Coalition®

coalitioninc.com

2023 Cyber Claims Report

Mid-year Update

Table of Contents

Executive Summary

After a brief respite, ransomware came roaring back in 2023. New records were set and surpassed as the months passed, and threat actors found the newest exploitable vulnerabilities to turn a profit. Now, years after it first rose to prominence, we've been confronted again with the realities of ransomware, only the stakes are higher. Businesses are more reliant on technology, threat actors are more sophisticated, and our economy is more interconnected than ever before.

Businesses are getting hit harder and more often with cyber attacks, and the threats go beyond ransomware. Financial fraud remains a mainstay of the threat actor economy, while third-party compromise looms large amid discussions of data privacy and security at the federal level. With any digital risk, the key is recognizing that it cannot be solved by passive means. **Dynamic cyber risks require an active solution.**

Active Cyber Insurance is focused on helping prevent digital risk before a cyber incident strikes and reducing the impact of every claim. Amid the recent uptick in cyber claims, Coalition, Inc., employed highly specialized financial recovery tactics to minimize the impacts of cyber claims. We negotiated ransoms on behalf of our policyholders and reduced the payment amount to nearly half of the initial demand. We chased down fraudulent wire transfers and recovered $23 million — all of which went directly back into our policyholders' pockets.

Cyber insurance is not a set-it-and-forget-it solution. We believe that cyber risk is manageable with the right insurance partnership — but it must be a shared responsibility. Many of the claims we received this year could have been prevented with stronger security controls and better cyber risk management decisions. Our role is to help protect organizations by promoting good cyber hygiene and helping businesses understand the financial impact of their decisions.

Good cyber hygiene goes beyond the act of purchasing a cyber policy. It often requires a shift in how businesses approach their daily operations. We want our policyholders to consider digital risk in every digital interaction, whether it's clicking a link or adopting new software. This is the power of Active Insurance, and it's why Coalition policyholders experienced 64% fewer claims than the industry average.[1]

Coalition's 2023 Cyber Claims Report: Mid-year Update features data from organizations across the United States. Cyber risk is global in nature, and we believe the trends and risk mitigation strategies within this report are applicable regardless of location. We're proud to share these insights to help our policyholders, broker partners, and others in the cyber insurance industry stay informed about the ever-changing threat landscape.

1. *Industry average determined using market frequency data reported by U.S. insurers to the National Association of Insurance Commissioners (NAIC).*

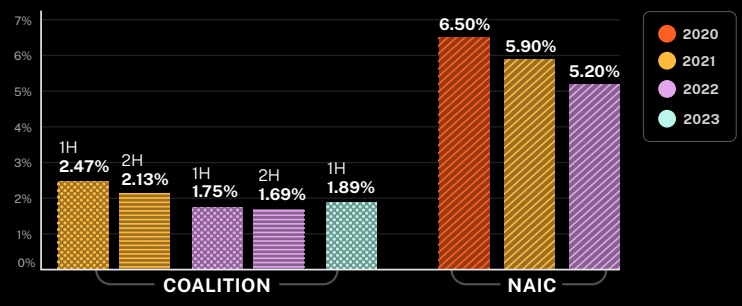
Cyber Claims Increased in the Face of Surging Attacks

Ransomware was the largest driver of the increase in claims frequency, accounting for 19% of all reported claims.

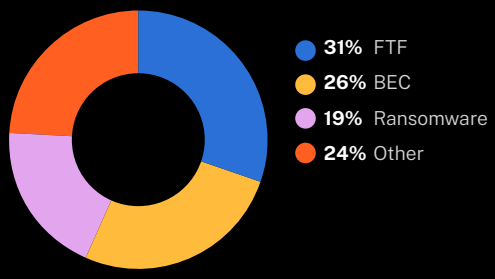
Overall claims frequency[2] increased by 12% in the first half (1H) of 2023. However, Coalition policyholders experienced 64% fewer claims compared to the broader cyber market[3], with 52% of reported events handled at no cost to the policyholder (Figure 1.1).

Ransomware was the largest driver of the increase in claims frequency, accounting for 19% of all reported claims (Figure 1.2). Claims related to funds transfer fraud (FTF) remained steady at 31%, while business email compromise (BEC) decreased to 26%. "Other" event types — non-encryption malware, legal, errors, etc. — increased slightly to 24%.

Claims Frequency: Coalition vs. U.S. Cyber Insurance Market 1H 2023 *(Figure 1.1)*

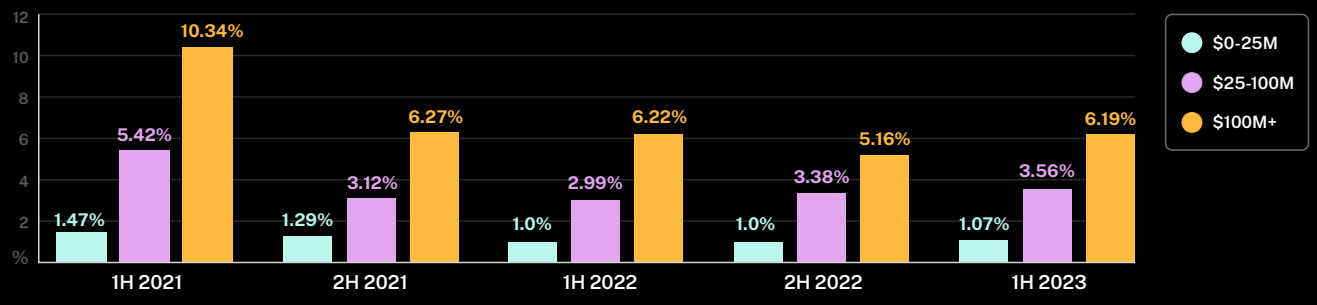


Gross Reported Claims by Event Type 1H 2023 *(Figure 1.2)*

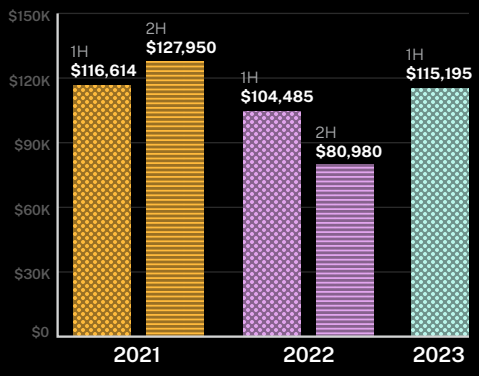


2. *All data based on reported claims and incurred losses between January 1, 2023 and June 30, 2023.*
3. *Industry average determined using market frequency data reported by U.S. insurers to the National Association of Insurance Commissioners (NAIC). When compared to NAIC, claims frequency calculated as reported events resulting in a gross loss greater than zero, developed to ultimate, divided by annual earned policies.*

Claims Frequency by Revenue Band 1H 2023 *(Figure 1.3)*



Claims Severity 1H 2023 *(Figure 1.4)*

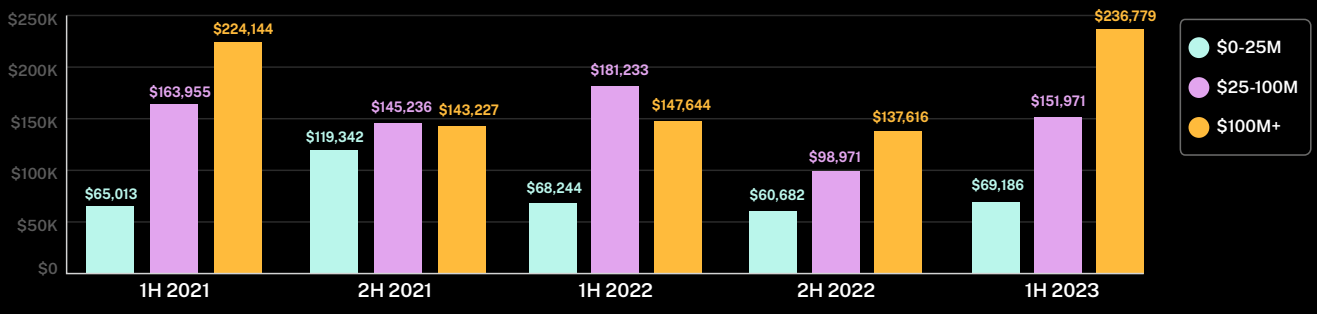


Claims frequency increased for all revenue bands. Businesses with more than $100 million in revenue saw the largest increase at 20%, while those with less than $25 million in revenue saw a 7% increase (Figure 1.3). Businesses between $25 million and $100 million in revenue were the most stable, experiencing only a 5.3% increase.

As claims frequency rose, so did claims severity. Overall claims severity increased by 42% in 1H 2023 with an average loss amount of more than $115,000 (Figure 1.4). Despite the increase, severity remains below the historic high of $127,950 in 2H 2021.

Businesses across all revenue bands saw more substantial losses. Businesses with more than $100 million in revenue were hit the hardest, experiencing a 72% increase in claims severity (Figure 1.5). Similarly, businesses between $25 million and $100 million in revenue experienced a 54% increase, while those with less than $25 million in revenue saw only a 14% increase.

Claims Severity by Revenue Band 1H 2023 *(Figure 1.5)*



Ransomware Severity Climbed to Historic High

Among ransomware claims that resulted in a payment, Coalition successfully negotiated the amount down to an average of 44% of the initial demand.

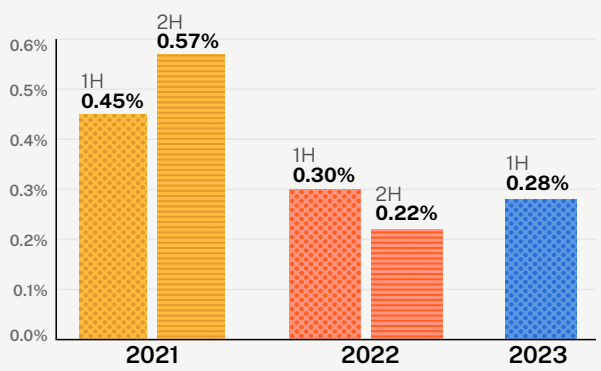
After trending downward for 18 months, ransomware appeared to have fallen out of favor among threat actors. However, recent spikes in both the frequency and severity of ransomware claims indicate threat actors are unwilling to pass up on such highly lucrative attacks.

Ransomware claims frequency increased by 27% in 1H 2023 (Figure 2.1). The largest contributor to this spike was the increase in frequency during May, which marked the most ransomware claims in a single month in Coalition history.

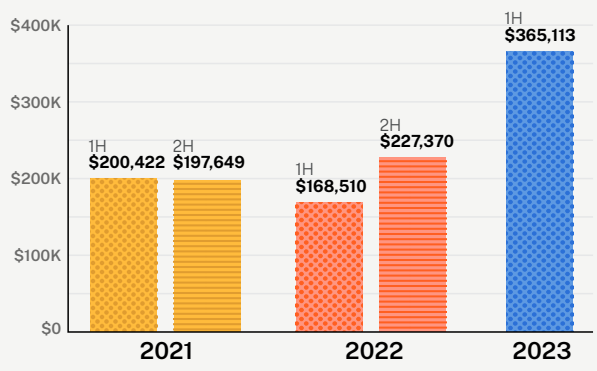
Despite speculation that geopolitical strife contributed to ransomware volatility,[4] claims data spanning 1H 2022 to 1H 2023 does not show fluctuations significant enough to warrant such a conclusion.

Ransomware claims severity reached a record-high in 1H 2023 with an average loss amount of more than $365,000 (Figure 2.2).

Ransomware Frequency 1H 2023 *(Figure 2.1)*

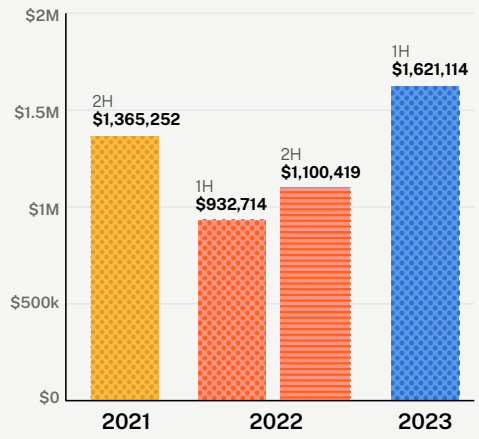


Ransomware Severity 1H 2023 *(Figure 2.2)*



4. NPR, *The rise in ransomware attacks this year may be related to Russia's war in Ukraine, 2023.*

Average Ransom Demand 1H 2023
(Figure 2.3)



The average ransom demand in 1H 2023 was $1.62 million, which marks a 47% increase over the previous six months and a 74% increase over the past year.

This spike represents a 61% increase within six months and a 117% increase within one year.

Unsurprisingly, ransom demands increased alongside more frequent attacks. The average ransom demand in 1H 2023 was $1.62 million, which marks a 47% increase over the previous six months and a 74% increase over the past year (Figure 2.3).

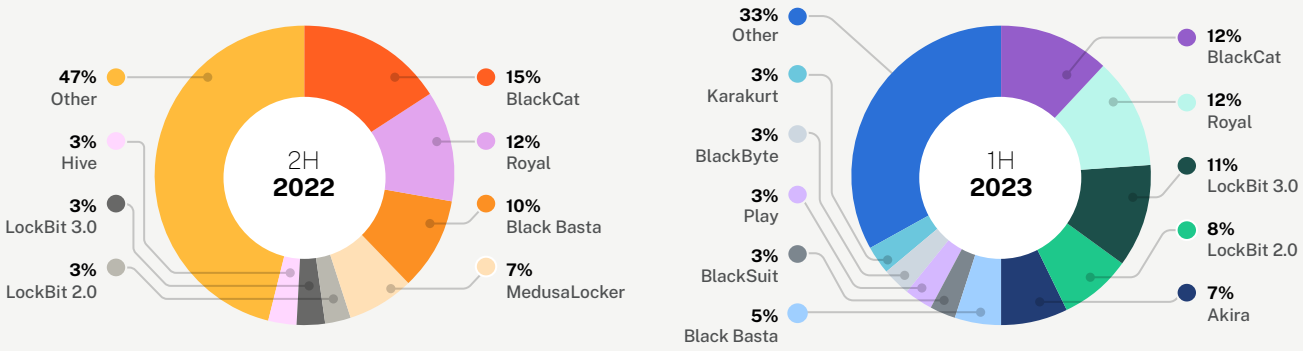
When reasonable and necessary, 36% of Coalition policyholders opted to pay a ransom in 1H 2023. Among ransomware claims that resulted in a payment, Coalition successfully negotiated the amount down to an average of 44% of the initial demand.[5]

Ransomware Variant Trends

As ransomware resurged, the variants that drove losses shifted. Royal Ransomware accounted for 12% of reported ransomware variants (Figure 2.4). Coalition Incident Response (CIR) reported this sophisticated malware strain has been associated with ransom demands of up to $2 million.[6]

Coalition alerted policyholders to the risk of Royal Ransomware in April 2023. The alerts followed an observation by CIR that multiple cases associated with this variant used an unpatched, end-of-sale (EOS) firewall appliance, highlighting the importance of establishing a regular patch cadence and deprecating legacy technologies.

Ransomware Variants 1H 2023 *(Figure 2.4)*



5. *Decrease in ransom amount paid only includes negotiations handled by Coalition Incident Response, an affiliate firm made available to all policyholders via panel selection.*
6. *Data based on determination of root cause, as reported by Coalition Incident Response.*

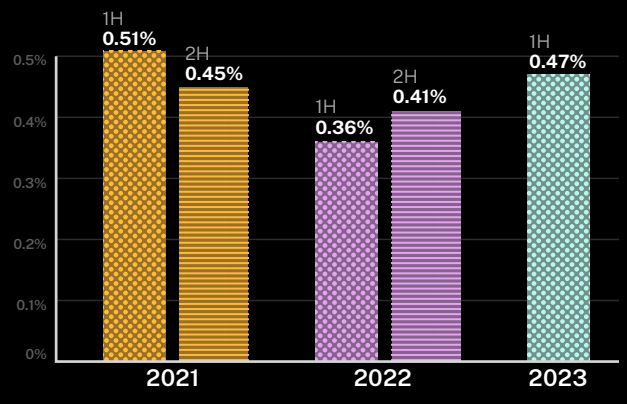
Funds Transfer Fraud Severity Spiked

The growing sophistication of threat actors and their tactics is a contributing factor in the upward trend in FTF claims severity.

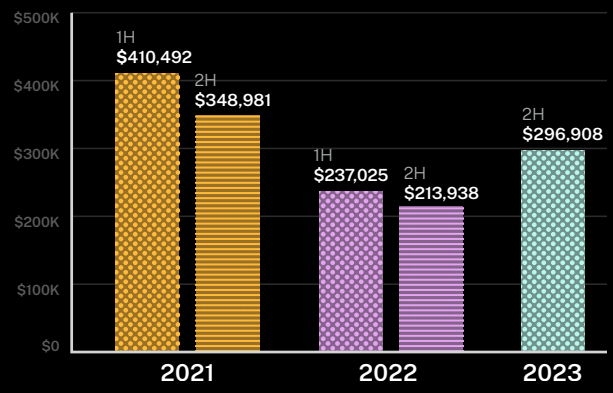
Unlike the volatility seen in ransomware FTF remained a reliable way for threat actors to monetize their cybercrimes. This is largely due to the relative ease of the attack method and its pairing with tried-and-true phishing tactics.

FTF claims frequency increased by 15% in 1H 2023, continuing to hover around the same rate over the past two years (Figure 3.1). Meanwhile, FTF initial severity[7] increased by 39% to an average loss of more than $297,000 — though still well short of the historic high of $410,000 in 1H 2021 (Figure 3.2).

FTF Frequency 1H 2023 *(Figure 3.1)*



FTF Initial Severity 1H 2023 *(Figure 3.2)*



7. *FTF initial severity calculated prior to recovery activities.*

The growing sophistication of threat actors and their tactics is a contributing factor in the upward trend in FTF claims severity.

The growing sophistication of threat actors and their tactics is a contributing factor in the upward trend in FTF claims severity. The longer a threat actor remains in an email account after compromise, the more difficult it becomes to recognize and report abnormal activity — and they appear more willing to wait for the right moment to intercept or redirect large payments.

If an event is reported before a threat actor fraudulently transfers money, Coalition can provide forensic support and expel them from the account, in which case the event is categorized as business email compromise (BEC). If the event is reported after the transfer occurs, it's categorized as FTF, and Coalition pursues tactics to aid in recovery.

Coalition Clawbacks

When an FTF event occurs, threat actors often move money across various jurisdictions to cover their tracks. Through relationships with government entities and financial institutions, Coalition drastically increases the chance of recovery by moving quickly — and going where others can't — to "claw back" stolen funds.

Coalition successfully clawed back more than $23 million in fraudulent transfers in 1H 2023 — nearly three times more than 2H 2022. In instances where recovery was possible, we recovered an average amount of $612,000 per FTF claim, which represented 79% of all FTF losses.

$23M
Total FTF recovery amount in 1H 2023

200%
Increase in recovery amount since 2H 2022

$612K
Average amount recovered per FTF claim

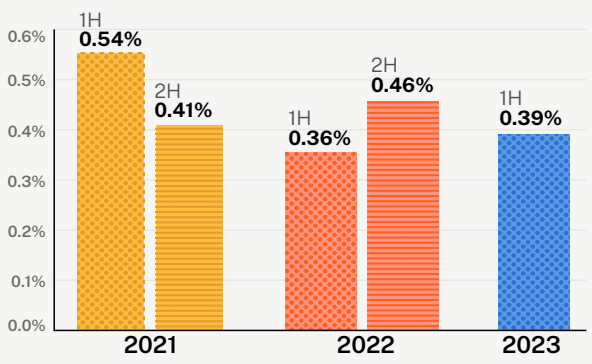
Email Security Remained Critical to Claims Reduction

BEC claims severity decreased by 7% to an average loss of $21,000, marking the lowest amount in recent years.

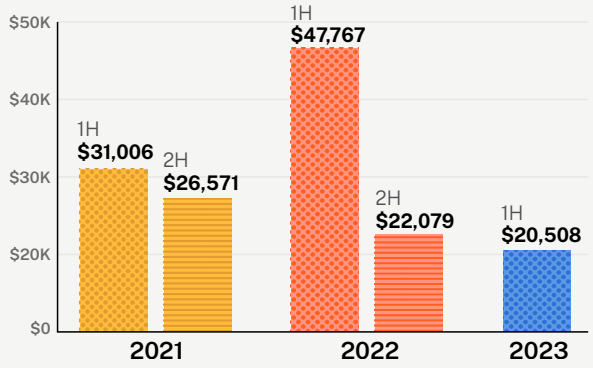
Email inboxes were once seen only as treasure troves of data that attackers could sell to monetize their cybercrimes. Now, they're increasingly used as pathways to financial systems, as evidenced by recent increases in FTF claims. BEC events that result in fraudulent wire transfers, as opposed to data loss, are classified as FTF events.

BEC claims frequency decreased by 15% in 1H 2023 (Figure 4.1). Further, BEC claims severity decreased by 7% to an average loss of $21,000, marking the lowest amount in recent years (Figure 4.2).

BEC Frequency 1H 2023 *(Figure 4.1)*



BEC Severity 1H 2023 *(Figure 4.2)*



Google Workspace users had a 25% reduction in FTF or BEC claims and a reduction of up to 10% in ransomware claims.

Email Vendors Impacted Risk of Cyber Claims

Coalition claims data continues to support a correlation between the mechanism and vendor companies select for email and the likelihood of a cyber insurance claim.

Businesses using Google Workspace for email were markedly more secure than those using Microsoft Office 365 (M365) and on-premises Microsoft Exchange. M365 users were more than twice as likely to experience a claim compared to Google Workspace users. On-premises Microsoft Exchange users were nearly three times more likely to experience a claim compared to businesses using Google Workspace.

However, the decreased risk experienced by businesses using M365, compared to hosting their own on-premises Exchange server, applied only to ransomware claims. Neither group of Microsoft product users saw a decreased risk of FTF or BEC claims (Figure 4.3). This was in stark contrast to companies using Google Workspace, which experienced a 25% risk reduction for FTF or BEC claims and a 10% risk reduction for ransomware claims.

The discrepancy in claims among Google and Microsoft users may be tied to whether a business purchases Defender for Office 365, which is not included in Microsoft's base E3 license. Defender and Google Workspace both include important, comparable email security features, such as impersonation protection and malicious URL protection.

Relative Likelihood of FTF or BEC Claim by Email Provider 1H 2023 *(Figure 4.3)*

MOVEit Quickly Evolved into Widespread Exploitation

Coalition policyholders continued to experience cyber incidents related to MOVEit beyond 1H 2023, with most of the 53 reported incidents stemming from third-party compromise.

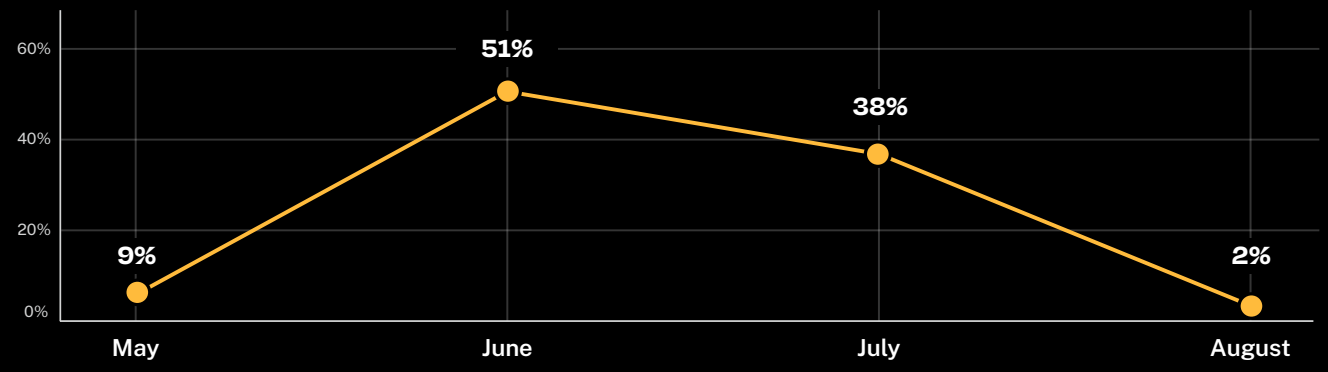
After Progress Software disclosed a critical vulnerability in its file transfer program in May,[8] MOVEit became headline news. What started as one zero-day vulnerability evolved into six over several weeks. During that time, the Cl0p ransomware gang capitalized on the vulnerabilities, compromising hundreds of organizations globally — notably using only data exfiltration and not data encryption — and published their data through the Cl0p ransomware leak site.

Coalition policyholders have continued to experience cyber incidents[9] related to MOVEit — even beyond 1H 2023. Across 53 reported incidents, the overwhelming majority were due to third-party compromises, in which the vendors or suppliers of our policyholders were directly compromised, reaching a high point in June (Figure 5.1).

One of the defining characteristics of the MOVEit vulnerabilities is that evidence of attack is minimal, making it difficult to determine if threat actors accessed a network. Because the initial vulnerability was zero-day, many organizations were impacted despite patching their technology. While the influx of incidents has slowed among Coalition policyholders, many organizations will likely find themselves indirectly impacted, given the breadth of the Cl0p victim list.

8. *Progress Software, MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362).*
9. *Incident defined as an adverse cyber event reported to Coalition by a policyholder that may or may not evolve into a cyber claim. Unless otherwise noted, a claim is an incident that incurred a gross loss.*

MOVEit Incidents by Month 1H 2023 *(Figure 5.1)*



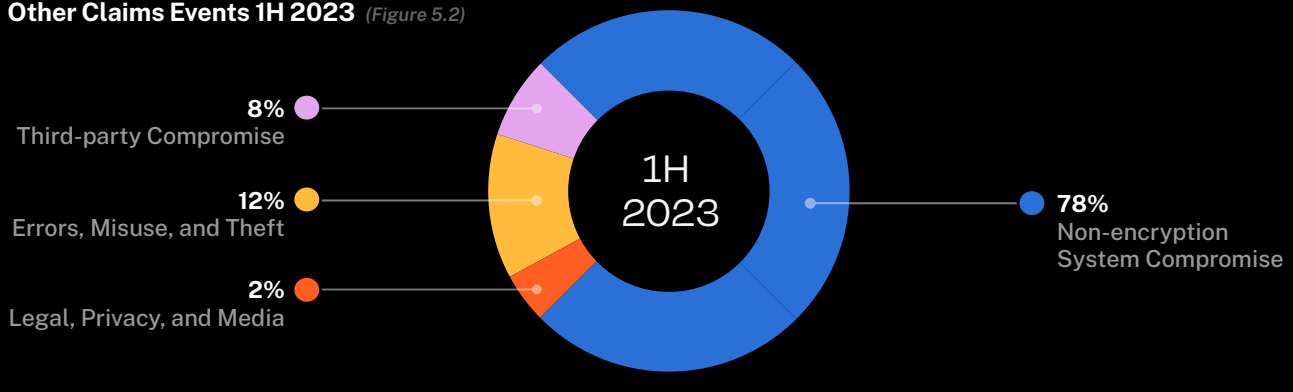
One of the defining characteristics of the MOVEit vulnerabilities is that evidence of attack is minimal, making it difficult to determine if threat actors accessed a network.

Third-party Compromise and 'Other' Events

Coalition categorizes claims events that did not result in ransomware, FTF, or BEC as "Other." As we saw with MOVEit, these events can result in data breaches, as well as legal and regulatory issues (Figure 5.2).

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

Other Claims Events 1H 2023 *(Figure 5.2)*



How Businesses Can Actively Address Cyber Risk

Among Coalition policyholders, 14% received at least one security alert regarding a critical vulnerability in 1H 2023 — and 47% of them successfully resolved the issue within 30 days of notification.

While digitization has unlocked significant advancements for our global economy, the speed at which information can be transferred and technology can be adopted is often in direct opposition to good cyber hygiene.

In the face of more frequent and costly attacks, businesses have an opportunity to counteract the likelihood of a cyber event by proactively improving their cybersecurity posture. Simple but actionable security controls can help businesses avoid many of the cyber risk pitfalls we witnessed in 1H 2023.

Implement multi-factor authentication (MFA) on all critical accounts

FTF events and BEC claims often begin with a phishing attack, the leading attack vector of cyber insurance claims, that would have otherwise been preventable with MFA.

Maintain credible offline backups of critical business data

Businesses want to avoid paying a ransom demand or losing data. Implement and test offline backups so that in the event of a ransomware incident, restoration is possible without paying a hefty demand.

Establish a formal procedure for electronic payments

Exercise caution when making financial transactions, particularly those tied to email communications. Never confirm new or payment instruction changes via email, always require two-party reviews (or more) for transferring funds, and report all suspicious activity.

Patch all software and firmware regularly

A regular patching cadence, combined with timely alerts, can help organizations act quickly and prioritize their response to critical vulnerabilities. Among Coalition policyholders, 14% received at least one security alert regarding a critical vulnerability in 1H 2023 — and 47% of them successfully resolved the issue within 30 days of notification.

We share these cyber insights to help our broker partners advise clients on new and emerging risks, empower policyholders to prioritize their cybersecurity posture, and bring more stability to the cyber insurance industry.

Deprecate legacy and risky technologies

EOL software or otherwise risky technology can signal to cyber attackers that a business has weak security controls in place. To reduce the likelihood of a cyber claim, avoid outdated software and technologies with a history of critical vulnerabilities when possible.

Security controls are more than just incentives or recommendations: they're meaningful mitigation tactics that can help businesses reduce the risk of a cyber attack. Cybersecurity best practices aren't always convenient, but our claims data shows that security controls, when coupled with Active Cyber Insurance, can meaningfully reduce an organization's cyber risk. **That's why Coalition policyholders experience 64% fewer claims than the industry average.**

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

Methodology

The *2023 Cyber Claims Report: Mid-year Update* is based on reported claims data from January 1 to June 30, 2023. A claim is defined as an adverse cyber event reported by a Coalition policyholder that incurred a gross loss. Our team of data scientists and actuaries used our own internal claims data to complete the analysis.

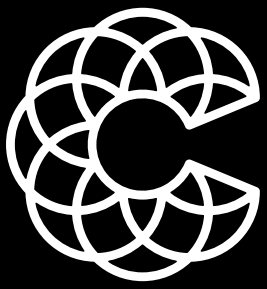
In this report, we updated our methodology to use the reported experience as of six months of age rather than ultimate loss projections. Ultimate loss is the total sum paid by the policyholder and its insurers. As a projection, ultimate loss can change overtime due to future loss development. By shifting our methodology to 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.

This shift allows Coalition to highlight the trends in cyber claims that are impacting policyholders today. Our new methodology was retroactively applied to Coalition's historical data. In doing so, overall claims frequency and severity data from reports issued in 2021 forward, as well as data for specific event types, may have experienced changes.

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

Root cause analysis

In partnership with forensics vendors, we work to identify and attribute the root cause of every possible policyholder cyber incident. We aggregate and ingest root cause data in our Active Risk Platform, the data collection and analytics platform that powers our underwriting, continuous monitoring, and alerting capabilities. This process allows us to better understand which root causes and attack vectors result in losses.



Coalition®

coalitioninc.com

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