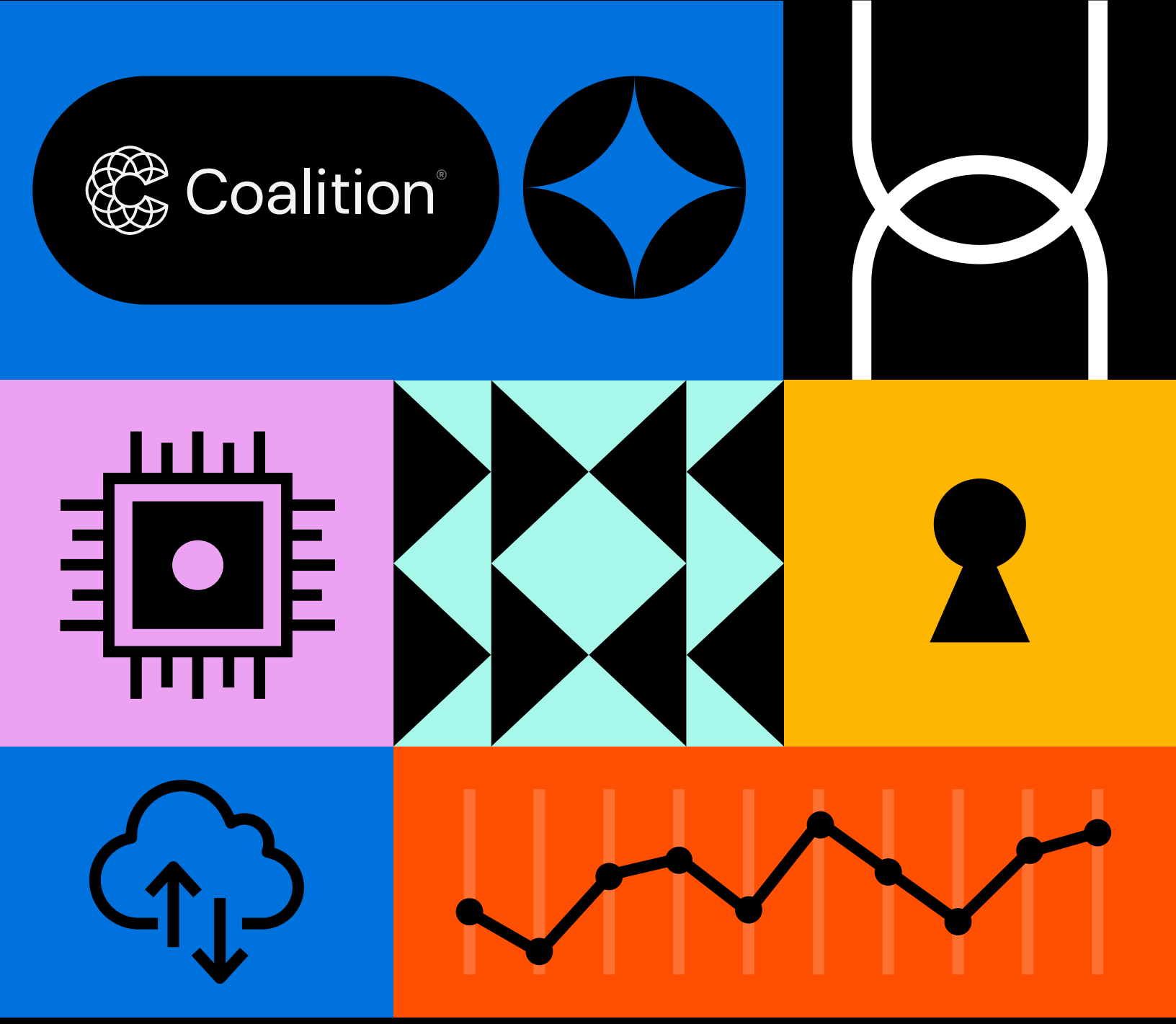


2024 Cyber Claims Report

Mid-year Update

Table of Contents

Executive Summary

We may very well remember 2024 as the year that businesses were first widely impacted by third-party disruptions. Between ransomware attacks on Change Healthcare and CDK Global and the global IT outage caused by CrowdStrike, high-profile cyber events are the new normal in cyber insurance.

Healthcare providers were blocked from processing insurance claims, bringing pharmacies' cash flow to a screeching halt and threatening patient access to vital care. Car dealerships were unable to conduct new sales and manage inventory, resulting in extended delays for customers and lost revenue for dealerships. Airlines were grounded, federal agencies were knocked offline, and emergency dispatchers resorted to pen and paper.

The common thread in these events is a shared dependency on technology, underscoring not only how many businesses rely on the same technology infrastructure to operate but also how fragile that technology can be. Third-party risk will continue to impact businesses of all sizes and industries, and cyber risk aggregation will remain a key consideration for cyber insurance providers.

Ultimately, claims activity in the first half of 2024 (1H 2024) has reaffirmed that the only constant in cyber is change. Threat actors returned to ransomware as a high-ROI cybercrime and further incorporated artificial intelligence into their tactics to infiltrate inboxes at scale. Meanwhile, as once-popular wire fraud efforts decreased, attackers targeted web-accessible applications and other risky technologies at a higher rate.

Key findings

- **Ransomware drove a 14% increase in overall claims severity.** With an average loss amount of $353,000, ransomware reared its ugly head yet again. Despite the spike, ransom demands were cut in half through successful negotiations.
- **Business email compromise (BEC) was the leading cyber event.** Continuing a steady trend that spanned all of 2023, BEC frequency increased 4% and accounted for nearly one-third of all claims.
- **Funds transfer fraud (FTF) continued a steady decline.** After nationwide fraud losses reached $10 billion in 2023, FTF initial severity decreased 15% to an average loss of $218,000.
- **Exposed login panels tripled a business' likelihood of attack.** Due to threat actors trolling the internet for easy access, businesses using web-accessible applications were 3.1 times more likely to experience a claim.

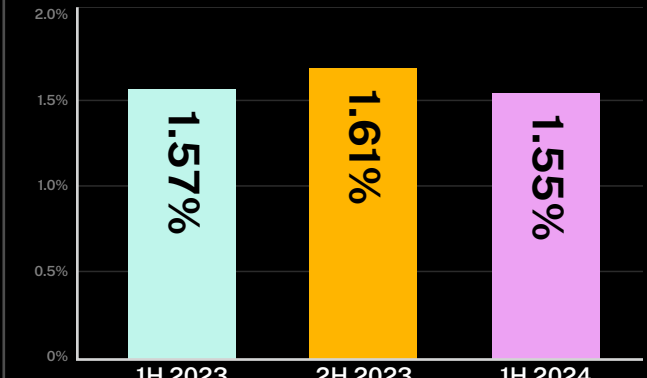
This report features statistics, charts, and risk insights based on data from businesses in the United States, Canada, the United Kingdom, and Australia. Cyber risk is global, and we believe the trends and risk mitigation strategies in this report are widely relevant and applicable. As an active partner in protecting businesses from digital risk, Coalition is proud to share these insights to help businesses, brokers, and security professionals stay informed about the ever-changing cyber threat landscape.

Claims Severity Climbed as Ransomware Became More Costly

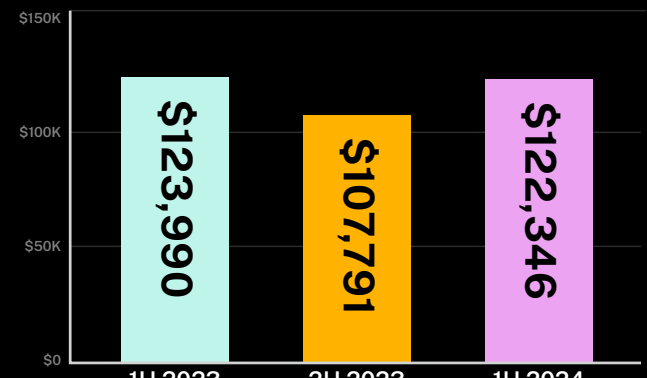
Threat actors targeted larger businesses and reaped the benefits with increased paydays.

Overall claims frequency decreased in 1H 2024, dropping from 1.61% to 1.55%, the lowest since 2H 2022 (Figure 1.1). However, overall claims severity increased 14% to an average loss amount of $122,000, largely driven by a spike in ransomware severity (Figure 1.2). Threat actors targeted larger businesses and reaped the benefits with increased paydays.

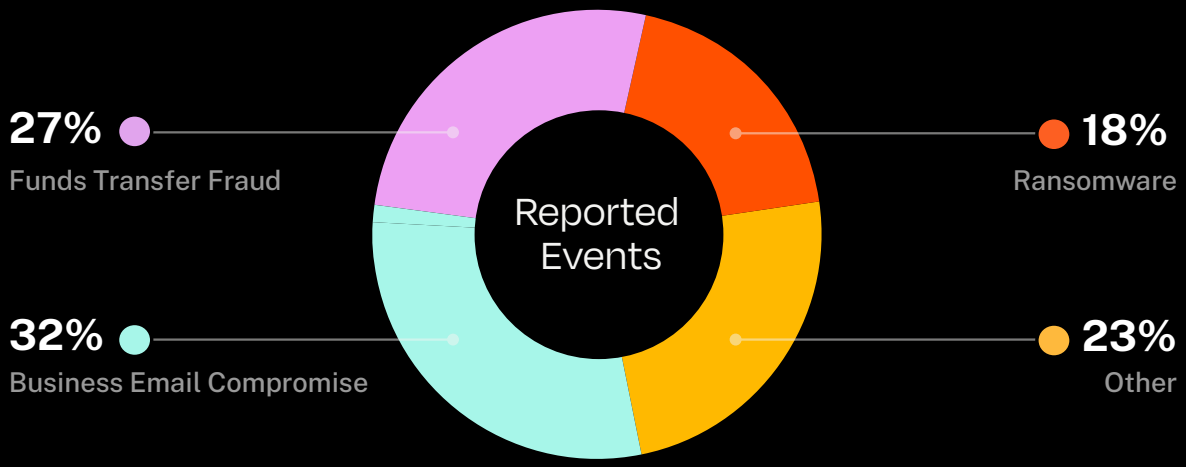
Overall Claims Frequency *(Figure 1.1)*



Overall Claims Severity *(Figure 1.2)*



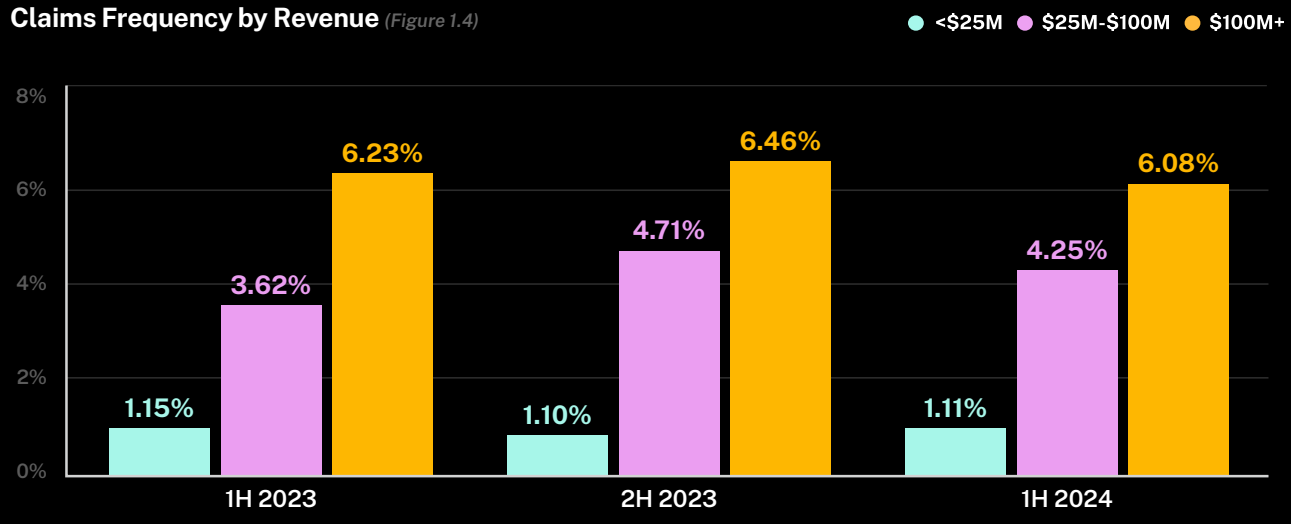
Claims by Event Type *(Figure 1.3)*



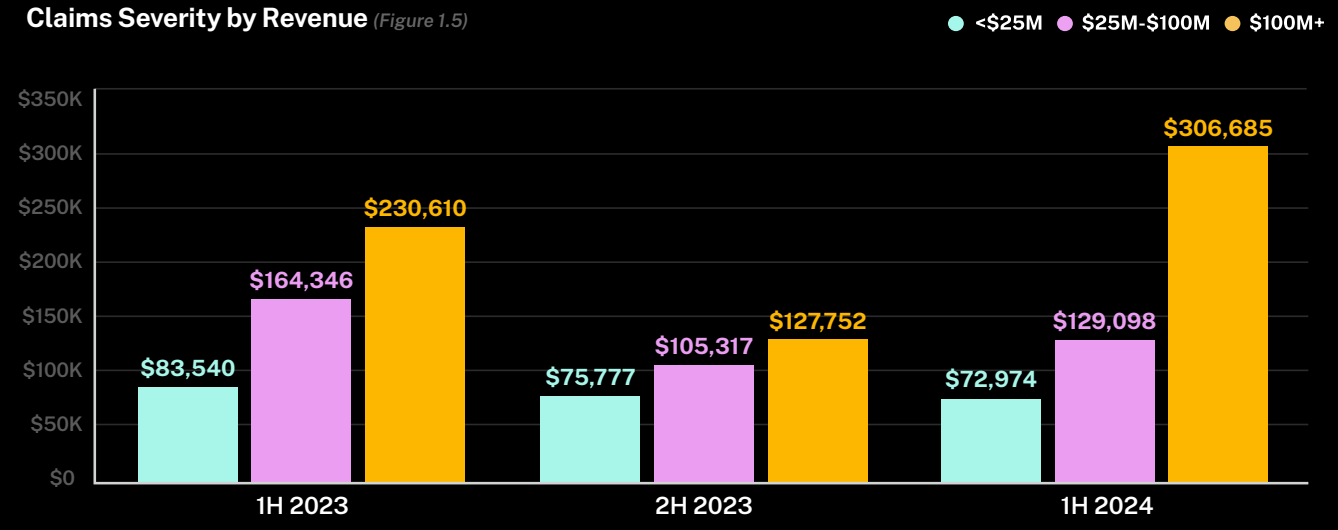
Business email compromise (BEC) accounted for nearly one-third of all reported claims in 1H 2024, marking a 9% increase for the historically low-severity event type (Figure 1.3). The increases are largely attributable to businesses between $25 million and $100 million in revenue ($25M-$100M) and businesses with more than $100 million in revenue ($100M+).

Overall claims frequency among businesses with $25M-$100M in revenue decreased 10% in 1H 2024 (Figure 1.4). Businesses with $100M+ in revenue dipped 6%, while businesses with less than $25 million in revenue (<$25M) increased 1%.

Claims Frequency by Revenue *(Figure 1.4)*



Claims Severity by Revenue *(Figure 1.5)*



Claims severity among businesses with $100M+ in revenue spiked 140% in 1H 2024 to an average loss amount of $307,000 — a historic high for this cohort.

The decreases in claims frequency among both businesses with $25M-$100M in revenue and businesses with $100M+ in revenue were more than offset by increases in claims severity.

Claims severity among businesses with $100M+ in revenue spiked 140% in 1H 2024 to an average loss amount of $307,000 — a historic high for this cohort. Businesses with $25M-$100M in revenue increased 23% to an average loss of $129,000, though businesses with <$25M in revenue dipped 4% to an average of $73,000.

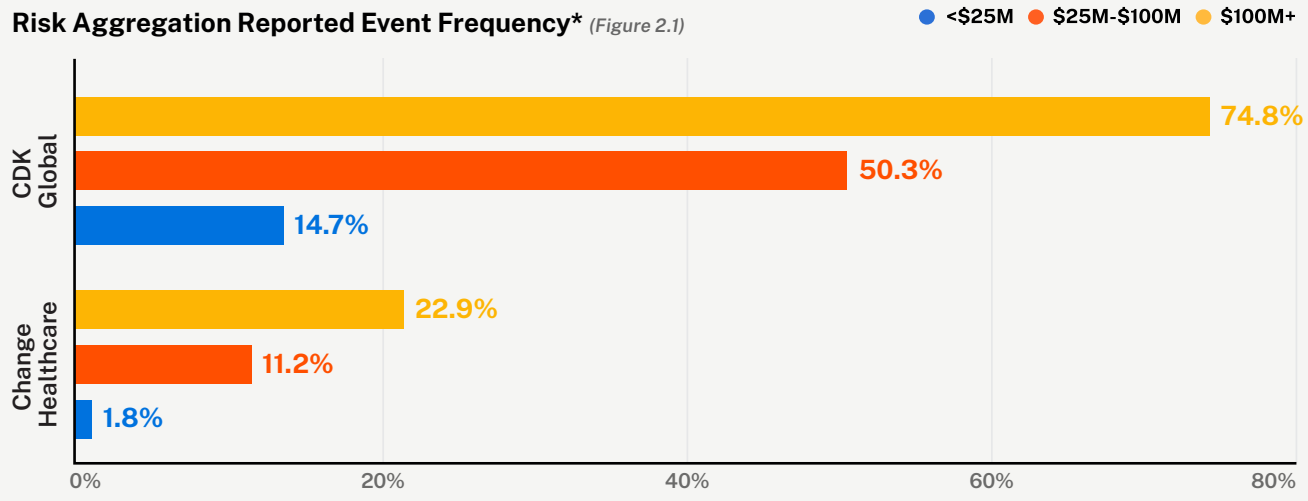
Third-Party Disruption Created Aggregate Risk, Hit Large SMBs and Mid-Market at Higher Rate

Nearly 23% of healthcare businesses with $100M+ in revenue were impacted by the Change Healthcare attack, as were 11% of those with $25M-$100M in revenue.

Two material cyber risk aggregation events occurred in 1H 2024: Change Healthcare and CDK Global. A risk aggregation event is a single cyber event that causes widespread loss to other organizations; an event is deemed "material" based on the number of impacted policyholders. Importantly, the global CrowdStrike outage in July also constitutes an aggregation event but occurred in the latter half of 2024 and will be further analyzed in our 2025 Cyber Claims Report.

Change Healthcare, a technology company that processes transactions among pharmacies, care providers, and insurers, experienced a ransomware attack in February and was unable to provide critical services for more than a month. Across the US, the disruption impacted more than 90% of pharmacies[1] with total losses projected to reach $1.6 billion.[2] Nearly 23% of healthcare businesses with $100M+ in revenue were impacted by the Change Healthcare attack, as were 11% of those with $25M-$100M in revenue (Figure 2.1).

Risk Aggregation Reported Event Frequency* *(Figure 2.1)*



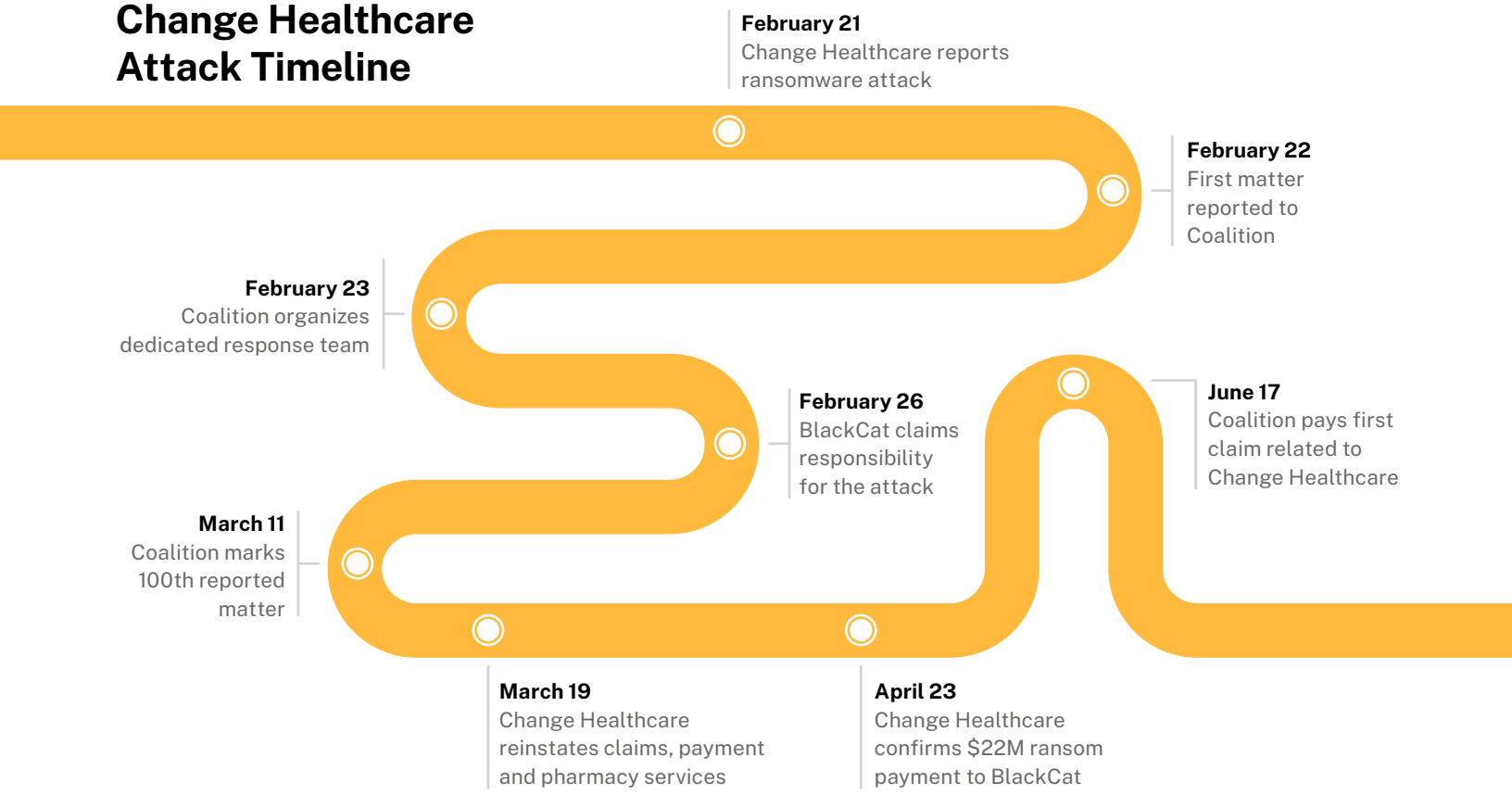
*Change Healthcare event frequency specific to healthcare industry; CDK Global event frequency specific to auto dealers.

CDK Global, a software vendor that facilitates vehicle sales, financing, and inventory management for car dealerships, suffered a ransomware attack in June that caused significant disruption across a network of 15,000 auto dealers. Total direct losses to impacted car dealerships are estimated at $1 billion.[3] Nearly 75% of auto dealers with $100M+ in revenue were impacted by the CDK Global ransomware event.

Most reported matters arising from these events didn't result in insurable loss, though these events had significant impact and reach. Policyholders that suddenly lost access to crucial business systems were relieved that they could speak to a knowledgeable claims handler familiar with the situation. In response to these aggregation events, Coalition assembled a focused team of claims handlers to respond. Our claims team also arranged dedicated resources at Coalition's panel privacy firms to represent affected policyholders.

By focusing our response to dedicated handlers and counsel, Coalition was able to ensure policyholders' interests were protected when dealing with the impacted parties. By keeping in regular communication with policyholders and breach counsel, we were also able to share information about likely timelines for restoration, as well as viable alternative software and manual workarounds.

Change Healthcare Attack Timeline



1. *The Washington Post, U.S. prescription drug market in disarray as ransomware gang attacks*
2. *Cybersecurity Dive, UnitedHealth expects up to $1.6B hit from Change cyberattack this year*
3. *Anderson Economic Group, Dealer Losses Due to CDK Cyberattack Reach $1.02 Billion*

Ransomware Severity Spiked Again Following Volatile Year

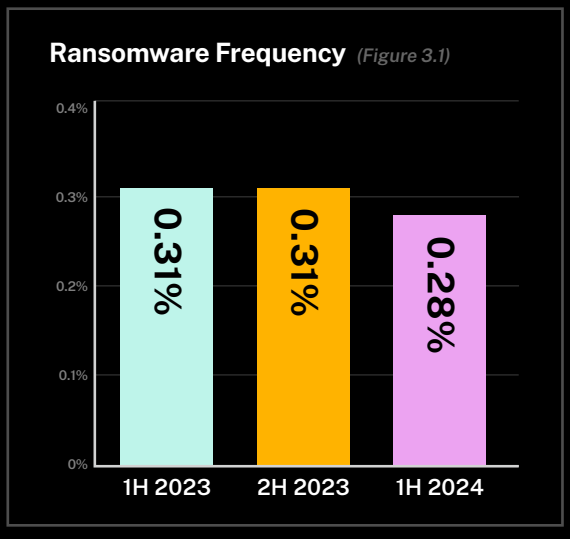
In general, ransomware has been fairly seasonal with consistent drop-offs in the summer months and spikes during winter holidays.

Ransomware continues to be a roller coaster ride. After a volatile 2023, in which ransomware severity spiked to nearly $402,000 in the first half of the year before falling to $239,000 in the back half, threat actors reinvigorated the cybercrime with one the highest returns on investment.[4]

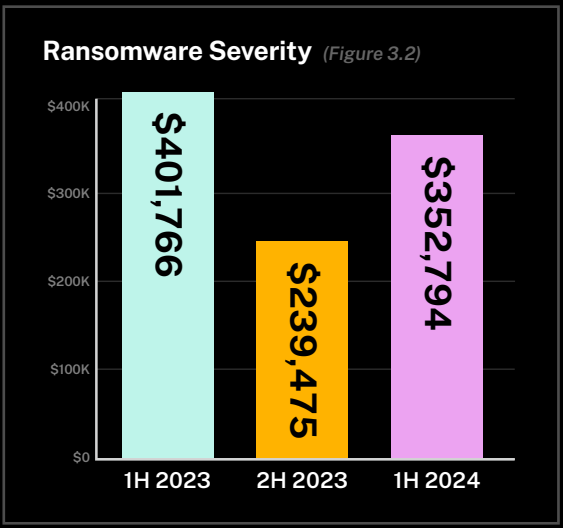
Overall ransomware frequency decreased 10% in 1H 2024, falling to 0.28% after hovering at 0.31% for all of 2023 (Figure 3.1). While ransomware frequency has been relatively stable in the US, Canada has experienced a 34% increase.

Ransomware claims among businesses with $25M-$100M in revenue steadily declined in the past 12 months, though businesses with $100M+ in revenue experienced hidden fluctuation: ransomware frequency in this cohort spiked in Q4 2023 and Q1 2024 but, due to half-year reporting, were offset by Q3 2023 and Q2 2024, respectively. In general, ransomware has been fairly seasonal with consistent drop-offs in the summer months and spikes during winter holidays — a conscious attempt by threat actors to go unnoticed within a system at times when businesses are typically slower to react.

Ransomware Frequency *(Figure 3.1)*



4. *Ransomware severity data for 2023 may differ from past reports due to future loss development. Please see Methodology for additional information.*

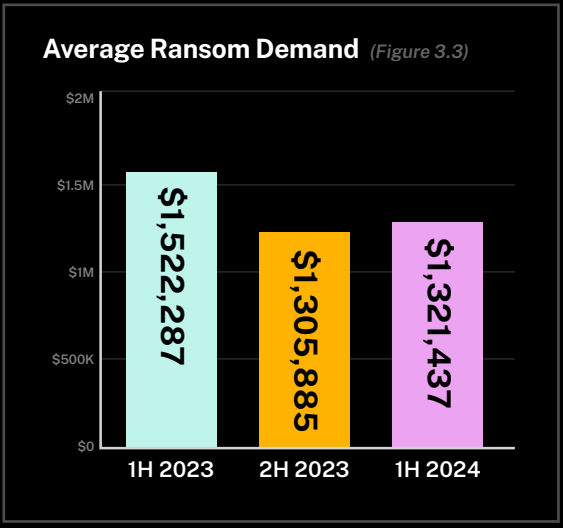


Notably, ransomware frequency among businesses in the financial services industry decreased for all revenue bands. Healthcare businesses with $100M+ in revenue experienced a 32% dip in ransomware frequency over the past six months, but are still up 134% from 1H 2023 rates. Consumer discretionary businesses saw increases in both the frequency and severity of ransomware events across all revenue bands, a trend that's persisted for two years.

Overall ransomware severity increased 68% in 1H 2024 to an average loss amount of $353,000 (Figure 3.2). Ransomware severity in Canada was a significant driver of the increase, especially among businesses with $100M+ in revenue — the revenue band that was hit hardest across all geographies.

Ransom Demands Cut in Half Through Successful Negotiations

Among ransomware events that resulted in a payment, Coalition successfully negotiated the amount down by an average of 57% of the initial demand.



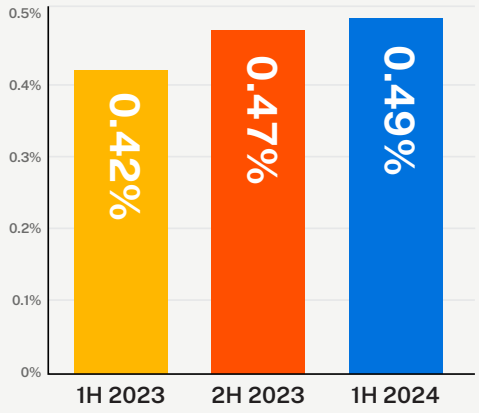
The average ransom demand increased 1% in 1H 2024 for an average of $1.3 million (Figure 3.3). The ransom demands associated with two ransomware variants, Play and BlackSuit, were noticeably higher with average demands of $4.3 million and $2.5 million, respectively.

When deemed reasonable and necessary, 40% of policyholders that experienced a ransomware event opted to pay the ransom. Among ransomware events that resulted in a payment, Coalition successfully negotiated the amount down by an average of 57% of the initial demand.[5]

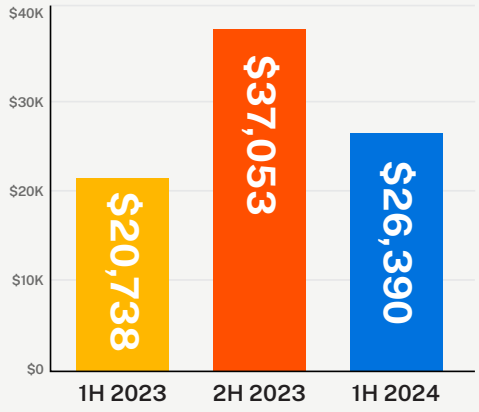
5. *Decrease in ransom amount paid based on negotiations handled by Coalition Incident Response, an affiliate firm made available to all policyholders via panel selection.*

AI Was Likely Contributor to Increases in Business Email Compromise

BEC Frequency *(Figure 4.1)*



BEC Severity *(Figure 4.2)*



Though concrete evidence has been sparse, threat actors have likely been using artificial intelligence (AI) to enhance their attacks. These tools can improve their success rate, making phishing emails easier to produce at scale and more difficult to detect.

Overall BEC frequency increased 4% in 1H 2024, growing from 0.47% to 0.49% and continuing a steady upward trend that spanned all of 2023 (Figure 4.1). Businesses with $100M+ in revenue experienced a 60% spike in BEC frequency, the sharpest of any cohort, while businesses with $25M-$100M in revenue saw a modest 9% increase. AI-enabled attacks are a plausible explanation for this trend.

Multiple industries drove the BEC frequency increase in 1H 2024. Financial services businesses saw a 20% uptick among businesses with <$25M in revenue, as well as a 390% spike among businesses with $25M-$100M in revenue. Consumer discretionary businesses saw a 250% spike among businesses with $100M+ in revenue. Industrial businesses experienced a short-term dip among businesses with $25M-$100M in revenue but increased 160% in the past year, bolstering the ongoing 18-month upward trend.

Despite the increase in frequency, BEC severity decreased 30% in 1H 2024 to an average loss amount of $26,000 (Figure 4.2). Businesses with <$25M and $25M-$100M in revenue were the biggest contributors to the decline, respectively dropping 29% and 8%.

Funds Transfer Fraud Continued Steady Decline

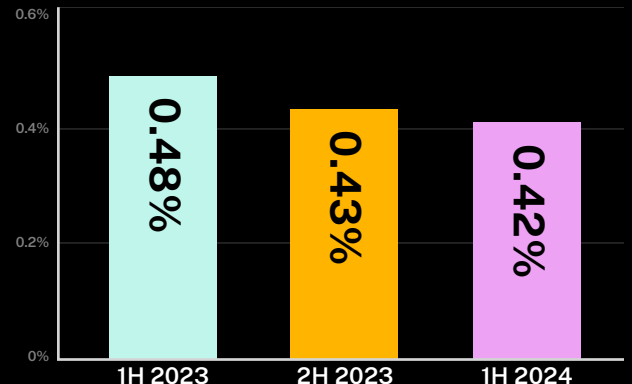
Although more inboxes were compromised with the help of AI tools, the frequency and severity of funds transfer fraud (FTF) events dipped. The decline comes after the Federal Trade Commission reported $10 billion in losses to fraud in 2023.[6]

Overall FTF frequency decreased 2% in 1H 2024, slightly dipping from 0.43% to 0.42% as part of a steady decline that persisted throughout 2023 (Figure 5.1). Although businesses with $25M-$100M in revenue have experienced fluctuations in the past 12 months, the biggest drivers of the decrease in FTF frequency are businesses with $100M+ in revenue, consistently decreasing for more than two years with an 11% drop in 1H 2024.

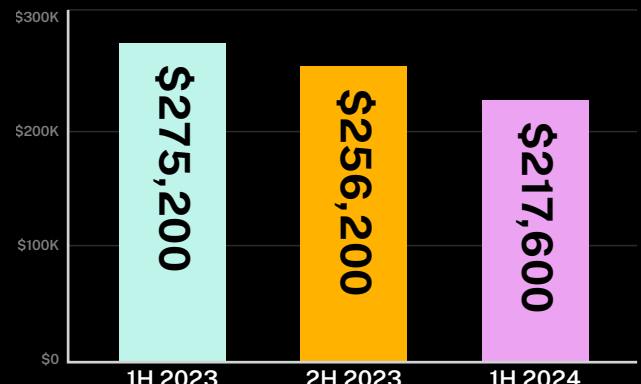
Despite the downward trend in overall FTF frequency, some industries experienced a contrasting increase in claims. Financial services businesses saw a 34% uptick among businesses with $25M-$100M in revenue, while nonprofits saw a 63% increase among businesses with >$25M in revenue — both of which furthered industry-specific upward trends over the past 18 months.

Overall FTF initial severity decreased 15% in 1H 2024 to an average loss amount of $218,000 (Figure 5.2).[7] Consumer discretionary businesses experienced meaningful increases in FTF initial severity across multiple revenue bands: Businesses with <$25M in revenue spiked 76% to a two-year high of $97,000, while businesses with $25M-$100M in revenue increased 21% for an average loss of $182,000.

FTF Frequency *(Figure 5.1)*



FTF Initial Severity *(Figure 5.2)*



6. *Federal Trade Commission, As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public*
7. *Coalition calculates FTF initial severity prior to recovery activities. Please see Methodology for additional information.*

Coalition Clawed Back $10.8 Million

Through cooperative efforts with these authorities and financial institutions, Coalition successfully clawed back $10.8 million in 1H 2024 with an average recovery of $208,000.

When a policyholder reports an FTF event to Coalition, we take direct and immediate action to "claw back" the stolen funds through our relationship with government agencies. Through cooperative efforts with these authorities and financial institutions, Coalition successfully clawed back $10.8 million in 1H 2024 with an average recovery of $208,000.

Clawing back fraudulent transfers is a critical and time-sensitive process for Coalition. Policyholders that quickly report FTF events to our claims team have a greater likelihood of recovery. In 1H 2024, Coalition made at least a partial recovery in 27% of all reported FTF events, including a full recovery in 15% of reported events.

Coalition Clawbacks

$208K

Average clawback

$10.8M

1H 2024 clawbacks

$94M

Lifetime clawbacks

Non-encryption System Compromise Continued to Drive Claims

Non-encryption system compromise accounted for nearly two-thirds of all reported Other events in 1H 2024, continuing an upward trend over the past two years.

Ransomware, FTF, and BEC accounted for nearly 75% of all reported claims in 1H 2024 — a trend that largely held true for more than three years. Coalition categorizes all other event types as "Other."[8]

Non-encryption system compromise accounted for nearly two-thirds of all reported Other events in 1H 2024, continuing an upward trend over the past two years (Figure 6.1). Data breaches are the most common example of non-encryption system compromise; the increase in the frequency of these events, alongside a slight decrease in ransomware frequency, suggests that better security controls are keeping these compromises in check.

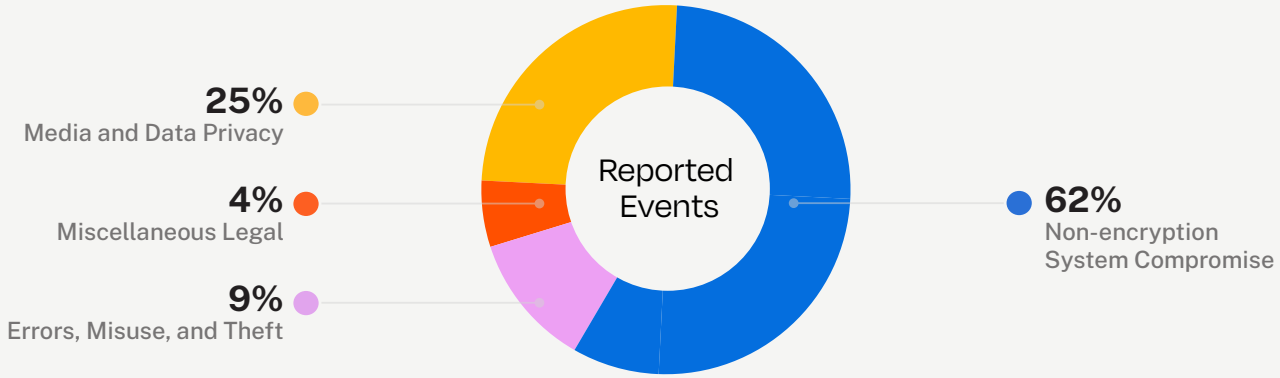
'OTHER' EVENTS DEFINED

- **Aggregation:** A single cyber event that triggers multiple disruptions and can cause widespread loss
- **Errors, Misuse, and Theft:** Misuse of business assets, inappropriate handling of information, and physical theft of assets
- **Media and Data Privacy:** A vendor, supplier, or other organization is compromised
- **Miscellaneous Legal:** Third-party allegations not involving media or data privacy
- **Non-encryption System Compromise:** A network or system compromise that did not originate via email compromise and in which no encryption was deployed

8. *Classification of "Other" event types may differ from past reports. Please see Methodology for additional information.*

'Other' Claims by Reported Events* *(Figure 6.1)*

*Aggregation events not included.



Endpoint security solutions, such as managed detection and response, have proven to be effective controls in preventing compromises from escalating into full-blown ransomware attacks due to rapid threat identification and faster response times.

Endpoint security solutions, such as managed detection and response (MDR), have proven to be effective controls in preventing compromises from escalating into full-blown ransomware attacks due to rapid threat identification and faster response times.

Overall claims frequency for Other events decreased 10% in 1H 2024, from 0.40% to 0.36%, and overall claims severity plummeted 60% for an average loss amount of $29,000. Despite the downward trends, System Compromise events steadily increased over the past year, while Miscellaneous Legal events increased over the past two years due to third-party lawsuits.

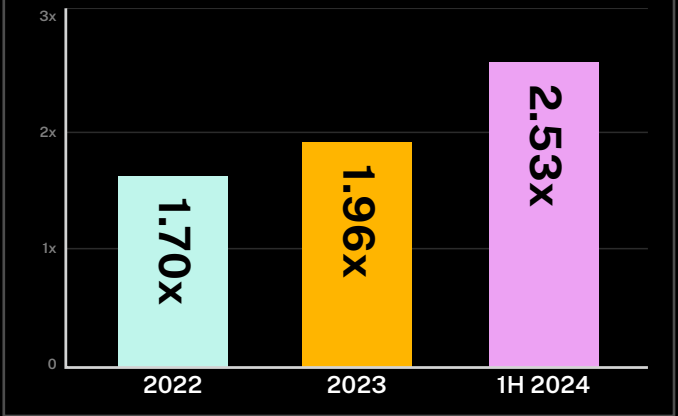
Healthcare businesses saw increases in frequency across all revenue bands, largely due to the Change Healthcare attack. Notably, businesses with $100M+ in revenue experienced jumps in aggregation events Consumer discretionary businesses with <$25M in revenue also saw a 67% increase in frequency, driven by Non-encryption System Compromise events.

Exposed Login Panels Put Businesses at 3x Greater Risk

Businesses with at least one contingency of any type were 2.5 times more likely to experience a claim in 1H 2024.

Overall Contingency Relative Claims Frequency

(Figure 7.1)



The continuous feedback loop that exists between claims activity and policy underwriting is a critical aspect of Active Insurance. New vulnerabilities can emerge at any time and impact any type of technology, often resulting in significant financial loss. When a new vulnerability emerges, we incorporate these insights into underwriting guidelines and require businesses to remediate the issue as a contingency to binding or renewing a policy.

Contingent vulnerabilities can also emerge during the policy period and are strongly correlated to an increased risk of experiencing a claim. Businesses with at least one contingency of any type were 2.5 times more likely to experience a claim in 1H 2024 (Figure 7.1). These contingencies include various risky technologies, such as certain boundary devices, remote access solutions, and end-of-life (EOL) software.

Coalition strongly recommends businesses enforce multi-factor authentication for all VPN users and ensure they're running the latest firmware

Exposed login panels were among the most significant contingent vulnerabilities putting businesses at increased risk. Login panels, or login screens, are a way for users to access a website or application. Many businesses' essential applications are web-accessible by default, which means the login panels are discoverable to threat actors trolling the internet looking for easy access. Businesses with internet-exposed login panels were 3.1 times more likely to experience a claim in 1H 2024.

Businesses often have legitimate reasons to have login panels visible to the public internet, such as with virtual private networks (VPN). In these cases, Coalition strongly recommends businesses enforce multi-factor authentication for all VPN users and ensure they're running the latest firmware — both of which help protect against brute force attacks, compromised credentials, and known vulnerabilities.

Requiring businesses to address risky technologies prior to binding or renewing coverage has proven to increase our policyholders' security posture and decrease the likelihood of claims. Over time, we've consciously narrowed our focus to only the most critical security risks, a decision that's been validated by increases in the relative claims frequency of our core contingencies.

Risky Technologies

Other internet-exposed technologies were also found to increase the likelihood of a business experiencing a claim in 1H 2024:

1.7x more likely	**Remote Desktop Protocol**
1.8x more likely	**SonicWall Firewalls**
2.3x more likely	**Microsoft Remote Procedure Call**
2.4x more likely	**EOL Microsoft Internet Information Services**
2.7x more likely	**Remote Desktop Web Access**
2.8x more likely	**FortiOS SSL VPN**
5.1x more likely	**Cisco Adaptive Security Appliance**

Active Engagement and Innovation Proved to be the Answer for Evolving Risks

We know that most people think of Active Insurance through the lens of first-party events, like FTF and ransomware. These are not only the cyber events Coalition sees most often but also the ones on which we've made the greatest impacts: $94 million in lifetime clawbacks, millions more saved by cutting ransomware demands in half through negotiation, and hundreds of businesses that avoided paying ransoms altogether thanks to swift and decisive incident response.

But as third-party risk continues to grow and aggregation events become increasingly common, it's equally important to spotlight how Coalition continues to innovate and differentiate Active Insurance from more traditional cyber insurance products.

In a typical business interruption claim, a policyholder submits its proof of loss and waits on the insurer to review the report with a forensic accountant — a slow process that usually ends in negotiating a payout. Coalition takes an active approach from the beginning of a matter involving third-party disruption, engaging policyholders upfront to strategize on what extra expenses they can incur to avoid experiencing a business interruption loss. We look for alternative ways to help them solve near-term problems, accomplish their business goals, and minimize the overall impact through proactive response.

The rise of third-party disruption reinforces what Coalition has always known: The true winners in our industry will be the cyber insurance providers that find meaningful and innovative ways to leave a positive mark on the businesses they pledge to protect.

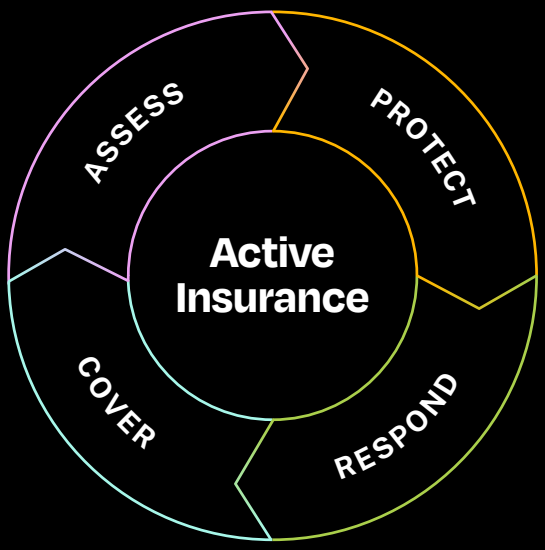
Threat actors will continue to pivot their tactics and capitalize on vulnerable technologies and other weaknesses in businesses' security postures. We recognize these cyber threats aren't going away, which is why Coalition continues to pursue security research efforts to identify threats sooner and gain confidence about which threats are most likely to result in widespread loss. We also remain committed to enhancing business security by delivering security solutions that are proven to help prevent cyber events, such as managed detection and response (MDR) services and security awareness training.

The rise of third-party disruption reinforces what Coalition has always known: The true winners in our industry will be the cyber insurance providers that find meaningful and innovative ways to leave a positive mark on the businesses they pledge to protect.

Stay One Step Ahead of Digital Risk

Our mission at Coalition is to help protect the unprotected. As the world continues to digitize, we actively partner with businesses to help them stay one step ahead of digital risk.

Active Insurance is the first cyber defense bringing together active cyber risk assessment, proactive protection, expert response, and comprehensive cyber coverage. We share the insights in this report to help empower others in the face of growing cyber risks.



How Active Insurance Works

Active Insurance is purpose-built to help protect businesses in the digital age. We pioneered Active Insurance to address the challenges of cyber threats in ways that traditional insurance can't.

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

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

COVER
Comprehensive coverage to give peace of mind following an attack

RESPOND
Immediate expert support to minimize impact and speed up recovery

Want to work with us?
Become an appointed broker

Looking for help?
Get matched with a broker

Curious about your risk?
Get a free risk assessment

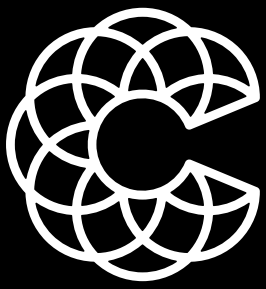
Methodology

The 2024 Cyber Claims Report: Mid-year Update is based on reported claims data from January 1 to June 30, 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.

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

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, overall claims frequency and severity data may have changed from prior reports. As a general practice, please reference our most recent reports when possible.



Coalition®

coalitioninc.com

44 MONTGOMERY STREET, SUITE 4210
SAN FRANCISCO, CA 94104

Important Disclosures: You are advised to read this disclosure carefully before reading or making any other use of this report and related material. The content of this report is (i) not all-encompassing or comprehensive; (ii) solely for informational purposes; (iii) not be construed as advice of any kind or the rendering of consulting, financial, legal, or other professional services from Coalition; and (iv) not in any way intended to create or establish a contractual relationship. Any action you take upon the information contained herein is strictly at your own risk and Coalition will not be liable for any losses and damages in connection with your use or reliance upon the information. The content of this report may not apply directly to specific circumstances and professional advice should be sought before any action is taken in relation to the information disseminated herewith. Coalition makes no representation or warranties about the accuracy or suitability of information provided in the report or related materials. The report may include links to other resources or websites which are provided for your convenience only and do not signify that Coalition endorses, approves or makes any representation or claim regarding the accuracy of copyright compliance, legality, or any other aspects of the resources or websites cited. Copyright © 2024. All Rights Reserved. Coalition and the Coalition logo are trademarks of Coalition, Inc.