1.3



Neutralizing Threats Before They Become Losses

Active Insurance is proven to help businesses break through the Cyber Protection Paradox by shifting from a passive policy to an active relationship. **In 2025, 64% of closed claims were resolved with no out-of-pocket loss for the policyholder.**

THE INVISIBLE FOOTHOLD

Business Email Compromise

How attackers turn trusted inboxes into internal threats

Business email compromise (BEC) remained the most common event type, representing 31% of all claims in 2025. Unlike other cyber events that rely on smash-and-grab tactics, BEC is a patient game of observation that often prioritizes stealth over speed.

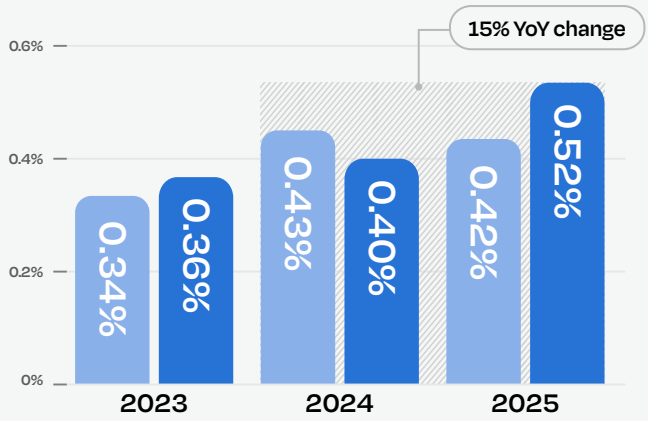
By gaining access to a legitimate business email account, an attacker effectively becomes a silent insider, capable of harvesting login credentials, sensitive financials, and internal workflows that can fuel subsequent attacks.

BEC claims frequency rose 15% YoY to 0.47%, driven largely by a significant surge in activity during the second half of 2025 (Figure 2.1). While the frequency of these incidents went up, BEC claims severity decreased 28% YoY, settling at an average loss of $27,000 (Figure 2.2).

BEC claims severity decreased 28% YoY, settling at an average loss of $27,000.

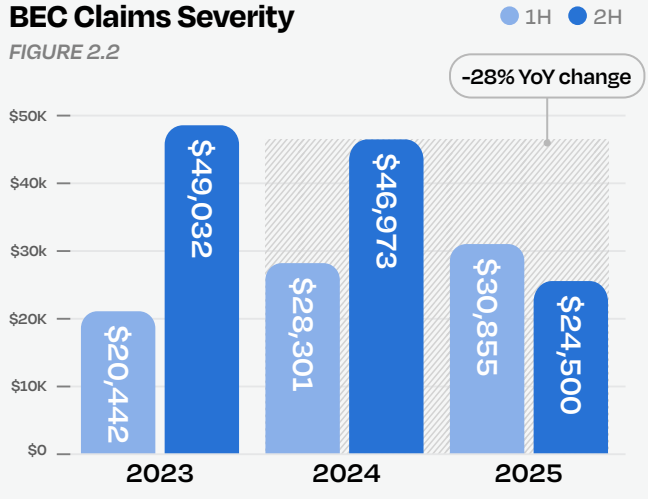
BEC Claims Frequency

FIGURE 2.1



BEC Claims Severity

FIGURE 2.2



Email as a Gateway to Greater Attacks

BEC is especially dangerous because it can serve as a gateway to more severe attacks. When an attacker is operating within a trusted channel, often posing as a colleague or vendor, they can move laterally through systems without raising alarms.

BEC events rarely start with malware; social engineering alone can be sufficient. A convincing phishing email can trick a user into revealing credentials, installing a hidden forwarding rule, or disclosing internal workflows, giving an attacker persistence and insight. Once an attacker has that foothold, they can escalate in multiple directions, from financial loss and data exposure to wide-ranging operational disruption.

CASE STUDY

Unmasking a Long-Term BEC & Wire Fraud Scheme

A property management company fell victim to a coordinated attack that started as BEC and escalated into FTF after a threat actor intercepted an active wire transaction. By altering a single character in a client's email address, the attacker duped the business into sending four fraudulent payments totaling $539,000. After the incident was reported, Coalition Incident Response (CIR)[6] discovered the attacker had been dwelling inside the email account for two months and implemented silent inbox rules to redirect communications. Working alongside the business' payment processor, our claims team successfully recovered $290,000 in stolen funds. After the business met its $25,000 self-insured retention, its Funds Transfer Fraud coverage paid the remaining $224,000.

6. Incident response services are provided by Coalition Incident Response Inc. dba Coalition Security, an affiliate of Coalition Inc.

Outpace Adversaries with Wirespeed™

When attackers compromise a business email account, they can do serious damage in a few short minutes. **Wirespeed's 24/7 fully automated managed detection and response** (MDR) keeps businesses a step ahead of cyber threats.

- **Lightning-Fast Defense:** Mitigation in seconds to stop threats before they lead to loss
- **Precision Filtering:** Logic-based algorithms deliver accuracy and cut out false positives
- **Conclusive Verdicts:** Automated analysis to investigate events for true peace of mind

Discover how Wirespeed can help businesses reduce the likelihood of a cyber claim >

THE FINANCIAL MISDIRECT

Funds Transfer Fraud

How attackers steal money through deception & manipulation

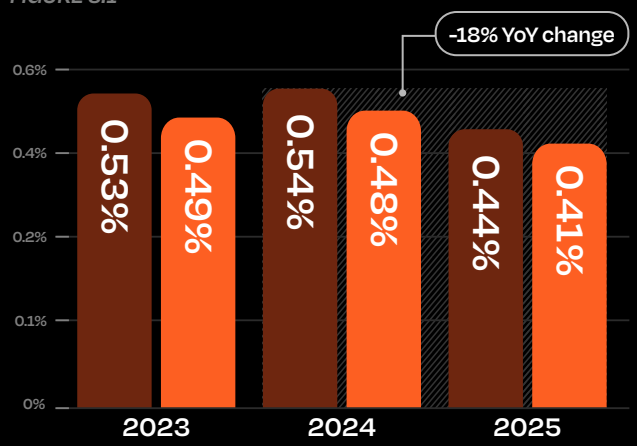
FTF claims severity decreased 14% YoY to an average loss of $141,000.

Funds transfer fraud (FTF) was the second-most common type of cyber event, accounting for 27% of claims in 2025. A typical FTF event involves an attacker manipulating businesses into unknowingly sending money to an account they control, often by inserting themselves into a legitimate transaction.

FTF claims frequency decreased 18% YoY in 2025 to 0.42%, representing a steady, incremental decline over the past two years (Figure 3.1). FTF claims severity decreased 14% YoY to an average loss of $141,000 (Figure 3.2).

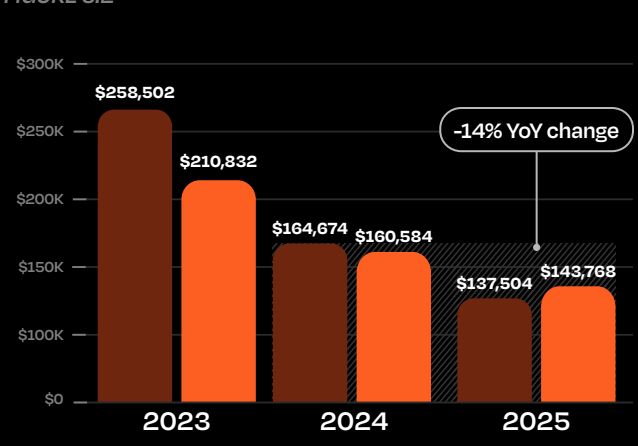
FTF Claims Frequency

FIGURE 3.1



FTF Claims Severity

FIGURE 3.2



Pathways to Funds Transfer Fraud

FTF events can unfold in various ways. In many cases, attackers directly manipulate people using social engineering tactics to carry out these attacks; they may pose as executives, vendors, or financial institutions to deceive others into sending fraudulent payments. In other instances, attackers have no direct interaction with the victim; instead, they may gain access to online banking credentials or payment systems and submit fraudulent transfer instructions directly to the bank.

Social Engineering

Across all FTF claims in 2025, 71% were a direct result of social engineering with an average loss of $127,000 (Figure 3.3). The key element in these tactics is human deception: Attackers persuade their victims to take action through impersonation and create a sense of urgency or legitimacy to convince the victim to change payment details or approve a transfer. FTF events caused by social engineering can be difficult to spot in real time because the payments are typically authorized, albeit under false pretenses.

Instructions to Bank

While most fraud relies on tricking employees into wiring money, attackers are increasingly cutting out the middleman. In 2025, 20% of all FTF events were caused by fraudulent instructions sent directly to banks, with a higher average loss of $218,000. In these cases, the employees of the affected businesses weren't directly involved in the transfer request; attackers deceived the banks using compromised credentials or account takeover tactics to initiate transactions directly.

2025 FTF Claims Severity by Tactic

Social Engineering

$126,588

Instructions to Bank

$217,979

2025 FTF Claims by Tactic

FIGURE 3.3

- **71%** — Social Engineering
- **20%** — Instructions to Bank
- **9%** — Unspecified

Email Breach a Catalyst for Financial Fraud

FTF events can occur as a direct result of BEC. When a BEC event leads to an FTF event, it means an attacker gained access to a business' email account and used that access to carry out an attack. An attacker may intercept a legitimate vendor invoice and alter the payment details or steal banking credentials stored in the mailbox and initiate transfers directly. Among all FTF claims in 2025, 52% originated from a BEC event with an average loss of $112,000 (Figure 3.4).

FTF events can also happen without BEC. A social engineering FTF event might stem from a convincing spoofed email that never required mailbox access, while an instructions-to-bank FTF event might be triggered by malware or credential theft unrelated to email. Across all FTF claims in 2025, 39% were confirmed as having no BEC event with a higher average loss of $187,000.

Ultimately, BEC is a catalyst for FTF, but not a prerequisite. Businesses must be prepared for both email-enabled and email-independent pathways to financial fraud.

CASE STUDY

Racing the Clock on a $1.9M Bank Impersonation Scam

A law firm fell victim to a sophisticated impersonation scam when an employee received a call from its bank's "fraud department." After the caller noted strange transactions on the firm's account that needed confirmation, the employee provided account details to authenticate. Almost immediately, more than 50 wire transfers were sent out from the account totaling $1.9 million. Suspecting foul play, the employee contacted the bank and confirmed the initial phone call was illegitimate. Fortunately, because the bank was notified promptly about the fraud, the bank was able to quickly recover nearly $1.1 million. Soon after the firm contacted Coalition, we immediately mobilized with support from the US government and the firm's bank to claw back an additional $577,000, while the firm's Funds Transfer Fraud coverage was used to cover the remaining $170,000.

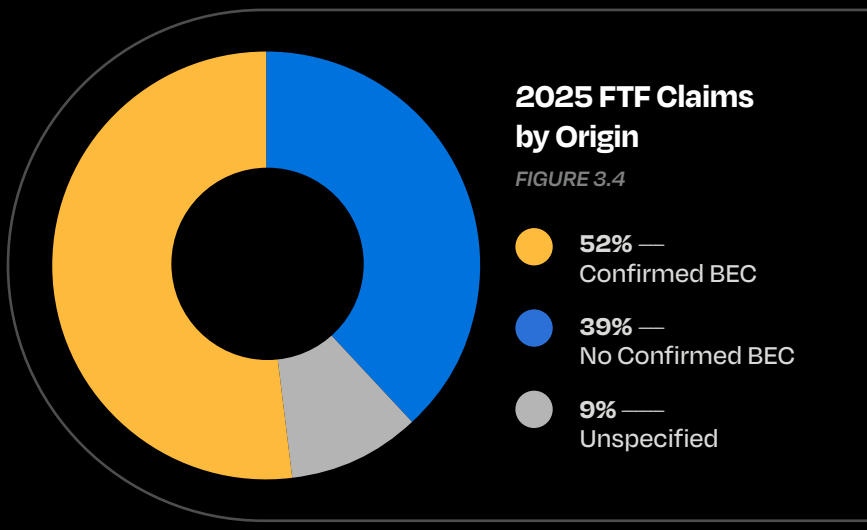
2025 FTF Claims Severity by Tactic

Confirmed BEC

$111,971

No Confirmed BEC

$186,940



2025 FTF Claims by Origin

FIGURE 3.4

- **52%** — Confirmed BEC
- **39%** — No Confirmed BEC
- **9%** — Unspecified

Recovering Stolen Funds After Fraud

When wire fraud occurs, time is of the essence. Reporting an FTF event to Coalition isn't just a standard claim filing; it's the start of a high-stakes race to recover stolen money before it vanishes forever. Our dedicated claims team leverages an arsenal of rapid-response tactics to help recover stolen funds, from activating emergency government channels and freezing funds at the destination to deploying specialist panel firms that intercept transfers midstream.

In 2025 alone, Coalition successfully "clawed back" $21.8 million on behalf of policyholders, with an average recovery of $202,000 per incident.

Recovery is a game of minutes, not days. Policyholders that report FTF events to Coalition immediately are significantly more likely to see their funds returned: 32% of reported FTF events resulted in at least a partial recovery, underscoring that while the threat of FTF is persistent, it doesn't mean the loss is permanent.

Coalition Clawbacks

$21.8M

FTF recoveries in 2025

$202K

Average amount recovered

32%

FTF events with a recovery

$158M

Total recoveries since inception

THE OPERATIONAL PARALYSIS

Ransomware

How attackers disrupt operations with encryption & exfiltration

Ransomware claims severity decreased 19% YoY to an average loss of $262,000.

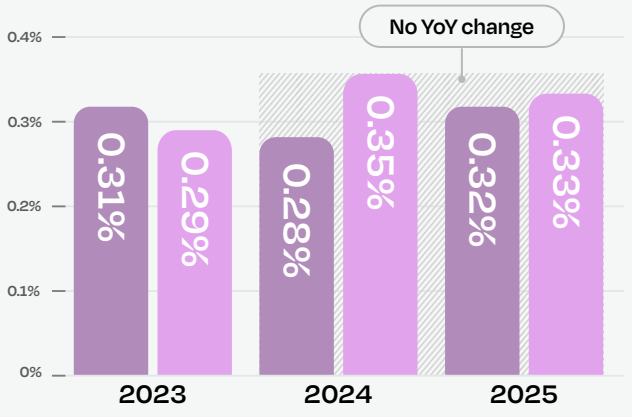
Ransomware may not be the most common cyber event, but it's undeniably the most costly and complex. At its core, ransomware is a crisis in a box, designed to lock a business out of its own systems or threaten exposure of sensitive data until a ransom is paid. The result is immediate operational paralysis, forcing executives into high-stakes situations, where they must weigh the cost of a ransom against the mounting price of business interruption, privacy exposure, and even total system restoration.

Ransomware claims frequency was flat YoY in 2025, hovering at 0.32% and mirroring its three-year average (Figure 4.1). Ransomware claims severity decreased 19% YoY to an average loss of $262,000 (Figure 4.2). Because ransomware claims often take time to develop, we expect these figures to evolve.

The downward trend of ransomware severity is not a result of attackers lowering their sights, as ransom demands continued to climb throughout the year. Instead, it marks a significant win for organizational resilience: More businesses are refusing to pay ransoms and are instead successfully leveraging viable data backups and restoration to get back online after an attack.

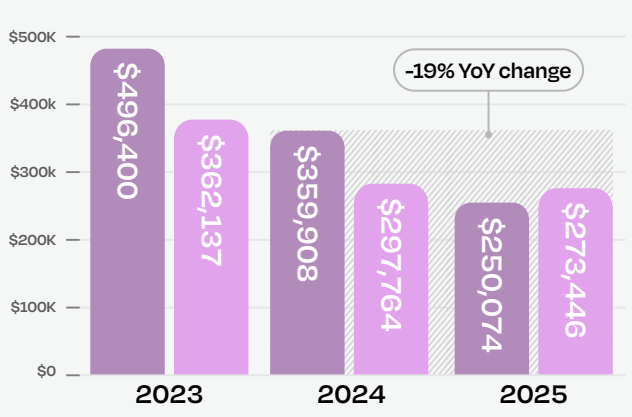
Ransomware Claims Frequency

FIGURE 4.1



Ransomware Claims Severity

FIGURE 4.2



The Intersection of Encryption & Exfiltration

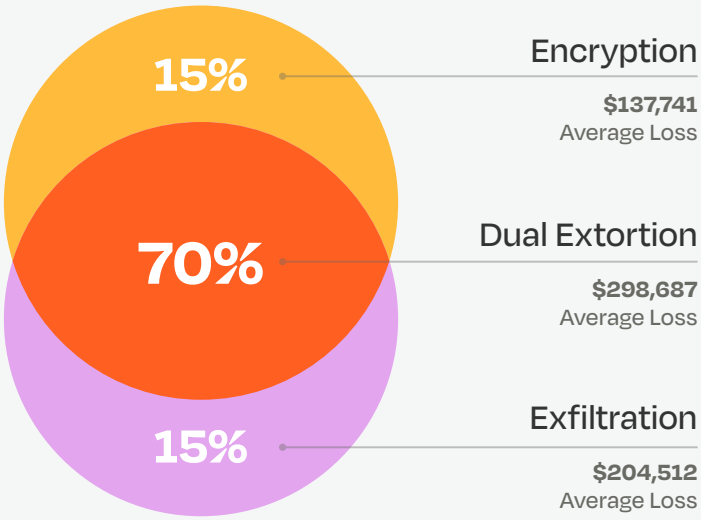
Historically, ransomware was synonymous with encryption, rendering files inaccessible until a victim purchased a decryption key. Today, the ransomware umbrella has expanded to include varied forms of digital extortion, and the impact of a ransomware incident is often dictated by whether an attacker chooses to lock systems, steal data, or pursue both simultaneously.

Encryption

Encryption represents the traditional lock-and-key tactics, where attackers deploy malware to trigger operational paralysis. Encryption-only ransomware attacks accounted for 15% of ransomware claims, with an average loss of $138,000 (Figure 4.3). In these scenarios, the attack focused entirely on system lockout, while the business faced a demand to purchase a decryption key to regain control.

2025 Ransomware Claims by Tactic

FIGURE 4.3



Because these attacks halt operations entirely, they're characterized by high business interruption costs and the immediate need for system restoration. However, encryption-only tactics are becoming less effective against businesses with robust, offsite data backups. As more businesses successfully restore systems without rewarding the attacker, the standalone leverage of encryption continues to diminish.

Exfiltration

Exfiltration occurs when a threat actor steals sensitive information without deploying encryption malware. Rather than a full lockout, the demand is leveraged alongside the threat of leaking or selling data. These thefts accounted for 15% of ransomware claims, carrying a higher average loss of $205,000.

The higher cost of an exfiltration-only claim is often driven by legal, regulatory, and reputational complexity rather than downtime. Even without operational disruption, the presence of stolen data can trigger expensive forensic investigations, mandatory reporting and notification costs, and possible subsequent class-action lawsuits. These tactics are gaining ground as a stealthy alternative to encryption, specifically targeting businesses with large volumes of sensitive data.

Dual Extortion

Dual extortion represents the intersection of both tactics, where threat actors simultaneously encrypt systems and exfiltrate data. This is the most severe type of ransomware attack, leaving a business both operationally paralyzed and legally vulnerable. In 2025, dual extortion was the dominant threat, accounting for 70% of all ransomware claims with an average loss of $299,000.

By pursuing both paths, attackers remove a business' ability to simply "restore from backup" to solve the problem. Even if a company can get its systems back online, the threat of a data leak remains a massive financial, legal, and regulatory pressure point. The data underscores this exfiltration multiplier, as dual extortion claims are more than twice as expensive as those involving encryption alone.

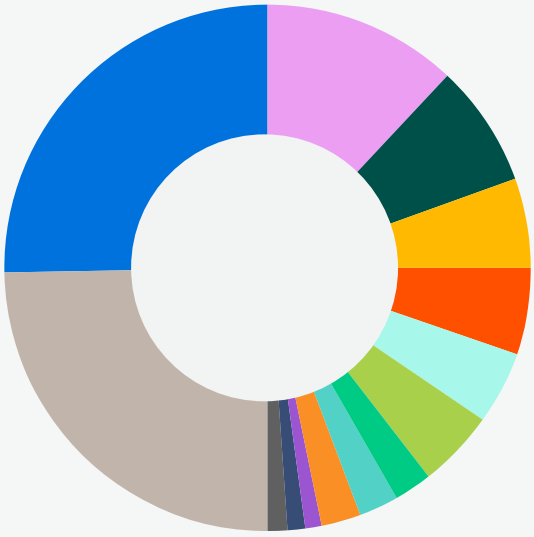
Ransomware Demands & Negotiations

The sticker price for a ransomware attack hit a new milestone in 2025. The average demand rose to over $1,019,000, a sharp 47% YoY increase from $692,000. However, the numbers represent a wide range, as some victims faced demands as low as $9,000, while others were as high as $16 million.

Smaller demands were generally associated with opportunistic attacks against smaller businesses, in cases where threat actors scanned the internet and found an easy way into businesses' networks. Conversely, big-dollar demands were more likely to be connected to highly targeted attacks, where threat actors were aware of their victims' financial resources and adjusted demands accordingly.

Demand volatility was also driven by a diverse landscape of threat actors and variants. For example, Akira (linked to 25% of ransomware events) was associated with average demands of $926,000 (Figures 4.4, 4.5). Qilin (12%) pushed higher with an average of $1,167,000, while the most aggressive ransom demands were linked to RansomHub (7%) with an average of $2,331,000.

Ransomware Claims by Threat Actors or Variants[7] *FIGURE 4.4*



Divergent Demands: Top Ransomware Threat Actors or Variants[7] *FIGURE 4.5*

Threat Actor or Variant	Average	Median	Minimum	Maximum
Akira	$925,666	$670,000	$150,000	$4,900,000
Qilin	$1,167,187	$175,000	$15,000	$10,000,000
RansomHub	$2,331,250	$525,000	$70,000	$9,000,000

7. Data based on incidents where ransomware variant was confirmed by forensic investigators.

The Art of Ransomware Negotiation

Despite rising ransom demands, businesses increasingly refused to pay. Only 14% of victims chose to settle with attackers in 2025, suggesting that businesses are improving their resiliency with viable data backups and incident response plans. Ransomware victims that walked away from the table faced an average initial demand of $1,139,000, whereas those that paid faced a lower initial demand average of $873,000.

For the businesses that decide payment is necessary, the first number demanded is rarely the final ransom paid. In 2025, negotiators at Coalition Incident Response (CIR) and other panel firms directly engaged threat actors and successfully cut initial demands by 65% on average. This pushback moved the average starting demand for paying victims from roughly $873,000 down to a final average payment of $355,000.

The average ransom payment was higher than the median payment of $200,000, providing a more realistic view of what most businesses actually experienced. This gap shows how a few multimillion-dollar payouts tied to certain variants and threat actor groups, like Play and RansomHub, can skew the average, even while half of all victims are settling for significantly less.

Ransomware demands have jumped significantly in the past year, but the ransomware economy is under pressure. Between the 86% of organizations refusing to pay and the deep reductions secured by those who do, the leverage is moving back to the side of the defenders. Attackers are finding that as their demands get more aggressive, their chances of actually getting paid continue to drop.

$1.1M+ average initial demand

$355K average ransom paid

65% average reduction via negotiation

CASE STUDY

Negotiating a Path to Ransomware Recovery

A consulting firm experienced a dual extortion ransomware attack after being hit by the Akira threat actor group. The firm intended to restore from backups, but faced loss of critical operational data after the backups failed. Recognizing the threat to the firm's reputation and business continuity, CIR stepped in to manage the crisis and initiate contact with the threat actor. CIR successfully negotiated the initial $500,000 ransom demand down to $300,000. The firm's Breach Response and Cyber Extortion coverages handled costs for breach counsel, CIR, and the ransom payment, while its Extra Expenses coverage funded over $20,000 for IT consultants to assist with remediation, bringing the total claim cost to roughly $400,000.

The Mechanics of Initial Access in Ransomware

An initial access vector (IAV) describes how an attacker gains access to a network. To understand the anatomy of a ransomware attack, we look at both the compromised technology (the targeted device or software) and the attack vector (the method of compromise). While the root cause cannot always be determined in ransomware cases, many claims in 2025 skewed toward technical exploits, with attackers increasingly targeting the very security tools designed to keep them out.

Targeted technologies

Virtual private networks (VPNs) were the primary technology focus for ransomware attackers, accounting for 59% of all incidents where a specific targeted technology was confirmed by forensic investigators (Figure 4.6). While SSL VPNs are designed to be internet-facing to facilitate remote access, this exposure makes them a high-value target.

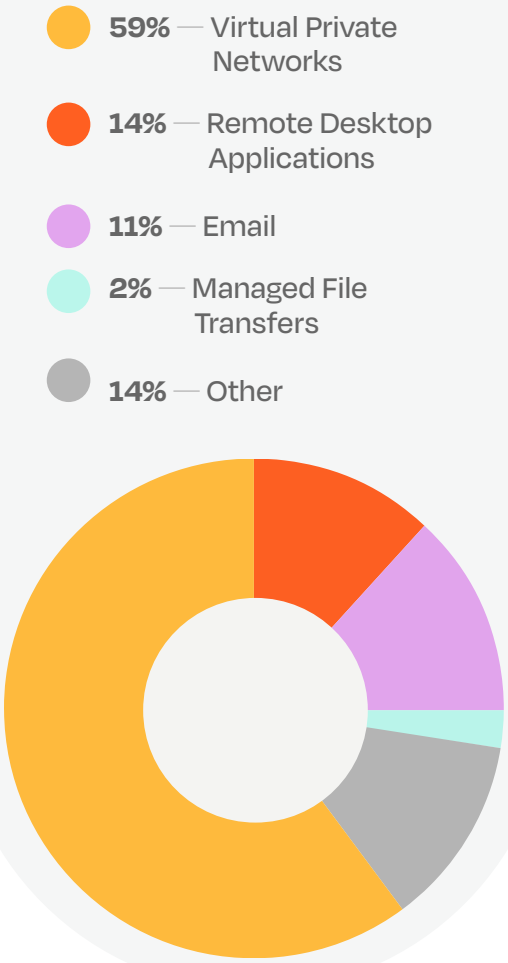
The mere presence of a VPN is a risk in today's threat environment. Coalition policyholders that choose to use SSL VPNs instead of migrating to safer solutions, such as Zero Trust Network Access (ZTNA), are advised to reinforce their technologies with two critical controls: universally enforced multi-factor authentication (MFA) and rigorous patch management.

In 2025, a small group of vendors that provide perimeter security appliances (not only VPNs but firewalls and other boundary devices) accounted for a majority of perimeter compromises in ransomware attacks. SonicWall was the most frequently targeted, followed by Fortinet, Cisco, Citrix, and Palo Alto Networks.

Attackers move with extreme speed to exploit vulnerabilities in these devices. To mitigate this risk, businesses that cannot yet migrate to ZTNA should ensure MFA is enforced across all users and embrace real-time advisories (like Coalition's Zero-Day Alerts) to identify when a technology requires immediate patching, effectively closing the window of opportunity for attackers.

2025 Ransomware Claims by Targeted Technologies[8]

FIGURE 4.6



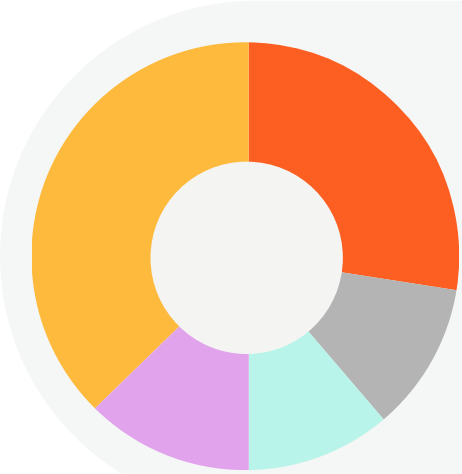
Top 5 Vendors Targeted in 2025 Ransomware Claims

1. SonicWall
2. Fortinet
3. Cisco
4. Citrix
5. Palo Alto Networks

8. Data based on incidents where compromised technology was confirmed by forensic investigators.

Beyond the network perimeter, remote desktop applications were another standout critical exposure, accounting for 14% of exploited technologies in ransomware events. Microsoft's Remote Desktop Protocol (RDP) is the most frequently targeted tool in this category of products; these technologies provide remote users with direct access to a system that often allows the ability to move laterally and deploy ransomware broadly across the corporate network.

By contrast, email represents a smaller share of the compromised technology landscape. The data suggests that attackers are finding more direct pathways to system control through perimeter appliances and remote access protocols than through traditional email infrastructure, though on-premises Microsoft Exchange remains a notable target within forensics investigations, particularly when web-based login and administration pages are exposed to the public internet.



2025 Ransomware Claims by Attack Vector[10]

FIGURE 4.7

- **38%** — Software Exploits
- **27%** — Compromised Credentials
- **14%** — Malware
- **11%** — Social Engineering
- **10%** — Other

Attack Vectors

Initial access for ransomware was driven by a combination of technical vulnerabilities and identity exploitation. Software exploits were the most common attack vector, observed in 38% of ransomware incidents where forensic investigators confirmed the attack vector (Figure 4.7), an indication that attackers are frequently utilizing automated tools to scan for and weaponize unpatched vulnerabilities in internet-facing devices.

Compromised credentials followed as the second-most common vector at 27%, highlighting that stolen or guessed passwords remain a primary threat to network integrity. Malware (14%), social engineering (11%), and other methods continued to play a role in the initial breach, often involving tactics like manipulating employees into installing remote access technology or clicking malicious links.

For businesses, this claims activity emphasizes that maintaining a secure perimeter requires a dual focus on rigorous patching and robust identity management.

Get That Off the Internet!

Businesses that expose critical technologies to the public internet are significantly more likely to experience a cyber incident.[9]

- **VPN Login Panels:** 3x-4x more likely
- **Remote Desktop Applications:** 3x-8x more likely
- **On-Prem Exchange Login Pages:** 4x more likely

Want to dive deeper into critical security exposures? **Check out our guide, Get That Off the Internet! >**

9. Calculation based on frequency of cyber incidents experienced by Coalition policyholders using a certain technology relative to all other Coalition policyholders that do not use said technology. See Methodology for more information. 10. Data based on incidents where the attack vector was confirmed by forensic investigators.

THE RESIDUAL THREATS

Miscellaneous First-Party Loss

How human & technical failures disrupt business operations

Third-party breaches accounted for 15% of all miscellaneous first-party loss events, with an average loss of $30,000.

While BEC, FTF, and ransomware comprise the majority of cyber insurance claims, many other types of first-party events can be just as disruptive. These miscellaneous first-party loss claims are varied, often unpredictable events that can expose the fragility of a business' operations, technology, and internal processes. Even when an attacker doesn't demand a ransom or spoof a wire transfer, these events force organizations to divert critical time, money, and resources toward remediation.

The Domino Effect of Third-Party Dependencies

The fallout from dependencies on external partners was a significant driver of claims in 2025. **Third-party breaches** accounted for 15% of all miscellaneous first-party loss events, with an average loss of $30,000 (Figures 5.1, 5.2). In a third-party breach, a vendor or supplier suffered a cyber incident that exposed the business' data or disrupted its operations, forcing the business to respond even though its own systems weren't breached. Similarly, **third-party account compromise** — when an attacker accesses a business' account on a cloud, SaaS platform, or online service that results in data loss or unauthorized activity — accounted for 5% of claims.

CASE STUDY

The Ripple Effect of a Third-Party Breach

A Canadian healthcare provider was swept into the global Salesloft Drift breach after a threat actor exploited an API key in its chatbot application. The breach exposed the sensitive health records of nearly 6,000 patients stored within the business' internal service tickets. Forensic analysis identified 165 malicious requests, but no evidence of large-scale data exfiltration. The business responded by notifying regulators and providing nationwide credit monitoring to impacted patients. In total, the policy's Breach Response coverage paid more than $42,000 in losses.

Internal Failures and Malice

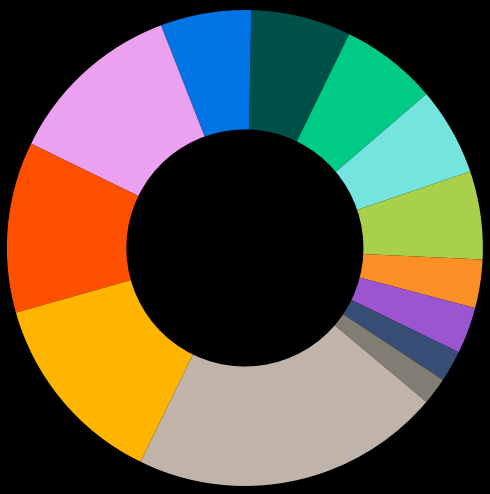
The frequency of miscellaneous first-party loss events is often driven by external partners, but the most severe financial hits commonly originate from within the business or through direct system interference. **Invoice manipulation** accounted for 6% of claims, with an average loss of $59,000; these claims involve an attacker altering billing information directly within a business' systems, leading to incorrect payments without a traditional email-based deception.

Stolen or misplaced property or data accounted for 5% of claims. These claims occur when physical devices, documents, or storage media containing business or customer information are lost or stolen, requiring recovery and breach evaluation.

Insider threats — when a current or former employee intentionally misuses system access and causes financial loss, data damage, or operational disruption — accounted for 5% of claims. **System failures** accounted for 4% of claims, pertaining to the failure of a critical system due to a technical glitch, bug, or outage, resulting in business interruption or data loss.

Miscellaneous First-Party Loss by Event Type

FIGURE 5.1



- **17%** — Unauthorized Access
- **15%** — Third-Party Breach
- **8%** — Email or Domain Impersonation
- **7%** — Inadvertent Disclosure
- **6%** — Malware Only
- **6%** — Invoice Manipulation
- **5%** — Third-Party Account Compromise
- **5%** — Stolen or Misplaced Property or Data
- **5%** — Insider Threats
- **4%** — System Failure
- **1%** — Negative Publicity
- **1%** — Denial of Service
- **20%** — Unknown Security Failure

Technical & Reputational Friction

The remainder of the miscellaneous first-party loss landscape covers persistent threats that disrupt daily business operations. **Unknown security failures** accounted for 20% of claims, with an average loss of $43,000. These are confirmed security breakdowns where a specific cause or method cannot be determined, yet the business is still required to remediate the issue. **Unauthorized access** accounted for 17% of claims, with an average loss of $44,000. These claims involve a business' systems or data being accessed without permission, but don't lead to malware deployment or data theft.

Email or domain impersonation accounted for 8% of claims, with an average loss of $37,000, occurring when an attacker spoofs an email address or brand to target customers, causing reputational harm and internal response costs. **Malware** accounted for 6% of claims, with an average loss of $45,000. These claims occur when malicious software infiltrates systems and disrupts operations without data theft or a ransom demand.

Inadvertent disclosure accounted for 7% of claims, with an average loss of $17,000, occurring when a business accidentally exposes sensitive information that results in internal investigation and remediation. **Denial of service (DoS)** accounted for 1% of claims; this is when an attacker overwhelms a system with traffic, causing outages, downtime, and recovery expenses. Finally, negative publicity (1%) highlights that harmful online attention often requires crisis communication support to mitigate long-term damage.

Though these claim types are diverse, they all share a direct impact on the impacted business, whether lost productivity, investigation and remediation costs, reputational damage, or unplanned security improvements.

Misc. First-Party Loss Severity by Event Type[11] *FIGURE 5.2*

Event Type	Average Loss
Email/Domain Impersonation	**$38,835**
Inadvertent Disclosure	**$16,512**
Invoice Manipulation	**$59,376**
Malware Only	**$44,982**
Third-Party Breach	**$30,377**
Unauthorized Access	**$43,974**
Unknown Security Failure	**$43,129**

11. Severity of some miscellaneous first-party loss claims not provided due to insufficient statistical significance.

THE EXTERNAL LIABILITY

Third-Party Allegations

How duty of care & legal obligations shape cyber incidents

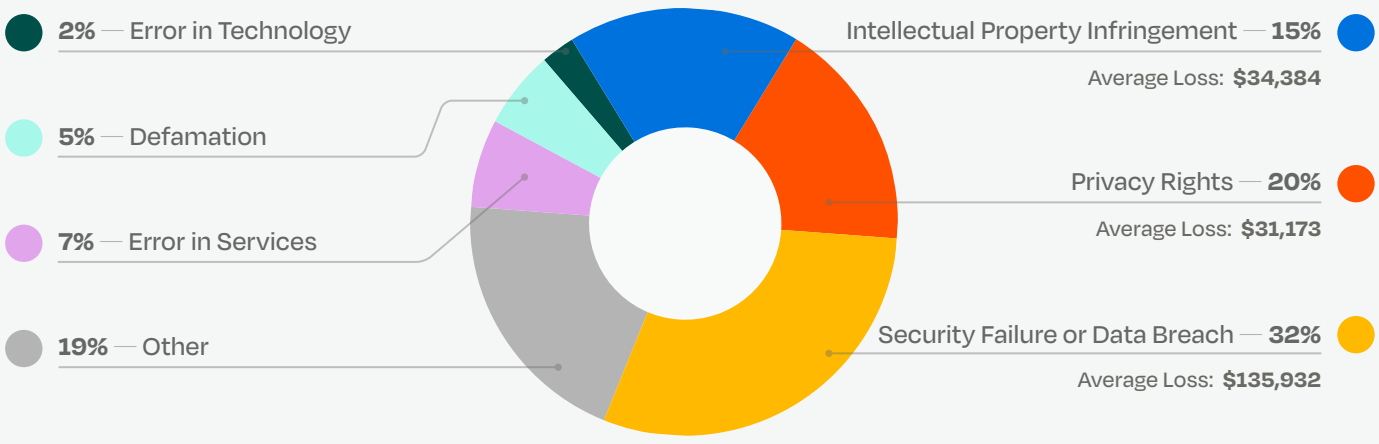
Third-party allegations refer to claims made against a business by external entities — customers, vendors, regulators, etc. — due to a cyber incident, privacy breach, or professional error that caused harm or legal liability. Unlike first-party losses, which cover a business' immediate recovery costs, these allegations arise when outside parties seek to hold the business legally responsible for the fallout of a security or privacy failure. These claims highlight a landscape where the cost of a breach is often defined by the litigation and settlements that follow the initial event.

The High-Severity Risks of Data Custodianship

The most significant financial exposures among third-party allegations stem from the failure to secure data and uphold the fundamental data rights of individuals. **Security failure or data breach allegations** accounted for 32% of all third-party claims, with an average loss of $136,000 (Figure 6.1). These claims arise when a business' systems are compromised and expose a third party's data, leading the affected party, or a regulator, to allege the business failed to adequately protect that information.

Third-Party Allegations by Event Type[12]

FIGURE 6.1



12. One outlier claim pertaining to security failure or data breach allegations omitted from calculation.

Privacy rights violations accounted for 20% of third-party allegations, with an average loss of $31,000. These claims occur when a third party alleges a business either violated legally protected privacy rights through its digital operations or data practices or handled personal data in a way that conflicts with its own stated privacy policy, leading to allegations of misused or improperly disclosed information.

Technical and Professional Errors

Third-party liability claims often extended beyond the data itself to the actual performance and integrity of a business' digital products and services. **Errors in technology** accounted for 2% of claims, arising when a flaw, defect, or failure in a business' software, platform, or digital product causes harm or financial loss to a customer. **Errors in services**, which accounted for 7% of claims, occur when a mistake or failure in the technology-related services a business provides leads to client losses.

Reputational Risks in Digital Communication

The remainder of the third-party landscape was driven by the legal risks inherent in digital content and communication. **Intellectual property infringement** accounted for 15% of claims. This occurs when a third party claims a business unlawfully used trademarked, copyrighted, or other IP material in its digital content, products, or marketing. **Defamation** — when a business allegedly makes false or misleading statements online or in digital communications that damage another party's reputation — accounted for 5% of claims.

While these claims may not always stem from an attack, they underscore the broad surface for legal liability created by a business' digital footprint and brand activities.

CASE STUDY

Mitigating a Multimillion-Dollar Copyright Dispute

A real estate firm faced a $3.2 million demand letter after a music publisher alleged the unauthorized use of copyrighted tracks across the firm's social media accounts. The demand cited 347 instances of infringement, with potential legal fees projected to reach an additional $1.5 million if the case went to trial. Coalition appointed specialized defense counsel to challenge the publisher's "per use" valuation and, through strategic negotiations and the application of market benchmarks, avoided a costly trial by securing a $1.7 million settlement. Because the firm held concurrent insurance coverage, Coalition successfully coordinated with the other carrier to split the loss, significantly reducing the direct impact on the firm's Media Liability coverage limits.

The Emerging Frontier of Privacy Rights

Compared to established threats like ransomware, allegations of privacy rights violations represent a small portion of cyber claims. Yet, they constitute a fast-moving frontier of legal exposure. These **web privacy claims** are increasingly driven by a repeatable formula: plaintiffs' attorneys utilizing decades-old statutes to target the everyday tracking technologies embedded in modern websites.

Across all reported allegations of privacy rights violations in 2025, the data reveals a clear concentration of risk around specific legal and technical citations:

- **72% cited the California Invasion of Privacy Act (CIPA):** Originally written in 1967 to prevent telephone wiretapping, CIPA is now the primary framework used to allege that web-tracking technologies (like "session replay" or chat features) constitute the unlawful interception of digital communications.
- **11% cited Meta Pixel:** A significant portion of privacy rights violations was tied specifically to this pervasive web tracking tool. Third-party allegations typically center on the wrongful collection of data, where sensitive user information is shared with third-party platforms without clear user consent.
- **6% cited the Telephone Consumer Protection Act (TCPA):** Claims under this act remained a consistent factor in the privacy landscape, primarily targeting businesses for unauthorized digital outreach, such as unsolicited text-based marketing.

Web privacy risk now extends far beyond defending against attackers. It's an ever-present digital threat that hinges on how data is collected and shared, as evidenced by the fact that the vast majority of privacy rights allegations, or "wrongful collection" claims, in 2025 relied on modern interpretations of older laws.

Interested in learning more about how wrongful collection is redefining digital risk? **Read our new report, The State of Web Privacy >**

SECTOR DYNAMICS

Claims by Industry

How sector-specific data & operational value influence cyber risk

Industry plays a significant role in shaping a business' overall cyber risk, influencing both the frequency and severity of claims. Organizations that handle high volumes of sensitive financial data, personal health information, or proprietary intellectual property are often primary targets due to the high resale value of their data. Conversely, sectors tied to critical infrastructure face heightened risks from ransomware campaigns that prioritize operational disruption over simple data theft.

Stability & Resilience

Despite being a high-value target, the average loss in financial services was among the lowest at $64,000.

Real Estate

Real estate maintained the lowest frequency of claims among the industries tracked at 0.84%, though its average loss was a notable $125,000 (Figures 7.1, 7.2). This suggests that while attacks on developers and brokerages are less common, they are often high-stakes events, likely involving significant funds transfer fraud or large-scale data theft.

Financial Services

Despite being a high-value target, the average loss in financial services was among the lowest at $64,000. This may reflect the maturity of cybersecurity strategies in banking, finance, and insurance, where robust incident response and continuity planning often mitigates the total financial fallout of a breach.

Nonprofit

Organizations in this space saw relatively low frequency and a low average severity at $83,000. While these organizations are still susceptible to phishing and credential theft, the financial stakes often remain lower than for-profit sectors.

High-Frequency Sectors

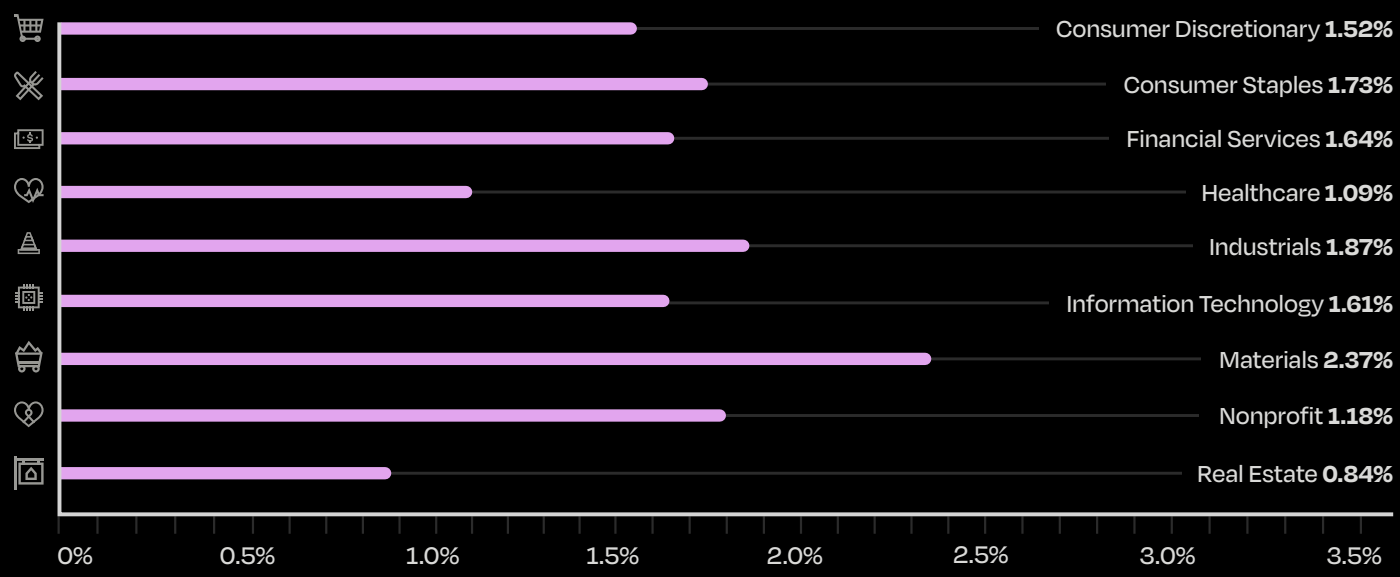
Materials

Materials saw the highest frequency of claims in 2025, with an average loss of $133,000. The complexity of mining, chemical, and plastics supply chains — combined with a heavy reliance on industrial control systems — makes these businesses frequent targets for both opportunistic and targeted attacks.

Industrials

Construction, manufacturing, and engineering firms continued to face significant attack pressure, with an average loss of $115,000. These businesses are often targeted by attackers looking to exploit the just-in-time nature of their operations through ransomware and extortion.

Claims Frequency by Industry *FIGURE 7.1*



High-Severity Outliers

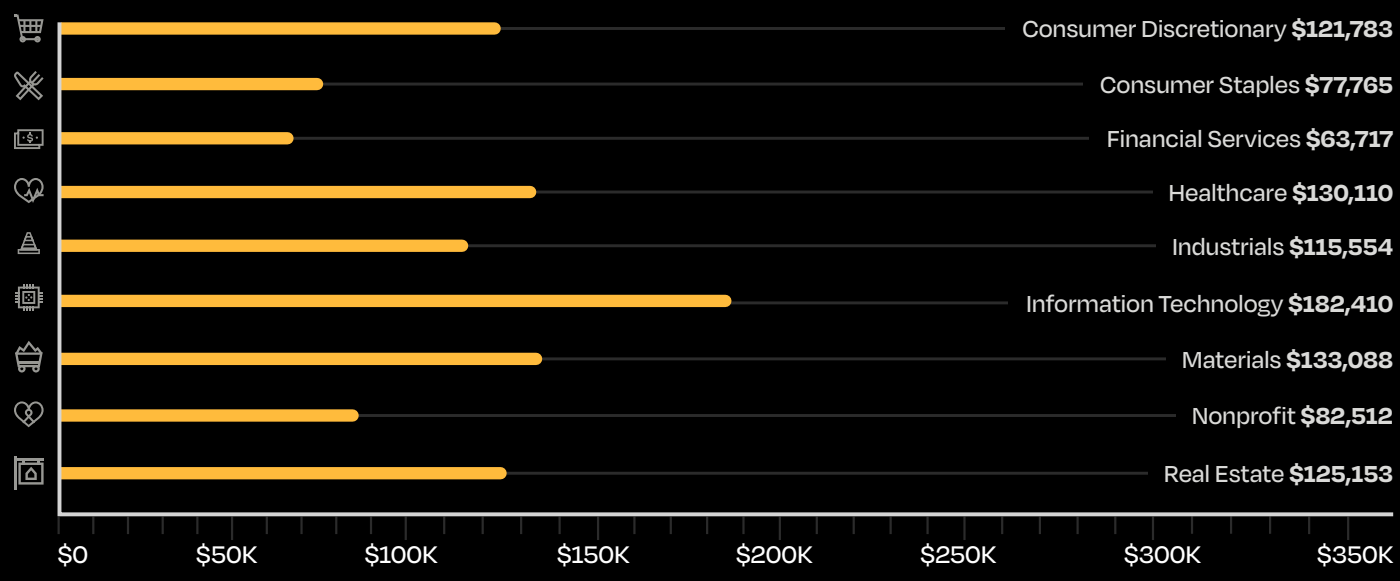
Information Technology

While its frequency sits in the middle of the pack, the IT sector faced a higher average loss at $182,000. This reflects the force multiplier effect of tech-sector breaches; when a hardware or software provider is hit, the cost to remediate and the potential for downstream liability significantly drive up the claim value.

Healthcare

Healthcare maintained a lower claims frequency than other sectors, but its average loss was high at $130,000. The sensitivity of protected health information and the critical need for 24/7 uptime in hospitals and clinics ensure that any incident in this space carries a heavy price tag.

Claims Severity by Industry *FIGURE 7.2*



SECTOR DYNAMICS

Claims by Revenue

How organizational scale & resources influence cyber exposure

Cyber risk impacts businesses differently based on their size, complexity, and available resources. While small and midsize businesses (SMBs) often face devastating consequences relative to their size due to limited in-house security expertise, larger organizations face highly targeted attacks due to their vast digital footprints. In 2025, the data revealed a clear trend: while the cost to remediate individual claims is trending downward, the likelihood of experiencing an event increases significantly as a company moves up the revenue ladder.

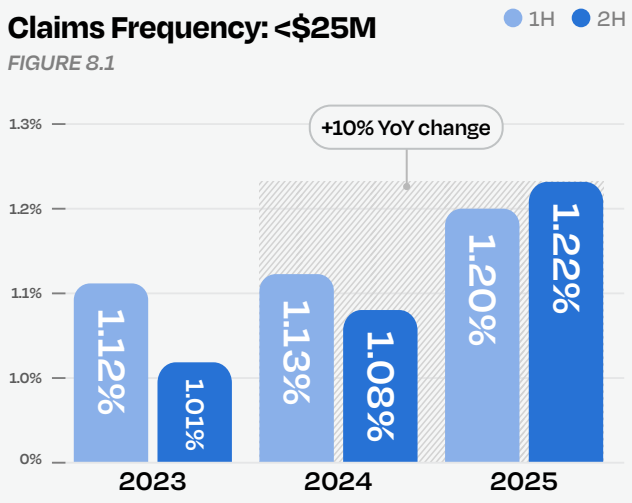
Micro SMBs: A Rising Tide of Frequency

Businesses with less than $25 million in revenue (<$25M) saw a notable shift in 2025 as attackers increasingly automated their efforts to find unpatched vulnerabilities in smaller perimeters. These micro SMBs experienced a 1.21% claims frequency, representing a 10% YoY increase from the 1.10% seen in 2024 (Figure 8.1). This steady rise throughout the year suggests that these organizations are no longer under the radar for opportunistic attackers.

While frequency was up, the financial impact per event was the lowest of any segment. Claims severity for micro SMBs decreased 15% YoY to an average loss of $77,000 (Figure 8.2). Despite the lower dollar amounts, a $77,000 loss can be far more disruptive to a micro SMB balance sheet than a six-figure loss is to a large enterprise.

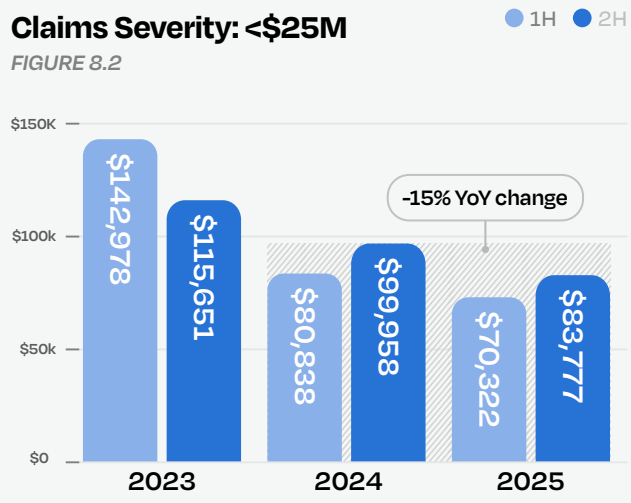
Claims Frequency: <$25M

FIGURE 8.1



Claims Severity: <$25M

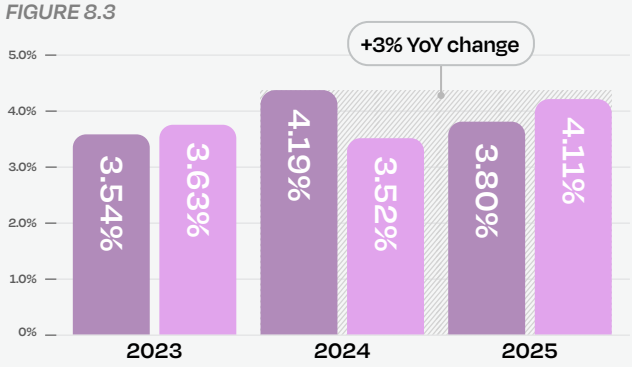
FIGURE 8.2



Claims Frequency: $25M-$100M

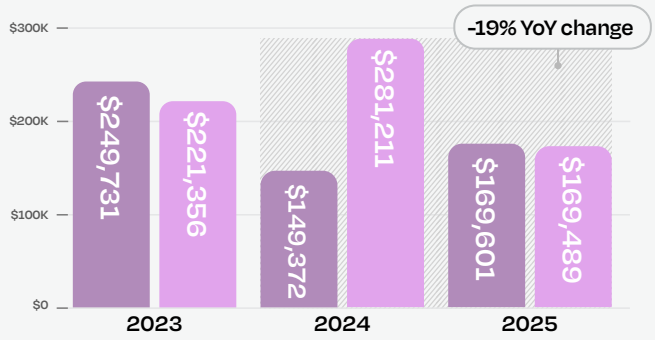
1H 2H

FIGURE 8.3



Claims Frequency: $25M-$100M

FIGURE 8.3



SMBs: Navigating Volatility

The traditional SMB segment remains a volatile area of the cyber landscape, often serving as a proving ground for more sophisticated attack methods. Among businesses between $25 million and $100 million in revenue ($25M-$100M), claims frequency rose to 3.96% in 2025, a 3% increase over the previous year. This cohort often finds itself in a difficult position: possessing enough digital assets to be an attractive target for attackers, but sometimes lacking the enterprise-grade security operations center (SOC) capabilities of the largest firms.

However, there's a silver lining in the financial fallout, as claims severity decreased 19% YoY to an average loss of $170,000. This trend — down from a 2024 full-year average of $211,000 — indicates that as these businesses grow, their maturing response protocols are helping to prevent typical claims from ballooning into catastrophic costs. The stabilization of loss amounts in 2025 further suggests a strengthening of defensive postures within this revenue band.

Mid-Market & Enterprise: High Frequency & Targeted Pressure

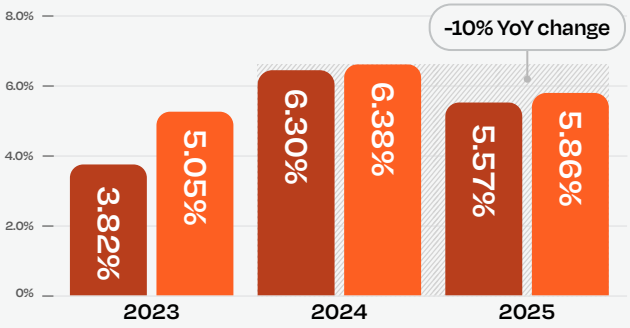
At the top of the revenue spectrum, the threat landscape is defined by volume and persistence. Businesses with more than $100 million in revenue ($100M+) continue to experience claims more often than any other segment. In 2025, claims frequency for this cohort was 5.72%, nearly five times higher than that of the smallest businesses.

Larger organizations present a massive attack surface that requires constant monitoring, but also possess the resources to contain threats more effectively. The financial impact of these claims saw a shift as severity fell 7% YoY to an average loss of $268,000. The steady decline from a 2024 average of $289,000 suggests that large enterprises are becoming more effective at rapid containment, effectively lowering the ceiling on the cost of a breach despite the high frequency of attempts.

Claims Frequency: $100M+

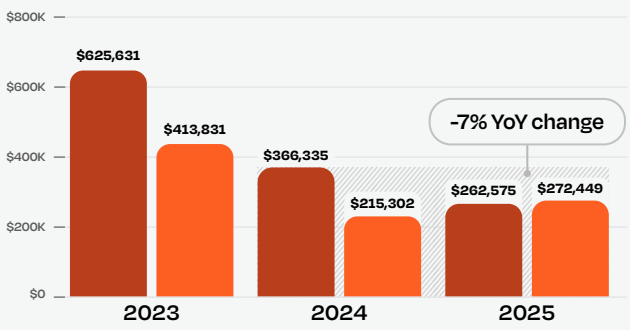
1H 2H

FIGURE 8.5



Claims Severity: $100M+

FIGURE 8.6

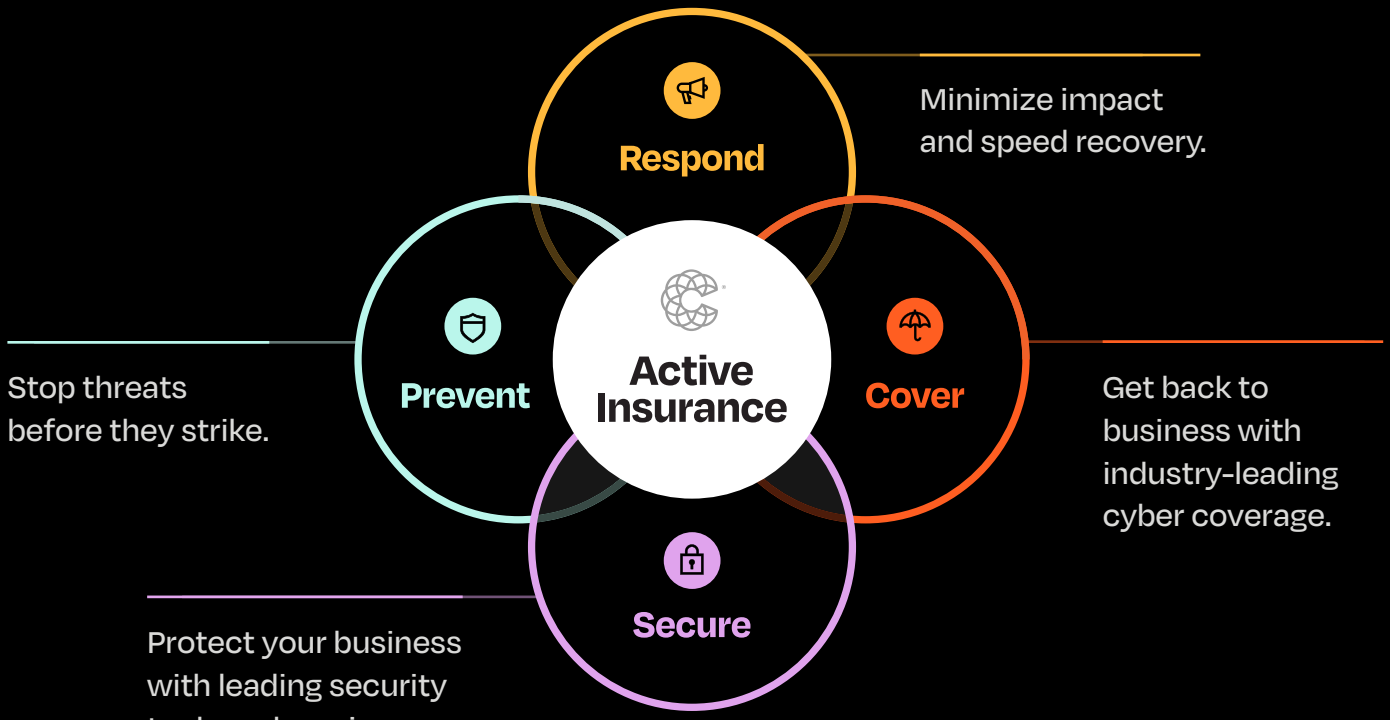


THE PATH FORWARD

Overcoming the Cyber Protection Paradox

How businesses can embrace Active Insurance

The Cyber Protection Paradox is a choice, not an inevitability. Coalition has proven that businesses can break the cycle of ineffective overspending by prioritizing collaboration and visibility over a fragmented collection of security tools. The shift toward resilience in 2025 is a testament to organizations that have moved beyond passive protection to embrace an active, data-driven defense.



The 4 Pillars of Active Insurance

Prevent: Spotting Threats Before They Strike

Coalition has helped businesses address over 175,000 critical security issues by identifying risks before they turn into claims, and the cost of inaction is stark: In 2025, 872 companies ignored critical alerts during the quoting process and later suffered ransomware attacks totaling $436 million in losses. Proactive visibility is key, yet 80% of businesses that reported a claim had never activated their Coalition Control® account, missing the opportunity to intercept threats early.

Respond: Expert Intervention in Minutes

When incidents occur, rapid intervention can prevent minor disruptions from becoming disasters. Our expert-led response ensures that the majority of reported incidents are contained quickly: In 2025, 64% of closed claims were resolved with no out-of-pocket loss for the policyholder. Furthermore, our claims team has recovered over $150 million in stolen funds since inception, while incident responders achieved a 65% average reduction in ransom demands in 2025 through negotiations.

Cover: Comprehensive Protection for the Digital Age

Industry-leading coverage helps provide the financial safety net that ensures a business remains whole. Our innovative policies are designed to prioritize liquidity and offer differentiated coverage to keep pace with an evolving risk landscape, while rewarding policyholders that take meaningful steps to improve their overall hygiene. Since inception, Coalition has handled 15,000 claims, and $723 million in losses have been paid.

Secure: Cybersecurity Proven to Protect

Coalition Security® offers additional security tools and technology built to protect against modern risks. Wirespeed's Automated Managed Detection & Response (MDR) analyzes security alerts in milliseconds, rapidly isolating compromised endpoints and delivering an 1,801 millisecond median time to verdict. By achieving a 99.9% reduction in alert noise, Wirespeed helps eliminate alert fatigue and provides an integrated defense that is proven to protect.

Our Mission: Protect the Unprotected

Active Insurance isn't your typical insurance that only engages after the damage is already done. We embrace an organic, continuous relationship and are invested in the long-term strength and health of every policyholder. The success of Active Insurance proves that the era of passive protection has passed. The future belongs to the businesses that embrace a holistic, active approach to cyber risk.

THE DETAILS

Methodology

Data integrity, classification standards & valuation criteria

The 2026 Cyber Claims Report is based on proprietary claims data reported by Coalition policyholders between January 1 and December 31, 2025. To ensure a direct year-over-year comparison and mitigate the bias of future loss development, Coalition's data scientists and actuaries evaluate all claims at a six-month maturity level rather than using ultimate loss projections. This standardized evaluation age allows for a consistent analysis of trends without the skew of long-tail development.

Refining Claims & Loss Signals

In 2025, Coalition received more than 4,000 reported claims, a broad designation encompassing everything from confirmed breaches to minor technical anomalies and abandoned claim inquiries. To provide the most accurate view of the cyber threats impacting modern businesses, we've narrowed our analysis to approximately 1,400 high-signal claims that resulted in a realized financial loss. Effective with this report, we've updated our minimum reporting threshold from a $10 gross loss to a $100 gross loss, a change designed to further remove "noise" from the data and focus on impactful events. As this criteria has been retroactively applied to historical data to maintain consistency, readers may notice a marginal decrease in historical frequency figures and a corresponding increase in historical severity figures compared to previous reports. By filtering out matters resolved without payment or where coverage did not apply, we ensure the data reflects the incidents that actually impacted a policyholder's bottom line. This refined criteria focuses the report on the threats that businesses should most prioritize in their defense strategies.

Classification & Geographic Scope

To allow for a clear analysis, every claim is categorized as a single event type. While one cyber event can lead to another, such as BEC evolving into ransomware, claims are weighted by their ultimate impact. Consequently, ransomware and FTF superseded BEC in our categorization due to the higher severity of these event types. Regarding geographic scope, claims data from policyholders in the US, Canada, the UK, Australia, and Germany are included in all global frequency and severity figures. All severity figures in this report have been standardized to US Dollars, regardless of where the claim originated.

Loss Valuation & Evaluation Criteria

Cyber claims unfold at varying speeds depending on the event type. For example, BEC and FTF incidents may be realized and closed rapidly, while ransomware and third-party allegations are far more intricate, developing over time as forensics, business interruption, and legal costs are finalized. We analyze these claims based on their most current valuation at the time of reporting.

Relative Claims Frequency

This report includes calculations and analysis on correlational risk related to the use of specific technology types. The calculation compares the frequency of cyber incidents experienced by Coalition policyholders using a certain technology relative to all other Coalition policyholders that do not use said technology. The analysis uses a univariate approach, which examines technology use in isolation. While univariate analysis is useful for spotting patterns and correlations, it does not establish causation. Other factors, such as company size, industry, or existing security practices, may also contribute to the difference in incident frequency.

Coalition®

coalitioninc.com

1 EMBARCADERO CENTER, SUITE 1200
SAN FRANCISCO, CA 94111