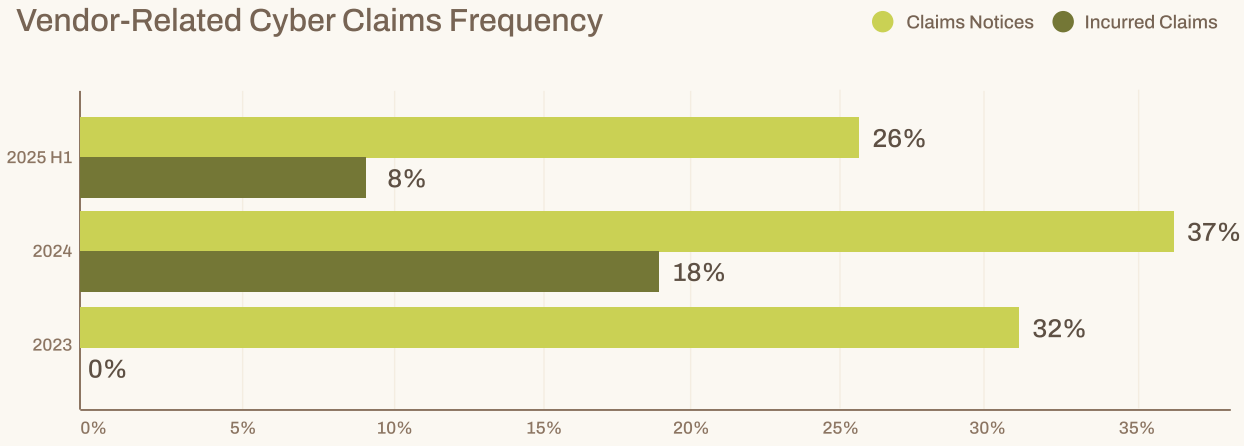
resilience | roc Resilience Risk Operations Center

Midyear *Cyber* Risk Report

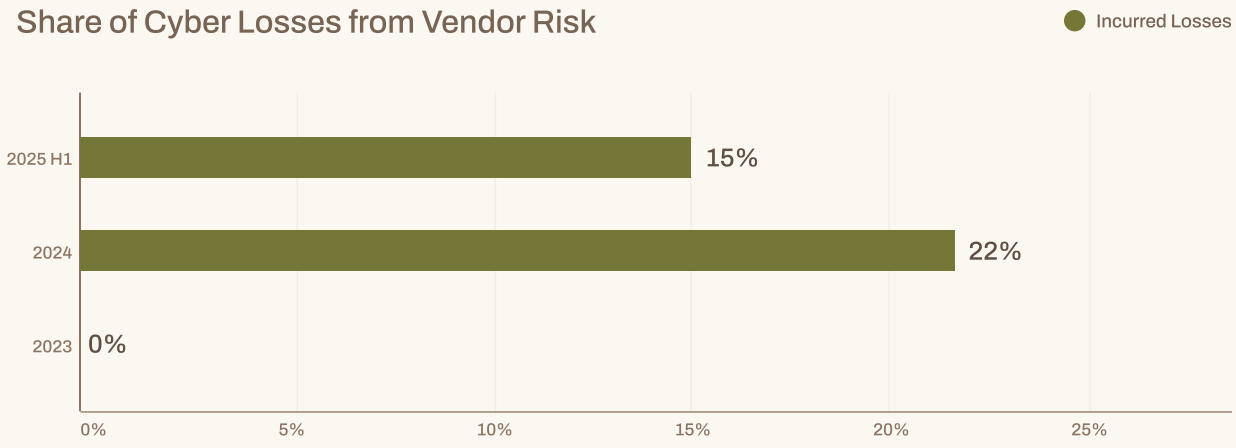
2025

2024 Lookback: An Evolution of Third-Party Risk

The cyber threat landscape underwent a fundamental transformation in 2024, with vendor-related risk emerging as the dominant force reshaping how organizations experience and respond to cyber incidents. In years past, vendor data breaches have driven a high number of claims notices (21% of claims notices since 2023), but only 2% of claims with incurred losses in our portfolio. In 2024, however, business interruption due to vendor unavailability emerged as the second highest cause of loss in our portfolio, behind only ransomware. High-profile incidents, like the CDK Global and Change Healthcare breaches, illustrated the vulnerability of critical vendors within certain industries and the widespread impact whey they are compromised.



In 2024, vendor-related incidents accounted for more than a third (37%) of all claims notices in our portfolio and led to 22% of incurred losses, compared to 32% of claims notices and 0% of incurred losses in 2023. This dramatic shift highlighted how exploiting a single point of failure in one company can lead to cascading disruption downstream, affecting entire industries and economic sectors



Ransomware attacks targeting vendors made up 18% of incurred losses in 2024, demonstrating the financial attractiveness of these targets to cybercriminals. Four percent of the portfolio's losses, the balance of vendor loss, was due to non-malicious vendor outages.

* *This report represents our analysis of cyber risk trends based on actual claims experience and threat intelligence. For the most current information and specific guidance for your organization, please consult with Resilience's risk management and insurance professionals.*

2025 Midyear Outlook: A Return to Equilibrium — or the Eye of the Storm?

There was a significant claims surge in 2024: claim notifications jumped 86% and vendor-related incidents went from zero to 21% of incurred losses. The first half of 2025 suggests a return to operational equilibrium, however, as claims notice frequency in Resilience's portfolio is down 53%.

Vendor-related incidents have also been quieter, with vendor-related claims accounting for 26% of claims notifications (down from 37% in 2024) and 15% of incurred losses estimated so far this year (down from 21% in 2024). While incidents dropped in frequency, clients who experienced business interruption from a vendor-related incident had significant losses that rivaled losses from companies directly affected by ransomware.

Successful attacks are also becoming more expensive. The average cost of a ransomware claim has increased 17% year-over-year. This isn't just inflation; it's a sign that threat actors are becoming more systematic in how they target and exploit organizations. The infamous Scattered Spider threat group, for instance, recently targeted retail, aviation, and insurance companies; we expect to see similar behavior of intense, focused campaigns going forward.

Looking Forward: Three Critical Expectations

AI IS MAKING SOCIAL ENGINEERING MORE EFFECTIVE.

According to CrowdStrike's 2025 Threat Hunting Report, 78% of enterprises experienced at least one AI-specific breach in 2025, with AI-generated phishing campaigns achieving a 54% success rate, compared to just 12% for traditional attempts. AI-driven browser-based attacks appear to be driving this surge, as they can bypass multi-factor authentication and endpoint detection software. When paired with SIM swapping, these attacks effectively access critical assets while remaining difficult to detect.

In the Resilience portfolio, social engineering accounted for 57% of incurred claims and 60% of incurred losses in the first half of 2025. Despite industry-wide training efforts, attackers are gaining ground through more believable digital phishing attacks.

And they aren't limited to email and voice: browser-based phishing has led to a rise in credential harvesting through infostealers. According to the Resilience Risk Operations Center (ROC), 1.8 billion credentials were compromised in the first half of 2025—an 800% increase since January—including over 1 billion corporate and personal email accounts.

ATTACKERS ARE WORKING SMARTER, NOT HARDER.

The ransomware playbook is evolving. While Resilience data shows that 79% of clients who were attacked with ransomware over the entire lifetime of our portfolio successfully avoided paying a ransom, these attacks are still costly and disruptive to recover from. For ransomware attacks that lead to incurred claims, the average claim in 2025 so far is over $1.18m. In H1 2024, a ransomware attack incurred an average loss of $1,01m ($983k for 2024). And in a troubling trend, double extortion—demanding a ransom payment for both data decryption and to prevent its public release—seems to have become standard.

ECOSYSTEM RISKS ARE CONNECTED — AND COMPOUNDING.

Vendor-related risk accounted for 22% of incurred losses in 2024 and 15% in the first half of 2025—underscoring how costly unseen risks can be. The retail attacks this spring not only inflicted heavy damage on the companies directly targeted, but also exposed their role as key suppliers. As a result, the impact rippled through the broader retail supply chain, magnifying losses far beyond the initial victims.

The interconnected nature of modern businesses compounds this issue: complex technical ecosystems, complex corporate structures, shared risk pools, and franchise relationships all link risk across portfolios. Because these entities may or may not share people, processes, or technologies, a vulnerability in one area can expose many others. Gaining visibility into both vendor and subsidiary risk is essential to reducing the probability and impact of cascading losses.

Claims Trends Analysis

↘ 53%

reduction in cyber claims in H1 2025 vs H1 2024

↘ 11%

reduction in average loss per incurred claim in H1 2025 vs H1 2024

↗ 17%

increase in severity of ransomware attacks H1 2025 vs H1 2024

As previously mentioned, cyber insurance claims surged in 2024 but dropped 53% in the first half of 2025 compared to the same period in 2024, indicating a stabilization in the cyber risk environment. But while claim frequency has stabilized, the financial impact of those claims tells a more complex story.

In the first half of 2025, the average loss per incurred claim decreased by 11% compared to the same period in 2024. However, ransomware attacks grew in severity by 17%, now accounting for 76% of incurred losses. The number jumps to 91% if you include losses from a vendor experiencing ransomware. Transfer fraud and data collection incidents have contributed to fewer losses this year.

The incurred claims rate (which represents the number of incurred claims to total claims) also climbed slightly to 11%. Some of last year's far reaching incidents—like the Change Healthcare attack—resulted in many claims notices, but fewer insured losses.

Cyber insurance claims offer the clearest evidence of which security failures lead to which types of losses. The Marks & Spencer incident in the UK this spring illustrated this vividly: among major cyber perils, business interruption has the most immediate and severe impact on both operations and revenue.

"The 53% drop in claims doesn't tell the whole story. Yes, we're seeing fewer incidents escalate to incurred losses, but when they do hit, they're hitting harder. The 17% increase in ransomware claims losses shows that cybercriminals are becoming more selective and more devastating in their approach."

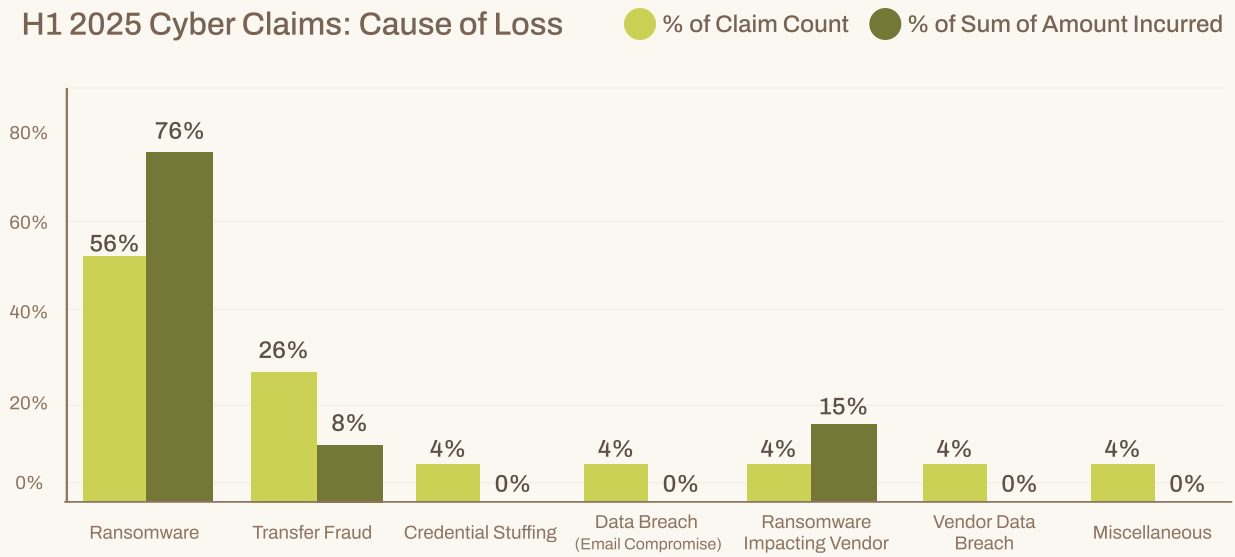
Jeremy Gittler
Global Head of Claims, **Resilience**

Cause of Loss Analysis

Incurred Claims Breakdown: H1 2025

Ransomware attacks continue to drive the majority of financial losses in cyber insurance claims. In H1 2025, ransomware accounted for 76% of incurred losses, while business interruption from ransomware affecting a vendor was an estimated 15% of incurred losses. Transfer fraud appears to be holding steady at 8% of losses.

This pattern highlights a key insight: Although there are many types of cyberattacks happening all the time, ransomware causes the most severe financial damage. That makes it the top priority for risk management and insurance strategies.



For Incurred Claims in H1 2025:

RANSOMWARE

56% of incurred claim count, contributing to 76% of the sum of amount incurred losses

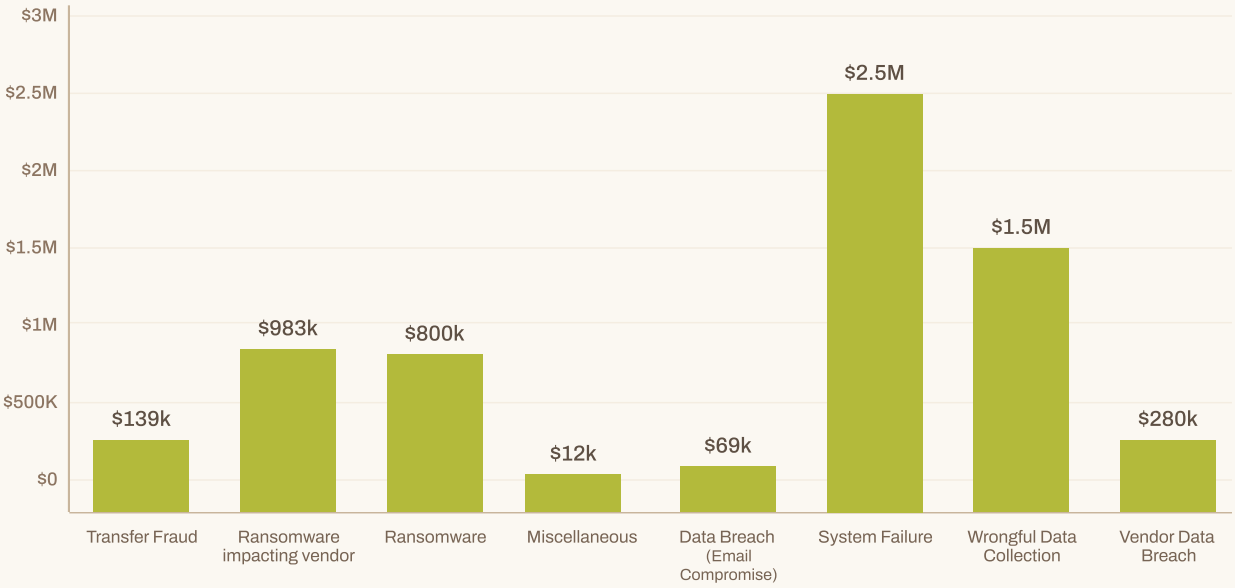
RANSOMWARE AFFECTING A VENDOR

At just 4% of our incurred claim count for the year, business interruption from ransomware affecting a vendor represents 15% of incurred losses

TRANSFER FRAUD

26% of incurred claim count, contributing to 8% of the sum of amount incurred losses

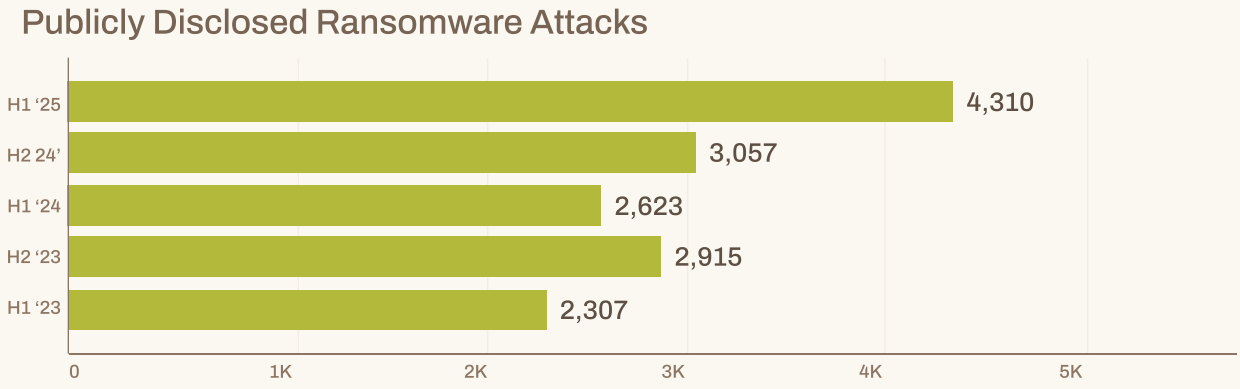
2024 Average Severity of Incurred Claim



Ransomware Threat Evolution: Key Insights from H1 2025

According to analysis conducted by the Resilience Risk Operations Center (ROC), the broader ransomware ecosystem underwent significant disruption and diversification in the first half of 2025. In Q1, ransom gang Scattered Spider abandoned the RansomHub platform in favor of the DragonForce platform. This move—together with some law enforcement activity associated with the group—caused a surge of attacks as ransomware affiliates rushed to cash in on planned campaigns before they were detected.

Among companies in the Resilience portfolio, researchers observed legacy groups fade while newer, more volatile actors rose to prominence, driving shifts in tactics and targets. This transition contributed to a large spike in publicly disclosed ransomware attacks during Q1, which our ROC attributed to multiple converging factors: Scattered Spider's platform switch created operational chaos; turf wars erupted among ransomware affiliates competing for territory; and intensified law enforcement activity pressured groups to accelerate their timelines. Attack volumes declined by 30% in Q2, though H1 ransomware attacks still exceeded the previous two quarters by 41%.



Global ransomware attacks increased 73% due to changes in the threat actor landscape.

Ransomware-related incidents are responsible for more than 90% of losses in the first half of 2025.

Ransomware affecting vendors is our fastest growing cause of loss at 15% of H1 2025 losses.

The attacks that did occur were more severe and unpredictable, particularly for mid-market organizations with lean security programs. This period tells a clear story: ransomware is becoming more dangerous, not less.

Globally, ransomware attacks across all sectors rose dramatically in the first half of 2025, but the details tell an evolving story. According to our analysis of publicly disclosed ransomware victim counts, ransomware attacks jumped 73% in Q1 largely due to changes in the ransomware threat actor landscape.

In Resilience's portfolio, ransomware incidents went from 5.8% of claims by frequency in 2024 to 9.6% in the first half of 2025, an increase of 65%. However, incidents are developing into claims with incurred losses at a slower pace: in 2024, 60% of ransomware claims led to losses, while so far in 2025 that rate has slowed to 42%. Many clients were able to recover from backups, which may also be driving a trend in demanding ransom for data suppression.

As threat actors evolve their extortion methods, we are commonly seeing double extortion, with primary extortion for decryption and secondary extortion to suppress exfiltrated data. In some reports, companies are even reporting triple extortion with the threat of bodily harm if ransom is not paid. While this is not something we have seen in the first half of this year, according to a recent report, over the past 12 months, executives were physically threatened in 40% of ransomware incidents.

Recommendations for Mitigating Ransomware

↘42%

of H1 2025 ransomware claims developed incurred cyber insurance losses

↘22%

clients affected by ransomware paid an extortion fee to threat actors

↗20%

increase in severity of ransomware attacks H1 2025 vs H1 2024

As companies improve their response to ransomware, payment rates have steadily declined. While Sophos' State of Ransomware report found that 46% of victims paid ransoms to recover their data, the Resilience portfolio saw significantly lower payment rates at just 22% in 2024. That number looks lower in the first half of 2025 with just 14% of ransomware claims involving a known extortion payment, according to early data.

Multiple factors influence whether clients pay extortion fees, but our data indicates that organizations with robust backup systems, regular validation testing, and comprehensive business continuity planning are far less likely to submit to ransom demands. This trend reflects a broader evolution in the threat landscape—ransomware attacks have grown far more sophisticated than simple file encryption, yet many organizations don't realize the gaps in their preparedness until they face a complex, multi-vector attack.

While many high profile attacks begin with a phishing attack or an exploited vulnerability, the speed with which actors move to take over and exfiltrate information is rapidly accelerating, with breakout occurring in fewer than 50 minutes, on average.

Many of the top “defense in depth” strategies against ransomware are well understood, if not always faithfully executed— backups, endpoint and network security, privileged access management, and many more play critical roles. Despite strong strategy and execution, some clients have given attackers unintended advantages.

DON'T PAY FOR DATA SUPPRESSION

Today's attackers steal data before encrypting it, then demand payment twice—once to unlock systems and again to prevent data publication. Paying for data suppression is a risky move with no guarantee of data destruction, while simultaneously providing no mitigation when it comes to regulatory investigations, notifying customers, or subsequent third-party actions.

With this in mind, organizations should prioritize building comprehensive resilience rather than relying on reactive measures. This means encrypting sensitive data by default, establishing clear breach protocols with pre-approved disclosure frameworks, and implementing intelligence-led defenses that can independently track stolen data without depending on ransom demands.

Leadership education is equally critical—executives must recognize that suppression payments offer only the illusion of protection. In reality, they can heighten long-term exposure by inviting repeat attacks and depleting insurance limits, ultimately perpetuating this form of cyber crime. A recent example underscores the risk: one company facing a class action lawsuit after a data breach was accused during settlement negotiations of diverting funds to criminals that could have gone toward compensating victims.

Meanwhile, cyber insurers must evolve beyond simply covering ransom payments to actively incentivizing security hardening, promoting intelligence sharing between clients, and providing robust post-breach support services that strengthen overall organizational resilience.

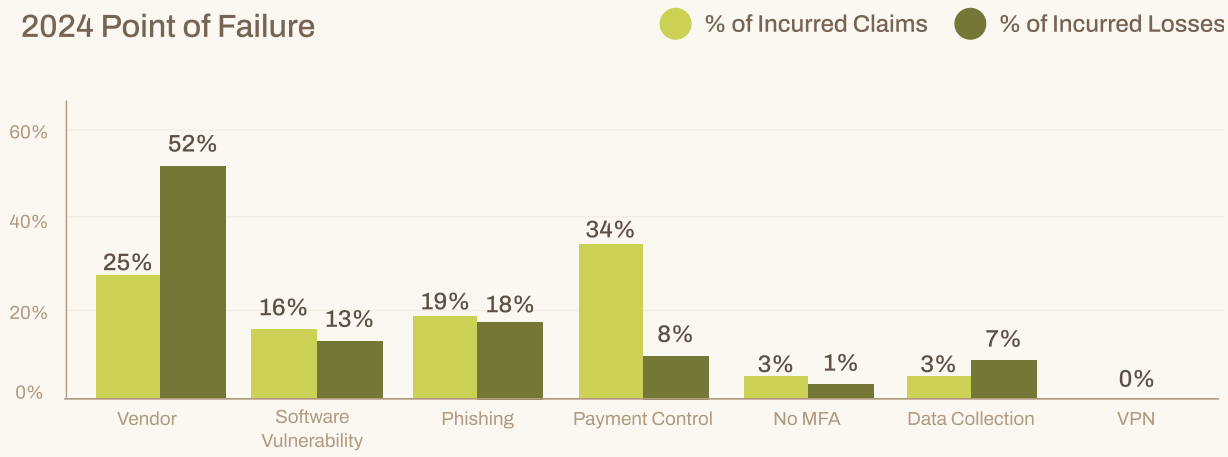
KEEP YOUR POLICY SAFE

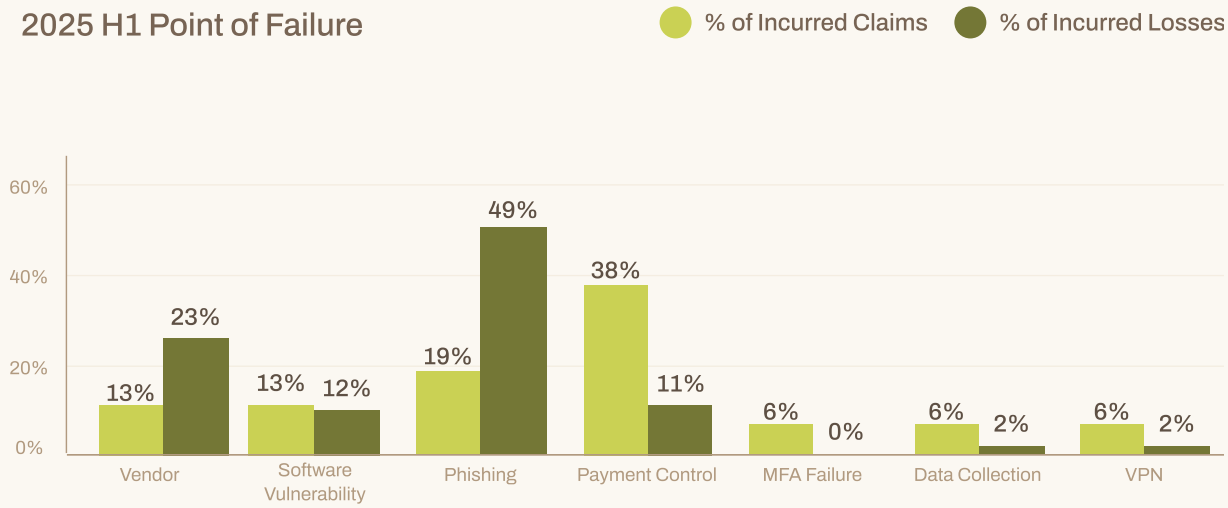
In at least two recent ransomware cases in the Resilience portfolio, threat actors located a copy of the client's cyber insurance policy and used that to determine their ransom demands. In one case, the threat actor directly referenced the client's policy, saying they had placed their extortion demand below the client's limit.

Protecting your cyber insurance policies isn't just about following best practices—it's about treating these critical documents with the same care you'd give your most sensitive customer data. Smart organizations are taking a comprehensive approach that starts with encrypted cloud storage featuring zero-knowledge architecture and AES-256 encryption, implementing identity-first security controls with role-based access and multi-factor authentication, and utilizing a specialized digital vault solution that goes beyond basic cloud storage. The goal isn't just compliance; it's peace of mind knowing your most important documents are truly secure.

At Resilience, we store your policy securely in our platform, though most clients receive a copy in email or store a copy in a file system. After verification, we recommend treating your policy as you would any crown jewel asset.

Point of Failure





**Point of Failure may differ from total loss analysis because point of failure is not known for all cyber claims. Point of failure analysis is different than cause of loss and indicates the control failure that leads to the loss.*

Findings

SOCIAL ENGINEERING

Phishing attacks continue to represent the most significant challenge in the threat landscape, responsible for 19% of incurred claims and 49% of incurred losses in H1 2025. Despite significant investment in security awareness training, phishing remains difficult to stop because its social engineering tactics often evade conventional security mechanisms. As a result, defending against these increasingly sophisticated social engineering campaigns requires ongoing innovation in both technology and training approaches.

Combined with social engineered financial attacks, social engineering accounts for 60% of losses in H1 2025.

VENDOR RISK

Vendor-related incidents persist as a point of failure in the Resilience portfolio with 22% of losses in 2024 and 15% in 2025 attributed to vendors experiencing ransomware, data breach, or system failure. While we have not seen a high impact vendor-related claim drive dramatic numbers of claims yet this year, clients have been affected by more isolates vendor outages that caused business interruption, a key driver in losses.

While many organizations rely on ratings programs and compliance checks to assess vendors, these only provide a snapshot of resilience at a single point in time. High-impact vendors require ongoing engagement to capture changes in their risk posture. At Resilience, the ROC continuously monitors vendor-related threats reported by clients and helps prioritize technical risks by their likely financial impact—so mitigation efforts are focused where they matter most.

TRANSFER FRAUD

Transfer fraud refers to internal failure of payment controls that results in fraudulent financial transactions; most often, these are carried out through social engineering. Business email compromise remains the leading driver, but attackers are now expanding their methods, using AI-driven voice synthesis to make their schemes more convincing and harder to detect.

Voice impersonation attacks have become a major threat, with voice-replication algorithms enabling criminals to exploit familiarity and trust when validating fraudulent transfers. The same techniques are also used in helpdesk impersonation, where attackers trick IT support teams into resetting passwords or disclosing sensitive information to gain privileged access.

Payment control failures now account for a significant share of cyber insurance activity—26% of incurred claims, and 8% of incurred losses in the first half of 2025. Yet the financial impact is likely understated, as transfer fraud coverage is often capped by sub-limits within cyber policies. In Resilience's portfolio, the average severity of $139,000 recorded in 2024 likely underrepresents the true scale of client losses.

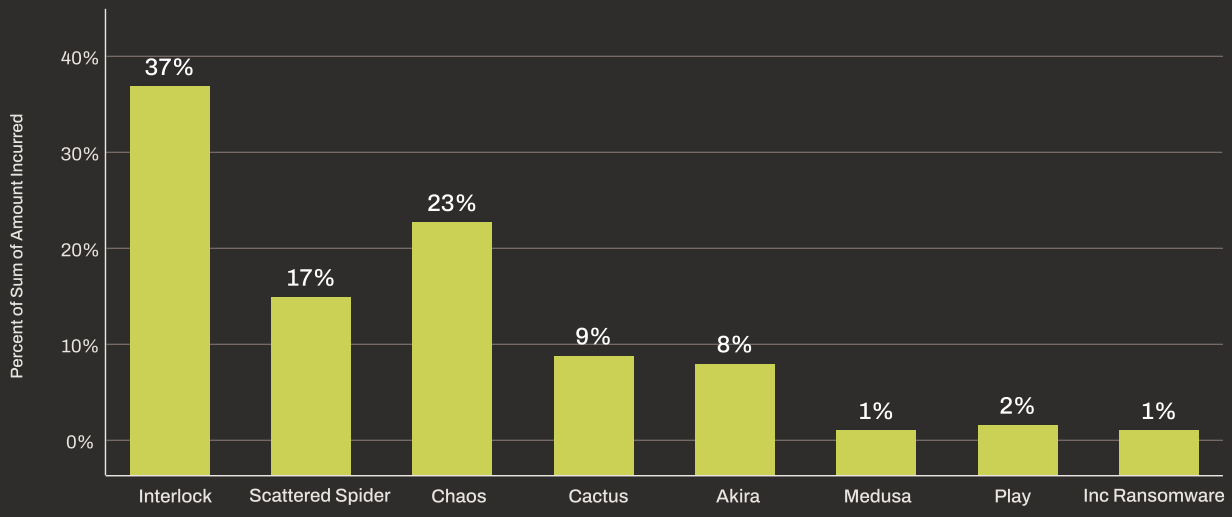
The scale of this threat can be seen in federal crime statistics. The FBI's 2024 Internet Crime Report documented over 21,000 business email compromise complaints, resulting in more than $2.7 billion in losses, making it the second most financially-damaging category of cybercrime after investment fraud.

Rogues Gallery

This year has underscored a troubling reality: cybercriminals are increasingly exploiting human error. Rather than relying solely on advanced malware or zero-day exploits, they are perfecting social engineering—using carefully crafted phone calls and impersonation schemes. The rise of AI-driven tools makes these tactics even more convincing, turning employees and colleagues into unwitting accomplices.

The following profiles represent the most active and impactful threat actors the Resilience ROC has tracked this year, as well as the groups that have been actively attacking the Resilience portfolio. Each tells a different story of criminal innovation, but together they paint a picture of an adversary that's becoming more sophisticated, more persistent, and more willing to cause real-world harm to achieve their goals.

Top Ransomware Gangs Attacking the Resilience Portfolio

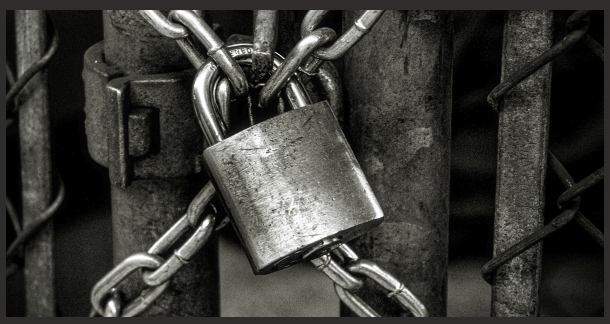


MEDUSA

Operates as a ransomware-as-a-service (RaaS) variant that employs a double extortion model, encrypting victim data and threatening to publicly release exfiltrated data if ransom is not paid. Over 300 victims impacted across critical infrastructure sectors as of February 2025.

AKIRA

A ransomware-as-a-service (RaaS) gang that emerged in March 2023 and has been linked to the dissolved Conti gang, operating with lightning-fast data exfiltration capabilities and generating $42 million in ransomware payments between March 2023 and April 2024 alone. They maintain a presence in financial services, suggesting continued sophistication in targeting and executing attacks against well-defended industries.



INTERLOCK

Known for targeting organizations across North America and Europe using double extortion tactics, this group emerged in 2024. They typically gain access through fake software updates or social engineering lures like ClickFix/FileFix tools, and deploy a range of tools, including remote access trojans, keyloggers, and CobaltStrike. Interlock supports cross-platform attacks on Windows, Linux, and FreeBSD, and has been linked to incidents across healthcare, finance, and government sectors. In Resilience's experience with Interlock, the group has located a client's policy and used it in ransom negotiations.

CHAOS

Operates as a ransomware builder that functions more like destructive wiper malware than traditional ransomware, with early versions permanently corrupting files rather than encrypting them, though later iterations evolved to include actual AES encryption capabilities. This group demonstrated significant impact in H1 2025 with attacks across multiple industries, showing a preference for high-value targets in real estate and manufacturing sectors. In our dealings with Chaos, the group was successful in extracting a payment for data suppression.

Highlight: Scattered Spider

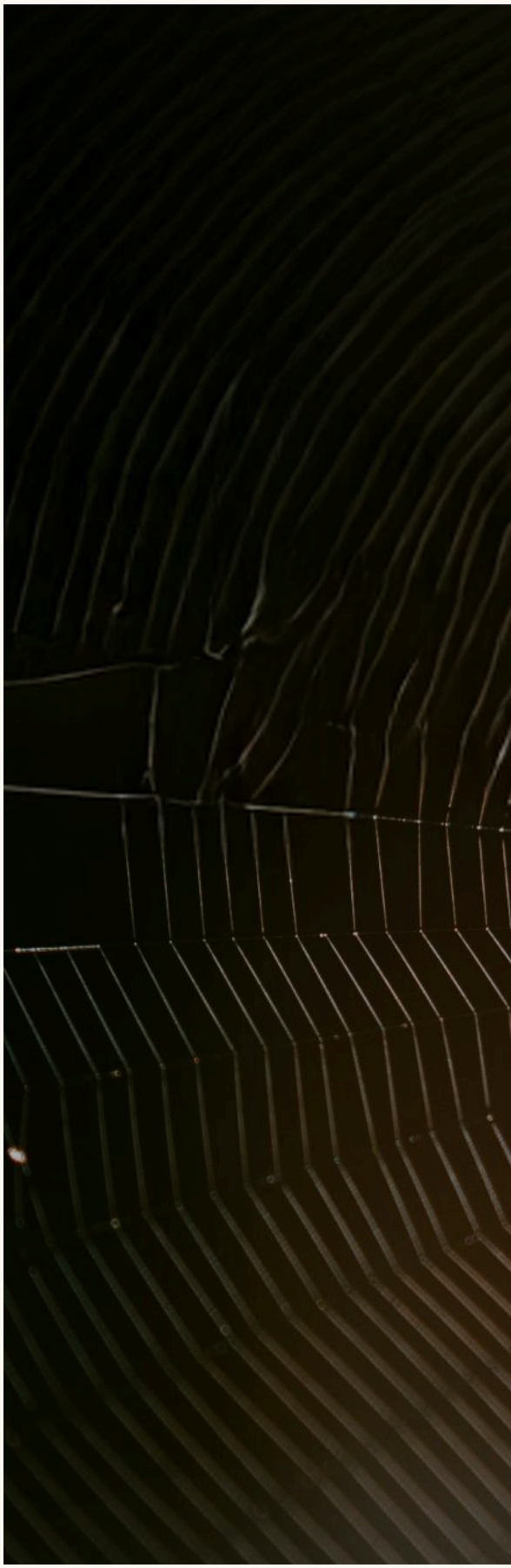
Scattered Spider stole the spotlight again in H1 2025, with high visibility attacks on retail, aviation, and insurance. A sophisticated, English-speaking cybercriminal group, Scattered Spider is believed to consist primarily of young UK- and US-based operatives and has been in operation since at least 2022. Its origins lie in a toxic subset of gaming culture where online harassment evolved into SIM swapping and eventually ransomware. The Resilience Risk Operations Center observed extensive activity from Scattered Spider in the first half of 2025.

Scattered Spider has a deep understanding of enterprise cloud platforms and has demonstrated an ability to leverage misconfigurations within globally used platforms, including Azure, AWS, and Microsoft 365. This, combined with an adept utilization of social engineering techniques that allow them to bypass traditional security controls, makes Scattered Spider particularly dangerous.

A wave of cyber attacks hit UK retailers in May 2025–including Marks & Spencer, Co-op, and Harrods–and quickly spread to impact major US retailers such as Victoria's Secret and Adidas. These attacks knocked not only these retailers offline, but also many of the downstream retailers they supply.

Recent reports also link Scattered Spider to cyber attacks on major airlines–notably the July 2025 data breach affecting six million Qantas customers–followed by a pivot targeting the U.S. insurance industry. This surge in activity comes after a quieter period following the arrest of five members in November 2024, suggesting the group's resilience and ability to continue operations despite law enforcement actions.

However, recent arrests by the UK’s National Crime Agency show that this group is more within reach of law enforcement—unlike Russian cybercriminal groups, which remain far more difficult to extradite or detain.



SCATTERED SPIDER PLAYBOOK

Scattered Spider is a sophisticated threat actor whose advanced social engineering tactics blur the lines between common cybercrime and nation-state tradecraft.

FOCUSED VERTICAL STRATEGY

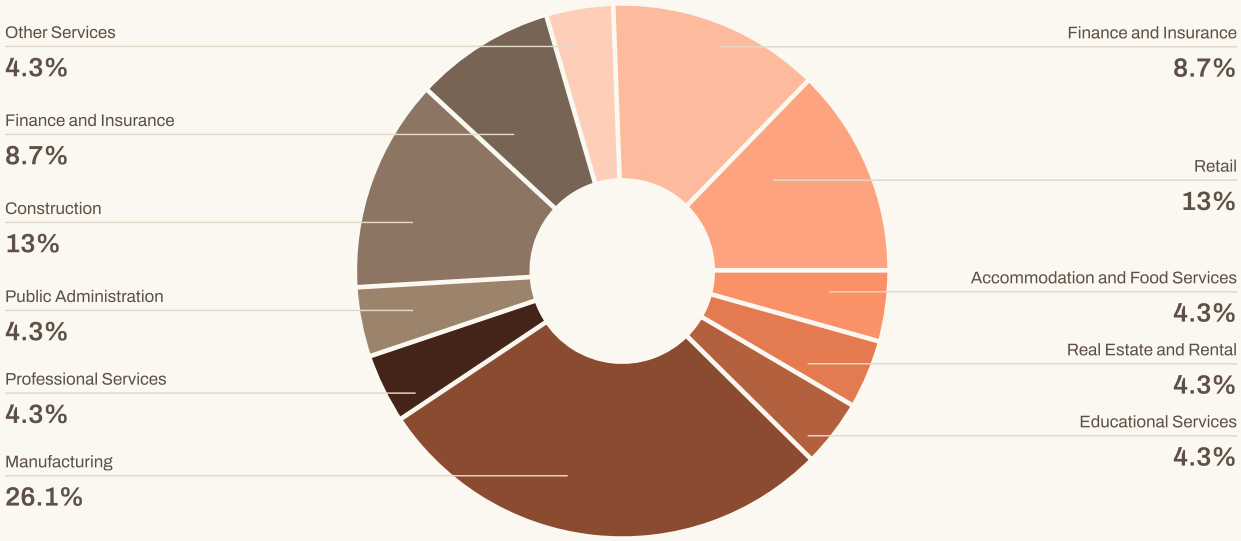
They tackle specific verticals at a time – as in recent retail attacks in the UK and their attacks on casinos in 2023 – which increases their disruptive impact on an entire industry sector.

SOCIAL ENGINEERING ATTACKS

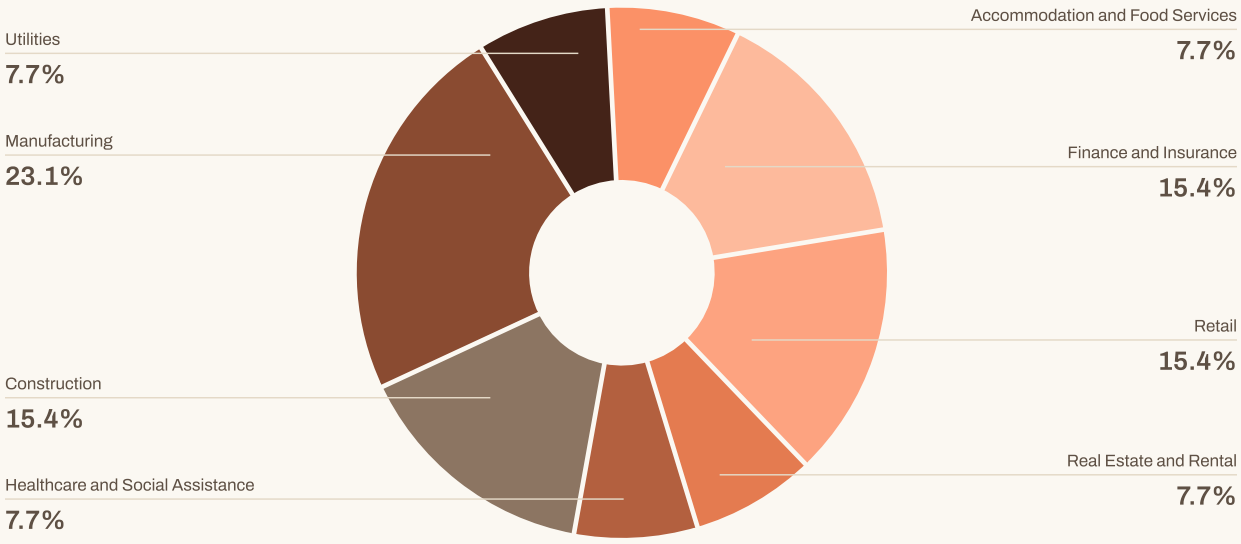
Unlike traditional cybercriminals who rely primarily on automated attacks, Scattered Spider employs real-time interaction with victims, dramatically increasing their success rates.

Sector-Specific Trends

H1 2025 Incurred Losses by Industry



H1 2025 Incurred Ransomware Claims by Industry



MANUFACTURING

Manufacturing organizations encountered significant cyber challenges in the first half of 2025, with several ransomware incidents generating claims averaging over $1 million in severity. We also saw multiple transfer fraud cases, which likely represent even higher unreported losses for affected organizations, given the sub-limited nature of this coverage.

Manufacturers face unique pressures that make them particularly vulnerable to extortion payments. Immediate business interruption losses can be catastrophic, while supply chain partners dependent on continuous operation often intensify pressure to restore systems quickly. This vulnerability manifests across multiple attack vectors: supply chain compromises—such as the CDK incident—accounted for 46% of sector losses among our clients in 2024, while direct ransomware attacks represented another 43% of total losses.

RETAIL

Retail losses from the Scattered Spider attacks in the spring affected the entire retail supply chain. Consumers, manufacturers, distributors, and downstream retailers were all left in the lurch . Retailer Marks and Spencer (M&S) in the UK took over 45 days to recover online ordering following an attack, which is believed to have cost upwards of £40 million a week.

While surprising at first glance, the experience of M&S is emblematic of broader sector-wide vulnerabilities. Retail, despite handling vast amounts of sensitive customer data, is still seen as lacking maturity in cybersecurity. Factors including under-resourced security teams, inadequate training, and reliance on third-party systems leave even major retailers exposed.

HEALTHCARE

In 2024, the healthcare sector suffered the most severe cyberattacks of any industry in the Resilience portfolio, with average losses reaching $1.3 million per incurred claim. By early 2025, extortion demands had climbed as high as $4 million, evidence of cybercriminals' relentless focus on this critical infrastructure.

Healthcare's status as a prime cyber target stems from the convergence of valuable digital assets and systemic vulnerabilities. Electronic health records hold personal and financial data with long-term criminal value, making them far more lucrative than credit cards on the dark web. At the same time, the sector's life-critical operations give attackers added leverage—hospitals cannot risk prolonged downtime when patient lives are at stake.

This creates a dangerous paradox. Industry guidance increasingly discourages ransom payments, yet healthcare organizations often face overwhelming pressure to restore services immediately. Recent cases highlight this dilemma: even with robust backup strategies, some providers were forced to pay ransoms to bring radiological and diagnostic imaging systems back online for urgent patient care. These realities underscore the need for healthcare organizations to go beyond standard compliance frameworks, designing disaster recovery plans that prioritize uninterrupted delivery of care above all else.

[Read more in our report, US Healthcare and Cyber Risk.]

roc Resilience Risk Operations Center

Case Study in Loss Control

Claims in Action: Chaos Ransomware Data Suppression

In February 2025, a high-end real estate firm was alerted by Homeland Security that it had been compromised by the Chaos Ransomware group. Attackers exfiltrated hundreds of gigabytes of sensitive client data—including Social Security numbers, financial statements, and personal details of prominent residents—and demanded $4 million for its release. Unlike many victims, the firm leveraged viable backups to maintain partial operations, though the potential exposure of confidential client data posed a severe reputational threat. While Resilience does not recommend paying extortion fees for data suppression, the client's policy allowed it, and our claims team coordinated with expert partners to negotiate the most favorable outcome.

Because the attack did not cause business interruption, the negotiation team had greater leverage. They employed calculated delays, periods of strategic silence, and psychological pressure tactics to exhaust the attackers' patience. Throughout the 10-day process, the Resilience Claims team managed client expectations and secured real-time insurer approval for counteroffers. The client's ability to withstand the initial encryption attack ultimately expanded their options at the negotiating table.

ROC RESPONSE

Resilience's crisis team took a strategic, deliberate approach tailored to the client's primary concern of data suppression to protect their clients— and their firm's reputation.

RESULTS

The patient negotiation strategy achieved an 85% reduction from the initial $4 million demand, with final settlement at approximately $615,000. The pace caused the threat actor to grow impatient, ultimately bringing their demand down to $2 million before final negotiations.

The ROC in Action: Microsoft SharePoint ToolShell Vulnerability

The Resilience Risk Operations Center operates as a fusion center, bringing together world-class teams across underwriting, claims, cybersecurity, data science, and threat intelligence into a single collaborative environment. Unlike traditional Security Operations Centers that are internally focused and reactive, the ROC functions like an Air Operations Center—externally facing and designed to create coordinated effects across our entire client portfolio. While most insurers focus on minimizing losses after incidents occur, the ROC proactively identifies and neutralizes threats before they can cause incurred damage.

In July 2025, Eye Security observed active exploitation of a zero-day Microsoft SharePoint vulnerability dubbed "ToolShell." Microsoft released emergency advisories the following day, with threat actors already conducting bypass techniques against enterprise environments. The vulnerability posed significant risk to organizations with SharePoint deployments, particularly those in sectors with high-value data targets.

ROC RESPONSE

The ROC immediately analyzed the entire client portfolio upon Eye Security's initial alert, working directly with affected customers to implement Microsoft's emergency guidance and patches. Targeted incident notifications were delivered to high-risk clients based on exposure analysis.

RESULTS

One client received ROC notification just as threat actors attempted exploitation, enabling mid-attack detection and containment. The early warning system prevented data exfiltration and limited business disruption to 1-2 days of partial operations.

"The ToolShell incident perfectly demonstrates why the ROC exists — we identified the threat within hours of Eye Security's alert and had targeted notifications out to our highest-risk clients before most organizations even knew they were vulnerable. That's the difference between reactive security and predictive defense."

Jud Dressler
Director of the Resilience Risk Operations Center

Appendices

Methodology

The data and insights presented in this report are derived from Resilience's internal insurance claims portfolio and threat research team. Our analysis covers claims reported and processed during the first half of 2025, with comparative data extending back to 2023 to provide context for emerging trends.

The incurred claims threshold of a non-zero loss is applied consistently across all time periods to ensure comparability. Our analysis includes both the frequency of incidents (number of claims) and their severity (financial impact) in order to provide a comprehensive view of the cyber risk landscape.

Definitions and Glossary

Average cost of a ransomware attack	The full amount Resilience is liable to pay for a claim.
Incurred claim	A claim notice that resulted in or is expected to result in a non-zero dollar loss.
Third-party risk/Vendor risk	Cyber incidents that originate from or significantly involve vendors, suppliers, or other third-party service providers in an organization's digital ecosystem.
Point of failure	The initial method or vulnerability that cybercriminals exploit to gain unauthorized access to an organization's systems or data.
Cause of loss	The type of cyber attack or incident that ultimately leads to financial losses, such as ransomware, business email compromise, or data breaches.
Double extortion	A ransomware strategy where attackers demand payment both for decrypting files and for preventing the public release of stolen data.

Data Sources and Limitations

The data sources for this report include internal Resilience sources, including raw claims and financial loss data and risk and threat intelligence.

While our portfolio provides significant insights into cyber risk trends, it represents the experience of Resilience's specific client base and may not reflect the broader market experience. Additionally, the full impact of some incidents may not be reflected in H1 2025 data due to the time required for complete loss development and reporting.

* *This report represents our analysis of cyber risk trends based on actual claims experience and threat intelligence. For the most current information and specific guidance for your organization, please consult with Resilience's risk management and insurance professionals.*

See the latest trends and analysis in cyber claims