resilience | roc Resilience Risk
Operations Center

2025 *Cyber* Risk Report

20
25

Table of Contents

Executive Summary

The 2025 cyber threat landscape was defined by a fundamental shift in criminal economics: the pivot from extortion through operational disruption (encryption) to reputational leverage (data theft). As organizations improved their backup and recovery capabilities, threat actors adapted by targeting the data itself, rendering traditional "recovery-focused" defenses insufficient.

Fueled by AI-amplified social engineering and a surge in litigious activity, the financial severity of claims has become increasingly concentrated. Resilience's 2025 claims data demonstrates that cyber criminals are no longer optimizing solely for immediate business disruption. Instead, attacks are now designed to generate sustained financial, regulatory, and reputational damage that extends well beyond the initial incident—accumulating over months and years rather than days.

Extortion tactics have evolved, with multiple layers of ransom demands adding to the financial impact of an attack. Criminals may demand ransom payment for data de-encryption, then to suppress stolen data from being exploited, and then to demand payment from victims' data constituents to avert reputational damage.

For the modern enterprise, the primary risk is no longer just "going offline"—it is the multi-year legal, regulatory, and reputational "tail" that follows a data exposure event. As the business of cybercrime reaches higher maturity levels, the real risk comes not just from disruption—but duration.

→ TOP TAKEAWAYS

01 **Extortion evolved from encryption to data theft.**

Data theft-only attacks accelerated from 49% of extortion claims in H1 to 65% in H2, rendering backup-based defenses ineffective against the primary threat: reputational and regulatory damage from data exposure.

02 **AI-amplified social engineering to unprecedented effectiveness**

Phishing surged to become the #1 point of failure, jumping from 21% of incurred losses in 2024 to 50% of incurred losses in 2025. While it is difficult to attribute any given attack to AI, the increased success may be explained by AI's ability to automate more believable attacks.

03 **Vendor risk continues to be a major cause of loss**

Vendor-related failures accounted for 22% of losses in 2024 with a modest decline to 18.8% in 2025. When a critical vendor serving an entire industry is compromised—as CDK Global was in 2024—losses concentrate across the supply chain simultaneously. While losses became more distributed by industry in 2025, vendors remained a key area of risk exposure.

04 **Waves of litigation extend risk**

Between the "no honor among thieves" reality—where threat actors continue selling data they were paid to suppress—and an increasingly litigious plaintiffs' bar eager to file lawsuits, the tail risk of ransom events is a growing concern from an underwriting perspective. Additionally, a wave of litigation over non-breach privacy and data collection practices on websites spurred a twofold increase in wrongful data collection claim notices in 2025. Few have resulted in losses that exceed clients' self-insured retention.

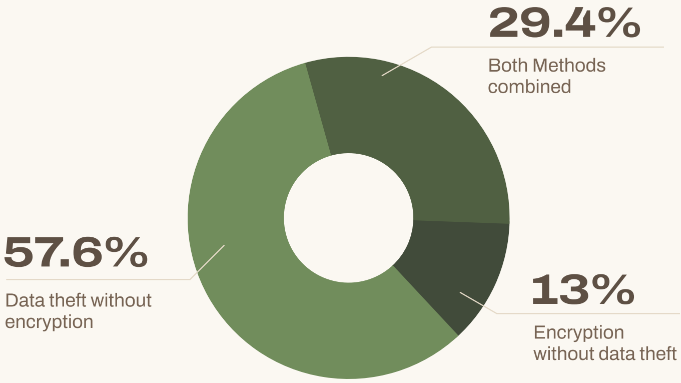
2025 in Review

The year ransomware pivoted away from encryption.

FROM ENCRYPTION TO DATA EXPOSURE: HOW THE PRIMARY THREAT EVOLVED

Throughout 2025, cybercriminals systematically shifted from ransomware based on encryption of data to pure extortion based on data theft. The acceleration was dramatic: data theft-only attacks rose from 49% of extortion claims in H1 to 65% in H2.

The full year breakdown



The shift reflects both law enforcement pressure and operational efficiency. As authorities successfully disrupted major ransomware operations and organizations improved backup capabilities, threat actors adapted by simplifying their approach: steal data, threaten to publish it, collect payment. No need for complex encryption tools, no need to maintain decryption infrastructure and, critically, no way for victims to recover through security operations alone.

This tactical evolution changed which organizations faced the highest losses. When the primary leverage shifted from operational disruption to reputational damage, the severity of successful attacks concentrated in sectors where exfiltrated data creates substantial regulatory and reputational exposure: healthcare's electronic health records triggering HIPAA notification requirements, retail's customer databases creating regulatory exposure under data protection laws, and exposure of manufacturing's intellectual property and operational data.

"We're seeing an alarming trend where paying for data suppression has proven unsuccessful," Maria Long, Resilience Chief Underwriting Officer, says. "In many instances, even when the insured pays the threat actor to suppress stolen data—and there is a belief that the stolen data has been destroyed, a dubious proposition—based on notification laws, the victims are nonetheless notified of the theft, and there is often a resulting class action lawsuit from consumers whose information has been exposed."

Moreover, plaintiffs' attorneys have argued that defendants chose to pay criminals over compensating the actual victims. This legal pressure, combined with the "no honor among thieves" reality—where threat actors continue selling data they were paid to suppress—makes the tail risk on ransom events a growing underwriting concern.

In May, notorious crime group Scattered Spider continued its trend of focusing on specific industry sectors by targeting retailers in a brutal campaign. Whether they encrypted systems or simply exfiltrated data, the leverage was the same: stolen customer data and payment information creating immediate regulatory notification obligations and lasting reputational damage. The sector went from near-zero material losses in the Resilience portfolio in 2024 to become one of the top three leading loss industries with a $2.6 million average severity—not because retail infrastructure suddenly became vulnerable, but because threat actors discovered that retail's distributed workforce, customer service authentication procedures, and concentrated customer data created perfect conditions for extortion, whether or not encryption was deployed.

THE PATH FORWARD: PREPARATION MATTERS

Organizations must prepare for the reality that successful attacks, driven by the shift from operational disruption to reputational and regulatory exposure, now carry substantially higher financial severity than in previous years.

This means:

Comprehensive insurance coverage that reflects 2025's severity levels, not historical averages. Organizations across all sectors need limits that reflect the concentrated severity documented in 2025. Transfer fraud, extortion, and contingent business interruption protection become essential across all industries.

Security investments focused on the attacks that are actually succeeding: AI-amplified phishing that achieves 54% success rates requiring enhanced employee training; session hijacking and OAuth abuse that bypass traditional MFA; and data loss prevention to address the 65% of extortion attacks that skip encryption entirely.

Vendor risk management that acknowledges you cannot control the security of your entire supply chain but can prepare for the cascading impacts when vendors are compromised. This includes continuous assessment, contingency planning, alternative sourcing strategies, and insurance coverage for vendor-originated losses.

Incident response preparation that assumes attacks will be more sophisticated and more costly than historical experience suggests. This includes tabletop exercises, which can meaningfully decrease the scope and severity of an event by familiarizing stakeholders with the team that would handle a real attack, resulting in a coordinated and rehearsed response. Additionally, breach and attack simulations find holes in current defenses, while legal defense mobilization alongside technical recovery, multi-year claim timeline planning, and stakeholder communication strategies all become standard components of cyber preparedness.

Additional Key Trends

AI-AMPLIFIED SOCIAL ENGINEERING

The phishing resurgence documented in 2025 suggests AI is making a significant impact on the threat landscape. After declining in 2024 as organizations improved security awareness training, phishing losses surged to a severity of over $1.6m per claim.

In 2025, an increasing number of phishing-related failures led to ransomware and extortion demands rather than other lower-severity threats, driving up losses related to this point of failure.

This reversal relates to AI-generated phishing campaigns achieving 54% success rates compared to just 12% for traditional phishing—a 4.5x effectiveness multiplier, according to a 2024 study by researchers from Harvard University and Harvard Kennedy School, Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects. These tools enabled attackers to craft perfectly worded messages, convincingly impersonate executives, and operate at scale without the language barriers that previously flagged attacks.

The pattern confirms that traditional security awareness training alone is insufficient. Organizations need technical controls—phishing-resistant MFA, email authentication protocols, behavioral analytics—to augment human judgment that can no longer reliably distinguish sophisticated attacks from legitimate communications. However, Resilience data shows that employee training programs do make a financial difference. Companies that implemented phishing awareness and regular security training reduced their total potential risk by over $100,000 according to Resilience Cyber Action Plan modeling.

Looking ahead, deepfakes represent the next frontier. AI-generated audio and video that's indistinguishable from reality will enable executive impersonation in video calls and real-time voice synthesis attacks. Traditional verification methods based on recognizing voices or faces will become a far less reliable safeguard, requiring organizations to implement out-of-band confirmation channels for high-risk decisions. Clients that implemented more stringent security on wire transfers, such as dual approvals, reduced their overall risk by an average of $795,000.

VENDOR RISK EVOLUTION

Vendor-related failures remained the second-highest loss category with an average severity of $1.36 million per incident for incidents with incurred losses.

While most companies affected by vendor outages are able to recover without substantial business interruption, the persistent high average severity demonstrates that when vendor compromises lead to business interruption, they still generate substantial losses, as demonstrated by the concentration of losses that can ripple from a single event. For example, in 2024 CDK contributed significant losses to companies in the automotive supply chain; separately, vendor-originated breaches in healthcare affected over five million patient records in one re-extortion case.

The vendor risk landscape now includes three distinct vendor risk categories: vendor ransomware attacks that cascade to clients in the form of business interruption, vendor data breaches that expose client information, and non-malicious vendor outages that disrupt operations without malicious intent. Each requires different mitigation strategies.

IDENTITY AS THE NEW PERIMETER

As traditional network defenses harden, identity has persisted as the primary battleground in 2025. Infostealers evolved from nuisance malware into the primary precursor for enterprise breaches, harvesting 2 billion credentials in the first half of the year, according to Resilience threat researchers. These tools enable session hijacking that can circumvent certain multi-factor implementations.

The data shows that the majority of ransomware victims find evidence of infostealers in their environment that precedes the main attack, marking credential compromise as a critical early warning signal. Organizations must hunt for infostealer compromise, assume breach when credentials are detected, and rotate session tokens immediately.

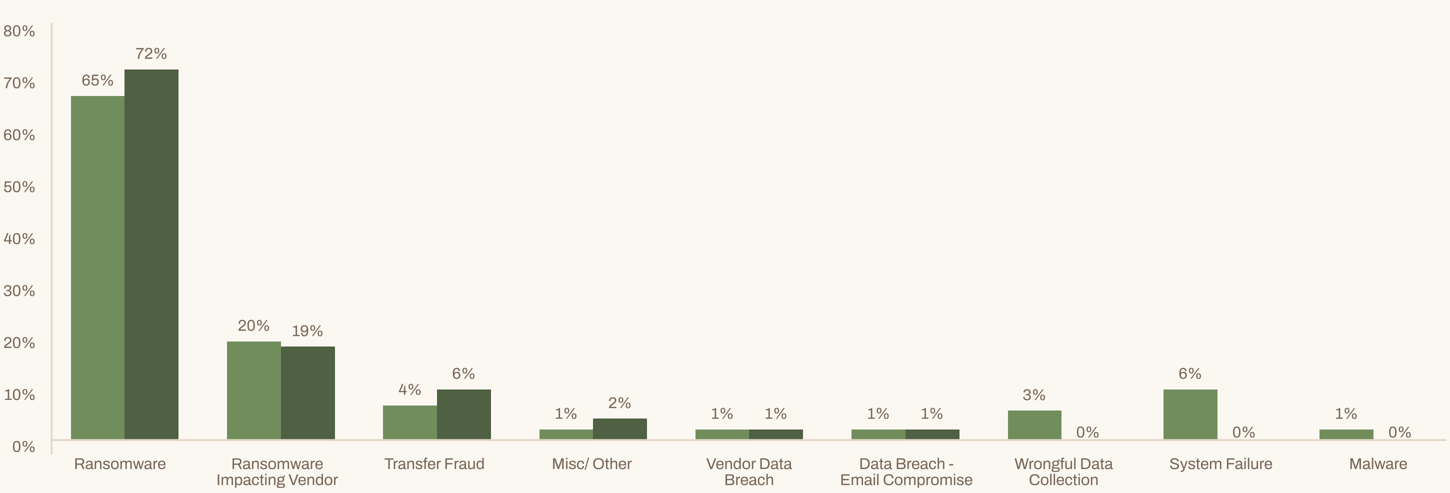
Beyond password theft, attackers leverage OAuth and API vulnerabilities. Third-party connected applications provide entry points that bypass traditional authentication. The deployment of autonomous AI agents capable of executing thousands of API requests per second to exfiltrate data demonstrates how identity-based attacks will scale in 2026.

AGGRESSIVE LAWSUITS SPUR WRONGFUL DATA COLLECTION CLAIMS

Wrongful data collection claim notices more than doubled from 2024 to 2025, driven by a wave of litigation targeting organizations' website data collection practices—specifically how visitor data is gathered, stored, and shared with third parties. The suits, often filed by individuals or brought as class action lawsuits, allege violations of the California Information Privacy Act (CIPA) based upon the use of tracking pixels, placing telemarketing calls to individuals on the Do Not Call Registry, or for privacy issues related to health information.

While some highly-publicized wrongful collection claims have resulted in large awards, claimants more frequently make lower-value demands that fall within the organization’s self-insured retention. While these claims can be contentious, organizations often find it more cost-effective to seek an early resolution rather than incurring the significant expense of a legal defense or arbitration, which also helps to mitigate reputational damage.

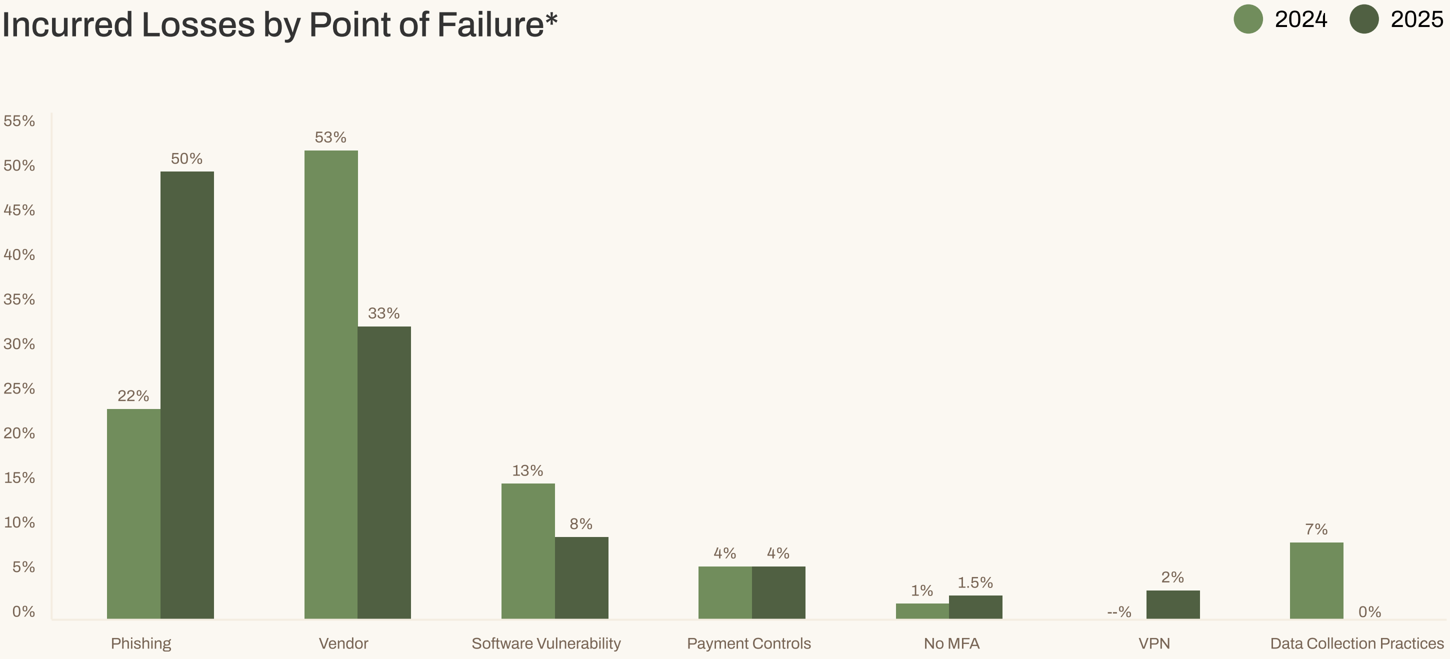
Incurred Claims Cause of Loss 2024-25



Point of Failure Analysis

Understanding how attackers gain initial access reveals both the effectiveness of AI-amplified threats and areas where defenses improved. The 2025 data shows some significant shifts from 2024 patterns.

Incurred Losses by Point of Failure*



*Analysis of losses for claims where point of failure is known.

The change in year-over-year severity in claims that originate in a phishing attack is stark and represents a shift in those attacks leading to ransomware events versus data breach or transfer fraud, which were more common in years past. While it's too early to call this change a trend, this highlights the direct connection between phishing and extortion and the significant impact that this can have on mid-sized to large enterprises.

While the severity and frequency of attacks due to supply chain and vendor-related issues dropped by just over a quarter, the potential impact of these attacks remains pronounced for companies that rely on software and cloud partners for critical functions.

Software vulnerability exploitation declined slightly (5.5%), indicating either improved patch management or threat actors shifting focus to identity attacks that are more scalable.

> You can outsource your services, but you cannot outsource your risk."

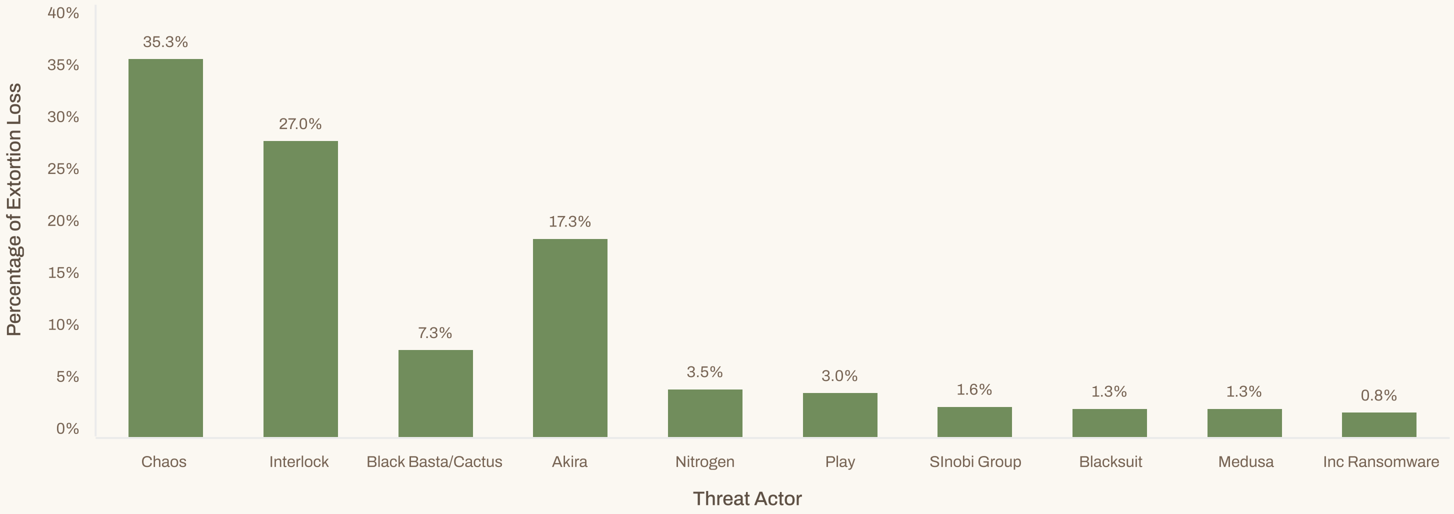
Jeremy Gittler
Global Head of Claims

Threat Actor Landscape

The 2025 threat landscape was dominated by a few high-impact groups executing sophisticated, high-severity attacks rather than high-frequency campaigns. This represents a fundamental shift in ransomware economics: rather than encrypting as many victims as possible, threat actors became more selective, researching targets carefully to maximize potential payouts.

What we used to refer to as “big game hunting” has transformed into a lucrative and scalable approach to extorting ever-more-valuable companies.

Top Ransomware Gangs by Incurred Losses



SCATTERED SPIDER

Scattered Spider dominated headlines throughout 2025, though the group's structure evolved significantly as the year progressed. A sophisticated, English-speaking cybercriminal collective consisting primarily of young UK- and US-based operatives, Scattered Spider demonstrates deep understanding of enterprise cloud platforms (Azure, AWS, Microsoft 365) and employs real-time social engineering that bypasses traditional security controls.

In May 2025, coordinated attacks hit major UK retailers (Marks & Spencer, Co-op, Harrods) and US retailers (Victoria's Secret, Adidas), with the M&S incident alone generating losses exceeding £40 million per week. Subsequent attacks targeted major airlines and the U.S. insurance industry.

What appeared to be Scattered Spider's disappearance in H2 2025 was actually a strategic transformation. The group merged with members of Lapsus, ShinyHunters, and the broader collective known as The Com to form Scattered Lapsus Hunters (SL/SH). This hydra-like structure—where one or two arrests lead to eight replacements—makes attribution difficult and operations resilient. Some reporting credits individual legacy groups while others attribute attacks to SL/SH, but membership shifts fluidly as operational needs change.

Unlike Russian cybercriminal groups beyond extradition, Scattered Spider's UK and US base makes them theoretically accessible to law enforcement. However, the decentralized nature of SL/SH—where individual operators communicate via encrypted platforms and collaborate opportunistically—creates a persistent threat that arrests alone cannot eliminate.

INTERLOCK

The largest individual loss in the Resilience portfolio for 2025 can be attributed to an attack by Interlock. Operating as a ransomware-as-a-service platform that emerged in 2024, Interlock employs double extortion tactics with sophisticated social engineering, targeting healthcare, finance, and government sectors.

Their most concerning capability: policy reconnaissance. Interlock actors locate and read client cyber insurance policies to inform ransom demands, calibrating asks to maximize payment likelihood while staying below coverage limits. This tactic demonstrates how threat actors are professionalizing their approach, treating extortion as a business with careful target research and pricing strategies.

CHAOS

Chaos generated two cases with multi-million-dollar damages across six total attributed incidents, demonstrating both frequency and severity. Operating as a ransomware builder that evolved from destructive wiper malware to proper encryption, Chaos focuses on high-value targets in real estate and manufacturing.

AKIRA

Akira's persistent targeting resulted in a high conversion rate with 40% of incidents converting to incurred claims at $800k average severity. This ransomware-as-a-service gang generated more than $3.2 million in losses across the Resilience portfolio in 2025.

Their lightning-fast data exfiltration capabilities allow them to steal massive amounts of data before detection, providing leverage even if organizations quickly isolate compromised systems. The group's financial services focus suggests continued sophistication in attacking well-defended industries.

Industry Analysis

Three sectors—manufacturing, healthcare, and retail—accounted for 68% of all portfolio losses, yet each experienced fundamentally different attack patterns and outcomes.

MANUFACTURING

Manufacturing retained its position as the highest total loss industry, though average severity declined by approximately 29% from 2024 to 2025. Anecdotal analysis suggests organizations in the sector improved backup strategies and incident response capabilities, which likely contributed to this decline. Higher policy retentions in the sector may also be a factor. Claims in manufacturing firms were not as frequent as those in finance or healthcare, and they were not as severe as those in healthcare or retail. However, the sector led in percentage of incurred losses in the Resilience portfolio at nearly 30%.

The persistence of manufacturing as the top target reflects fundamental vulnerabilities: just-in-time supply chains create extortion pressure as every hour of downtime disrupts customer deliveries, antiquated systems and deficiencies in IT/OT security, and downstream partners demand rapid restoration to maintain their own operations.

HEALTHCARE

Healthcare remains the highest-severity sector in our portfolio. While its 1.2% materialization suggests low frequency, the per-incident impact is more extreme due to the high concentration of sensitive data.

Electronic Health Records (EHR) hold long-term criminal value far exceeding credit cards on dark web markets, while life-critical operations create extortion leverage that few other industries face. Organizations that did not include vital records such as medical imaging in their backup strategy faced the threat of lapse in care if they did not submit to threat actor demands.

The re-extortion trend hit healthcare particularly hard, with one primary care provider compromised through a vendor affecting millions of patients—occurring against the backdrop of a previous ransomware attack.

Despite industry guidance increasingly discouraging ransom payments, the operational reality of patient care often overrides security best practices. Hospitals cannot risk prolonged downtime when patient lives are at stake, creating a paradox that attackers exploit ruthlessly.

RETAIL

Retail became 2025's outlier story, jumping from zero material losses in 2024 to become the second-highest average severity in the portfolio. This dramatic escalation was driven almost entirely by Scattered Spider's May 2025 campaign targeting major UK retailers (Marks & Spencer, Co-op, Harrods) before spreading to US retailers (Victoria's Secret, Adidas).

The M&S incident exemplified the devastating impact: 45 days to recover online ordering functionality, with losses exceeding £40 million per week. The attack exposed sector-wide vulnerabilities: under-resourced security teams relative to IT complexity, heavy dependence on third-party payment and e-commerce systems, and massive volumes of customer data.

The critical question for 2026: whether Scattered Spider's tactics—exploiting authentication procedures and distributed workforce vulnerabilities—will be adopted by other threat actor groups targeting retail and adjacent sectors with similar operational characteristics.

Looking Ahead to 2026

Based on 2025's data and threat landscape evolution, the following developments will shape the cyber risk environment in 2026:

EXTORTION-ONLY BECOMES THE DOMINANT MODEL

Data theft without encryption will continue its rapid acceleration as threat actors skip encryption entirely and demand payment to suppress stolen data. Based on 2025 trends showing extortion-only attacks rising from 49% in H1 to 65% in H2, this model may represent the majority of extortion incidents by year-end 2026.

Implication: Organizations must move from recovery-focused strategies (backups and incident response) to prevention-focused strategies (data loss prevention, zero trust architecture, encryption at rest, and identity containment).

DEEPFAKES REACH CRITICAL MASS

AI-generated deepfakes will become indistinguishable from reality, enabling automated social engineering campaigns at unprecedented scale. Organizations must prepare for executive impersonation in video calls and real-time voice synthesis attacks that bypass traditional verification methods.

Implication: Voice recognition and video calls are no longer sufficient for verification. Organizations need multi-factor authentication for high-risk decisions and out-of-band confirmation channels.

AI ADOPTION CREATES NEW ATTACK SURFACE

The first major breaches tied directly to AI adoption—not AI-assisted attacks, but vulnerabilities created by rushing AI tools into production—will materialize in 2026. Privacy violations from employees using AI tools improperly will generate unexpected claims that don't fit traditional data breach molds.

Implication: Organizations must implement AI acceptable use policies and governance frameworks before deployment, with clear guidelines on handling sensitive data in AI systems.

LITIGATION WILL FOLLOW MOST INCIDENTS

Lawsuits will follow most cyber incidents within days—sometimes before organizations fully understand what happened. Claim timelines will extend to 2-3 years as litigation, forensic accounting, and regulatory proceedings run parallel tracks.

Implication: Incident response planning must include immediate legal mobilization, not just technical recovery.

HYBRID EXTORTION MODELS MULTIPLY PRESSURE

Attackers will target companies, their subsidiaries, suppliers, and customers simultaneously in “portfolio extortion” campaigns that create network effects of pressure. Multiple tactics in sequence—encryption, data theft, DDoS, psychological warfare—will become standard rather than exceptional.

Implication: Incident response must account for cascading impacts across the ecosystem, not just direct organizational impact. Business continuity planning requires supply chain disruption scenarios.

THIRD-PARTY RISK DOMINATES HEADLINES

Even as organizations strengthen their own defenses, vendor and service provider compromises will drive the largest incidents. Ecosystem risk—not internal security gaps—will be the primary concern keeping CISOs awake, as organizations realize much of their exposure sits outside their own walls.

Implication: Contingency planning and business continuity for vendor failures becomes more critical than vendor security assessments. Insurance policies must reflect vendor dependencies.

INSURANCE MARKET SHIFTS

Coverage creep will intensify as traditional insurance products exclude AI risks, pushing exposures onto cyber and Tech E&O policies. Insurance gaps will become a board-level governance issue as the gap between exposure and coverage widens. Operational impact losses and litigation costs will rival or exceed direct response costs.

Implication: Organizations must quantify their value at risk and ensure coverage aligns with actual exposure, not just historical claims. Those who can articulate risk clearly will secure better placement.

IDENTITY PERIMETER COLLAPSES

Credential compromise will accelerate as infostealers harvest valid sessions at scale. Session hijacking and OAuth abuse will render traditional MFA ineffective without phishing-resistant authentication. The majority of ransomware victims will appear in stealer logs before their main attack.

Implication: Hardware tokens or passkeys become mandatory; SMS and push-notification MFA are insufficient. Organizations must hunt for infostealer compromise and assume breach when detected.

What Business Leaders Can Do

The shift to data theft-focused extortion in 2025 requires leaders to understand that comprehensive preparation matters more than prediction. The following guidance addresses the distinct needs of CFOs, CISOs, and CROs based on the year's learnings.

FOR CFOS

Shift investment from backup to prevention.
While backup infrastructure remains necessary for the 35% of attacks that still use encryption tactics, the 65% of extortion attacks that rely on data theft require different defenses. Invest in data loss prevention systems, zero trust architecture, and identity containment rather than solely focusing on recovery capabilities.

Implement more comprehensive transfer fraud coverage.
Transfer fraud comprises 26% of claim frequency but only 8% of incurred losses in our portfolio, illustrating the impact of industry-wide sublimits on these losses. Organizations are shouldering the losses for business email compromise and payment fraud. The $160k average severity understates actual impact.

Plan for severity concentration, not current sector averages.
Retail transformed from zero material losses to $2.6 million average severity in a single year when Scattered Spider identified systematic authentication vulnerabilities that enabled coordinated campaigns across the sector. Finance maintained the lowest average severity at $294k through sustained security investment and mature incident response.

FOR CROS

Model tail risk and severity concentration, not sector averages.
The 2025 data demonstrates concentrated severity even as overall portfolio metrics improved: few healthcare claims (1.2%) incurred losses, but those experiencing losses faced $2.6 million average severity. Risk models must account for the substantial difference between no loss and severe loss, requiring organizations to plan for worst-case scenarios rather than average outcomes. The multi-year legal and regulatory tail following data exposure events means claim costs extend far beyond initial incident response.

Stress-test vendor dependencies.
With vendor-related disruption still delivering multi-million-dollar losses, organizations must model cascading failures through their supplier networks. Attacks like that on education SaaS provider PowerSchool and the 2024 breakdown of the automotive supply chain brought about by attacks on CDK demonstrate how vendors you may not consider “crown jewels” nonetheless have the ability to cause large-scale business interruption.

Integrate cyber with operational resilience.
The shift to extortion-only attacks means cyber incidents increasingly manifest as business disruption rather than IT problems. Cyber risk belongs in enterprise risk frameworks alongside supply chain, regulatory, and operational risks, not siloed in information security.

FOR CISOS

Prioritize prevention over recovery.
With 65% of extortion attacks skipping encryption entirely, backup strategies no longer address the primary threat. Invest in data loss prevention systems, zero trust architecture, and phishing-resistant authentication. The battle has shifted from "how fast can we restore" to "can we prevent exfiltration."

Deploy credential monitoring as an early warning system.
The majority of ransomware victims show evidence of infostealers in their logs before an attack. Implement continuous dark web monitoring for compromised credentials, assume breach when employee credentials surface, and rotate session tokens immediately. Organizations that treated infostealer detection as critical security events contained incidents before they escalated to material losses.

Build vendor incident response into your security program.
Vendor-related incidents still generated $1.36 million average severity when they occurred. Your security controls stop at your network perimeter, but your business interruption risk extends through your entire vendor ecosystem. Develop contingency plans for critical vendor failures and ensure your incident response playbook includes vendor-originated scenarios, not just direct breaches.

Case Studies

High-severity vendor interruption: When third-party risk becomes business interruption

In 2025, a large-scale retail operation experienced the cascading impact of third-party cyber risk when one of its primary logistics vendors was paralyzed by a ransomware attack. The vendor compromise caused immediate collapse of the retailer's distribution and logistical operations, demonstrating how vendor incidents manifest as direct business interruption for dependent organizations.

Resilience provided immediate policy guidance and crisis communication support while arranging an interim payment to stabilize the insured's cash flow during the disruption. Direct incident response costs were a fraction of the total claim—business interruption losses exceeded them by more than fifty times, illustrating why retail emerged as a high-severity outlier in 2025.

KEY LESSONS

Vendor-related losses declined overall in 2025, but when they occur, they create operational disruption that dramatically exceeds response costs. Organizations must model cascading supply chain failures, not just direct breach expenses. Business interruption coverage becomes critical when vendors control operational dependencies.

Large-scale data exfiltration: The cost of healthcare breaches

A major healthcare chain processing hundreds of thousands of personal records suffered a ransomware attack after an unpatched server was relocated within their network. While acute services continued, the organization was forced to cancel routine treatments and manage a massive data exfiltration event.

Resilience coordinated with forensic specialists and privacy counsel to navigate complex regulatory review with the Information Commissioner's Office. The claim ran into the millions, with nearly two-thirds of total losses dedicated to legal costs and comprehensive data review—not technical recovery.

KEY LESSONS

Healthcare's consistently high average severity reflects the extraordinary legal and regulatory costs that follow data-heavy breaches in this sector. Even when operational recovery proceeds relatively quickly, the regulatory notification requirements, forensic investigation to determine scope of exposure, and legal defense create costs that far exceed technical response. This case illustrates why extortion-only attacks focused on data theft create leverage that backups cannot address.

Proactive risk management: Reducing extreme loss exposure by $10.4M

A diversified holding company managing multiple subsidiaries faced a common challenge: each subsidiary operated with its own IT team, policies, and controls. While this decentralized approach supported business autonomy, it created blind spots for the parent organization's risk manager, who needed consistent cyber risk oversight across the portfolio to reduce systemic exposure.

The company's static, spreadsheet-based risk assessments offered only snapshots in time, making it difficult to compare exposures or align security priorities across subsidiaries. Without continuous visibility into each entity's risk profile, the parent company struggled to guide investments strategically and lacked the quantified data needed for portfolio-wide planning.

Resilience deployed its continuous risk assessment platform to give each subsidiary tailored, quantified modeling through Loss Exceedance Curves and Cyber Action Plans. Each subsidiary received financial insights based on its unique threats and controls, ensuring security investments were prioritized where they would deliver the greatest risk reduction. The parent company gained centralized visibility through portfolio-wide dashboards while maintaining subsidiary autonomy through shared governance frameworks and quarterly alignment meetings.

The results demonstrated the value of continuous, quantified risk assessment: the company reduced potential extreme loss by $10.4 million in 2025 by implementing controls across three portfolio companies based on Cyber Action Plan recommendations. The portfolio maintained 97–100% risk profile completion, enabling consistent, data-driven visibility to guide both subsidiary security teams and parent-level investment decisions.

KEY LESSONS

Static risk assessments create gaps in understanding across complex organizational structures. Continuous risk assessment with quantified financial modeling enables both operational autonomy and strategic alignment. Organizations that implemented controls based on quantified risk reduction potential achieved measurable decreases in extreme loss exposure. Portfolio-wide visibility doesn't require centralized control—it requires consistent measurement and shared frameworks.

Appendices

Methodology

The data and insights presented in this report are derived from Resilience's internal insurance claims portfolio and threat research conducted by our Risk Operations Center. Our analysis covers claims reported and processed during the full year 2025, with comparative data from 2024 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) to provide a comprehensive view of the cyber risk landscape.

Data sources include Resilience's claims portfolio (827 total claims, 43 incurred claims in 2025), Risk Operations Center threat intelligence, internal security research, and external threat data where specifically cited.

Definitions

The following terms are used to establish the analytical framework for this report. These descriptions are for informational purposes and do not replace, modify, or supersede the legal definitions or conditions found in any insurance policy.

Ransomware

Malware designed to encrypt an organization's resources and deny access until a ransom is paid for a decryption key.

Cyber extortion

A broader category encompassing all events where a threat actor threatens a victim to pressure ransom payment, including data theft for suppression, encryption for decryption, psychological warfare, DDoS attacks, supply chain threats, and deepfakes or false whistleblowers.

Extortion-only

Data theft and extortion threat without deploying encryption, rendering backups ineffective against the primary threat.

Incurred claim

A claim notice that resulted in or is expected to result in a non-zero dollar loss.

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 led to financial losses, such as ransomware, business email compromise, or data breaches.

Limitations

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 2025 data due to the time required for complete loss development and reporting. Claims can remain open for 2-3 years as litigation, forensic accounting, and regulatory proceedings progress.

This document is based on internal benchmarking, client-reported outcomes, and qualitative insights from industry practitioners. The figures are illustrative and directional in nature and may vary depending on an organization’s structure, maturity, and existing processes. Financial figures are generally presented in USD based on exchange rate valuations at the time of reporting. This document is for informational purposes only and is not an offer to sell or purchase insurance. Resilience’s software solutions, including Arc and Edge, are offered separately from any insurance product and their use does not imply or guarantee insurance coverage, terms, or eligibility.

See the latest trends and analysis in cyber claims