

→ CyberResilience.com

r



Midyear 2024 Cyber Risk Report

Cyber Claims Trends and Analysis

resilience

Table of Contents

03 The Evolution of Third Party Risk

07 2023/24 Claims Trends

Vendor Risk Sends Ripples Through the Industry

Losses lead by Ransomware & BEC, again

Big Game Hunting is Growing in Ransomware

Point of Failure Analysis

Industry Focus

17 Case Studies

The Change Healthcare Hack

CDK Attack Deals a Blow to Car Dealerships

The PanOS Bug

21 The Resilience Difference

INTRODUCTION

The Evolution of Third Party Risk

Cyber threats continued to intensify in the first half of 2024 as cybercriminals exploited security gaps from growing business and technological consolidation. Increasing merger and acquisition (M&A) activity, coupled with reliance on ubiquitous software vendors created new opportunities for threat actors to unleash widespread ransomware campaigns —all by taking advantage of heightened third-party risk and deep industry interdependency.

High-profile cyber incidents like Change Healthcare and CDK Global illustrated that an attack on a heavily interconnected system can have devastating, long-lasting effects downstream —even to the point of putting an entire economic system on hold. The CrowdStrike outage in July 2024 was not itself the result of a cyberattack, but it serves as a stark reminder of the fragility and risk in the technology ecosystem.

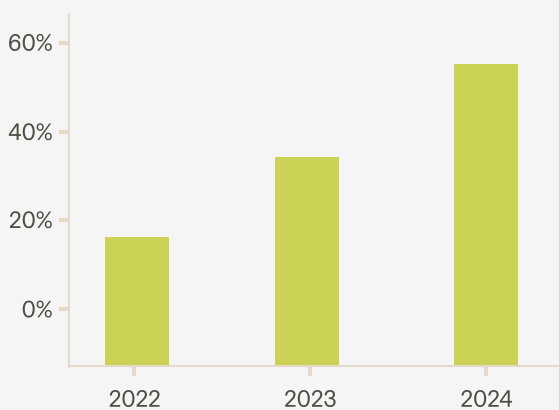
In tracking data from our threat research team and insurance claims portfolio, Resilience has identified several key ways in which the risk landscape has shifted over the past year.

Key Findings

1 Business and technology consolidation have injected new third-party risk.

Rebounding M&A activity and increasing technology consolidation—in which industries rely on single suppliers for critical platform services—both created a staggering number of potential new points of failure for hackers to exploit. Some of the past year’s most devastating cyber incidents involved heavily interconnected systems or recently acquired companies. Vendor-driven claims are the fastest-growing area of claims in our portfolio, and are now the fastest growing cause of loss for claims overall. 35% percent of claims originated in a vendor failure in 2023, and in 2024 that number is already 40% and expected to grow. Exploiting these two kinds of third-party vulnerabilities is the latest method of “big game hunting,” which we first observed in our [2023 Midyear Claims Report](#). No matter how effectively a company defends its own digital environment, businesses are interconnected and interdependent on the cyber resilience of others.

Vendor Driven Cause of Loss as a Percent of all Claims



48% of all Resilience portfolio claims were related to ransomware in 2023

64% of ransomware related events led to a covered loss

411% increase in the severity of loss for ransomware claims over 2022



2 Ransomware drives yet more losses, higher spending on recovery.

Ransomware remained the leading cause of loss in Resilience’s portfolio since January 2023, with 64% of ransomware-related claims resulting in a loss. After a steep drop in 2022, research from [Chainalysis](#) shows that ransomware payments rebounded to \$1.1B in 2023 with median extortion payments in more than 60% of ransoms and fees exceeding \$1m. The severity of ransomware claims in the Resilience portfolio also went up dramatically from 2022 to 2023 with a 411% jump in the financial severity of events. However, Resilience clients losses did not always result from paying extortion fees; fewer than 10% of clients paid extortion fees, the remainder opting to recover without paying a ransom. This reflects a trend toward increasing costs to recover from ransomware attacks regardless of whether an extortion is paid.

“While cybersecurity has historically been considered as a line item in a company’s budget, it’s clear that this is insufficient. Business leaders must adopt a risk-centric approach—one in which security strategies are grounded in the financial translation of cyber threats.”



Tom Egglestone
Global Head of Claims, Resilience

3 Humans are still the weakest link.

Many of the most notable and destructive cyber incidents this year have human error at their core. This is perhaps unsurprising when we consider that cyber risk is an inherently human-engineered risk. Phishing leads Resilience’s list of points of failure for incurred claims* again this year; these failures most often resulted in the deployment of ransomware or email compromise. M&A activity can amplify cyber risks for an enterprise not only from its own existing vulnerabilities, but also the new risks associated with the acquisition target and the challenges of integrating different IT systems post-acquisition.

[Change Healthcare Case Study→](#)

Understanding these changes in cyber criminals’ strategies, and where potential vulnerabilities lie, can help organizations better prepare for and mitigate the effects of attacks. By adopting a risk-centric approach, Resilience customers minimized material losses and avoided business disruption.

Cyber resilience is no longer a nice-to-have; it is a business imperative. While cybersecurity has historically been considered as a budget line item, the past year has confirmed this is no longer sufficient. Cyber risk management must be elevated to the board level as a strategic business decision to reach growth goals while remaining resilient to material losses. M&A deals must be deeply scrutinized for emerging vulnerabilities, and security strategies must be grounded in the financial translation of cyber threats.

The **2024 Midyear Risk Report** unpacks this new reality—and what enterprises can do about it.

*Incurred claims are claims for which payments have been made or case reserves have been set.

A Financially Driven Approach

Our team of cybersecurity and insurance experts bring decades of experience in **underwriting and claims,** **data analysis,** **threat hunting,** **& cybersecurity** to help protect our clients more effectively.

Where most insurers focus on minimizing losses after a cyber event, the **Resilience Risk Operations Center** proactively identifies exposure to vulnerabilities to prevent them from harming our clients.



from the Resilience
Risk Operations Center

The Ivanti logo, featuring the word 'ivanti' in a white, lowercase, sans-serif font on a dark blue background.

ivanti

Resilience identified clients affected by vulnerabilities in Ivanti products and mitigated risks, alerting dozens of clients, averting the potential for tens or in the worst case hundreds of million in claims.

The ScreenConnect logo, featuring the text 'CONNECTWISE' in small letters above 'ScreenConnect' in a larger, white, sans-serif font on a dark blue background.

CONNECTWISE
ScreenConnect

Rapid response to ScreenConnect vulnerabilities prevented potential network breaches for dozens of clients, again averting potential claims estimated in tens to hundreds of millions of dollars in potential impact.

A large white percentage '98%' on a dark blue background, representing the success rate of Edge Solution clients.

98%

Since 2022, 98% of Edge Solution clients with primary policies through Resilience have avoided any incurred costs for claims.

2023/24 Claims Trends

The frequency of attacks has picked up slightly in the first half of 2024, with an increase of 2.2% in total claims from the first half of 2023 versus 2024. If the trend continues, we expect to see an increase in claims in 2024. Incurred claims as a percentage of overall claims is down a half a percent in the first half of 2024 compared to first half of 2023.

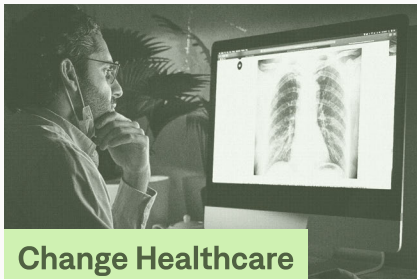
Vendor-related risks shows up in two important ways in 2024. The first is in the form of third-party risk from partners or suppliers that come under attack. The second, highlighted by the CrowdStrike outage in July, is risk from outages of important suppliers in a company's technology stack.

Vendor Risk Sends Ripples Through Industries

Two of the top three events are the result of ransomware attacks directly on clients or on the vendors of clients, while an exploited vulnerability in Palo Alto Networks OS led to the third most claims. The full impact of each of these recent incidents will take some time to tell, but here is what we do already know.

Top events that resulted in a claim in H1 2024 were:

Click on a case study event to read more about how these issues affected businesses.



Change Healthcare

This recently acquired subsidiary of healthcare giant United Healthcare was hit with a ransom attack that halted healthcare payments and approvals for week.



CDK Ransom Event

A previously unheard of lynchpin in the automotive industry was hit with a ransomware event that left car dealerships unable to transact during May and June.



PanOS CVE

A vulnerability with the potential to provide cyber criminals with unfettered network access was actively exploited in security stalwart Palo Alto Networks in April.

As we issue this report, the fallout from several major ransomware events at Change Healthcare, CDK and others have yet to be fully measured and could change our understanding The severity of these events.

While ransomware often takes the spotlight, several other causes of loss play significant roles in incurred claims in our portfolio.

↗ **411%**

The severity of ransomware attacks has increased as criminals have continued to pursue larger ransoms. According to claims made to Resilience, **severity of ransomware events is up 411% in 2023 as compared to 2022.**

↘ **80%**

In 2023 and the first half of 2024, ransomware attacks accounted for roughly half the claims made to Resilience, but they comprised slightly **more than 80% of the losses sustained in our portfolio** over the last 18 months.

Healthcare and **manufacturing** were the most affected in the 1H of 2024, but other areas of critical infrastructure, such as **energy,** **construction,** & **engineering** were subject to increased attacks.

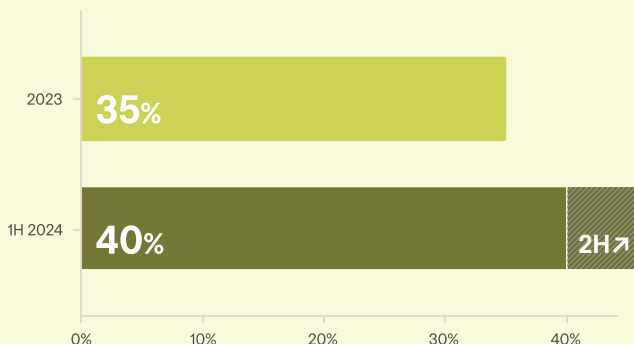
9.7%

9.7% of Resilience-insured ransomware victims paid extortion fees in 2023-24 versus an estimated 37% in 2023 across all sectors according to Coveware.

6%

Software vulnerabilities accounted for only **6% of total claims but 15% of losses with a significant jump in severity**; between 2022 and 2023.

Rising Vendor-Related Claims in '23-'24



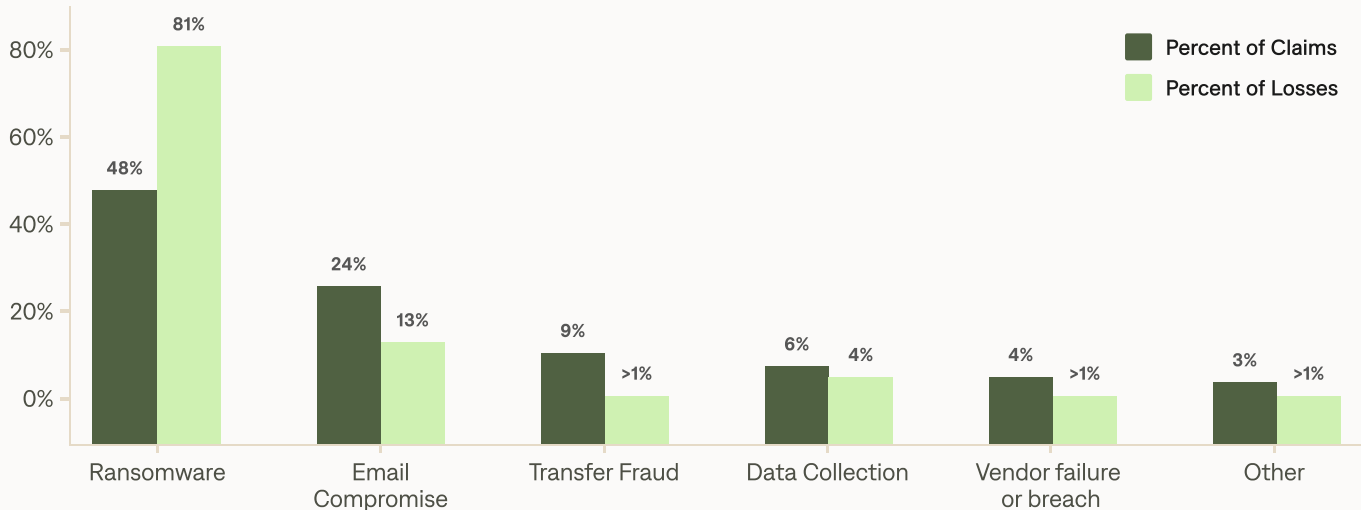
35% of claims in 2023, & 40% in the 1H of 2024,

are related to vendor failure of some kind – data breach, ransomware attack, or error-driven outages. **That number is already ticking higher in the second half of 2024.**

Losses lead by Ransomware & BEC, again

The cause of loss refers to what kinds of attacks led to material losses in our client portfolio. It is distinct from the point of failure which describes what the bad actor exploited in order to cause the losses. To be sure, in 2023, we saw the usual suspects. Ransomware, data breaches, and transfer fraud/business email compromise are the stalwarts of the last several years of cyber crime.

2023 Cause of Loss



We discuss ransomware trends at some length later in this report, but it’s worth noting the other major loss drivers in cyber events in 2023.

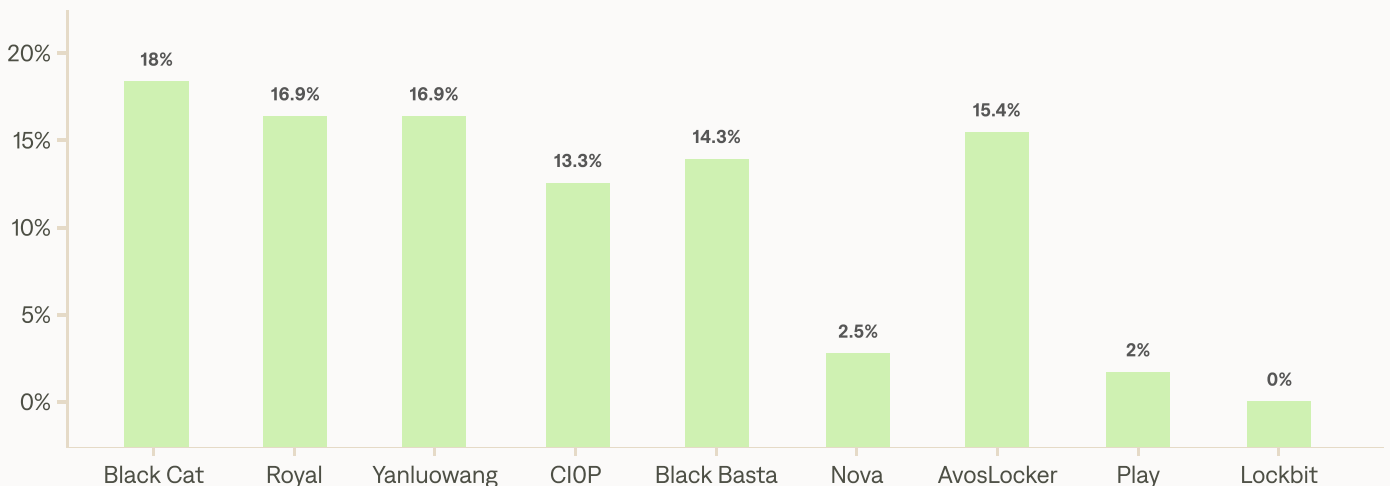
Business Email Compromise (BEC) can look as though it fell in prominence in 2023 and 2024, but that is only because ransomware gets so much media attention. BEC attacks have remained fairly steady at between 13% -15% as a cause of loss on claims between 2022 and 2024. A larger proportion of those claims became material in 2023 jumping 11% over 2022; data on 2024 is too undeveloped to report, of the large losses ransomware is causing. In fact, BEC attacks are becoming three times more frequent and are more than doubling in severity among our portfolio.

Data collection issues resulted mainly from an issue with pixel trackers used to track website and visitor analytics sending data to third parties against data collection laws. This drove higher than usual losses in that category for clients, a departure from years past and likely not part of a lasting trend.

Big Game Hunting is Growing in Ransomware

When companies are hit with ransomware, the severity of the attack can depend on the tactics of the particular group. Losses from ransomware claims might reflect extortion fees, recovery costs, crisis management costs, and other losses stemming from a ransomware attack and may not reflect the full measure of losses to the client. Our claims data shows that several ransomware groups had significant impacts in 2023.

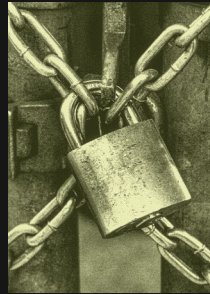
2023 Share of Portfolio Losses by Ransomware Group



But what does this tell us about which ransomware groups are winning? While fewer than 10% of Resilience clients who were directly affected by ransomware paid an extortion fee in 2023, Black Basta carried out the most attacks that led to the payment of an extortion fee among Resilience clients affected by ransomware. While Lockbit is still a relative heavyweight in the overall ransomware market, no Resilience client has yet paid an extortion fee to the group. For companies that paid an extortion fee, more than half were compromised via a software vulnerability. Clients unable to restore systems from their backups were more likely to pay extortion. While backups aren't a failsafe, a properly segregated and tested set of backups are probably the biggest mitigation against paying ransoms.

Rogues Gallery

We saw many ransomware groups active in our portfolio in the last 18 months. Here are some of the worst:



CIOP

This gang targets systems with inadequate security and encrypts files. CIOP's mass exploit of the MOVEit file transfer software impacted more than 2,000 organizations.

Though they are associated with the most claims in our portfolio, this group has not been as successful at extorting ransoms from our clients.



BlackCat

BlackCat is leading in frequency and severity of attacks in 2023-24.

Known for a "triple extortion" model. In February 2024, after an attack against Change Healthcare, BlackCat's operators shut down their dark web site in what is widely believed to be an 'exit scam' keeping the payment from the affiliate that conducted the attack.

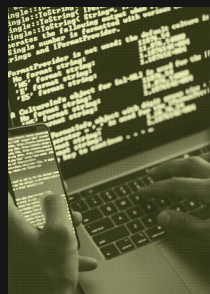


Royal

We didn't see much Royal, but when we did, it caused above-average losses per incident in our portfolio.

Since September 2022, Royal has targeted more than 350 known victims worldwide and ransomware demands have exceeded \$275 million.

(source: CISA)



Black Basta

Believed to be a Conti splinter group, Black Basta affiliates are known for targeted double extortion tactics—they both encrypt and exfiltrate data, charging for decryption and non-release of held information.

Healthcare organizations have been a high-value target for Black Basta affiliates, with high-profile attacks against Ascension and Synlab, Italia in 2024.

(Source: Barracuda Blog)

Based on [Chainalysis](#) the median payment size for ransomware has surged with more than 60% of ransoms exceeding \$1m. Their data also suggests that Lockbit, Black Basta, Royal, and BlackCat were frequently paid their ransom with Black Basta, Royal, and BlackCat having some of the largest median payment amounts. CIOP and BlackSUIT were more targeted in their attacking (some big game hunting here) netting a larger median payment amount. Lockbit seems to have more frequent smaller median payments.

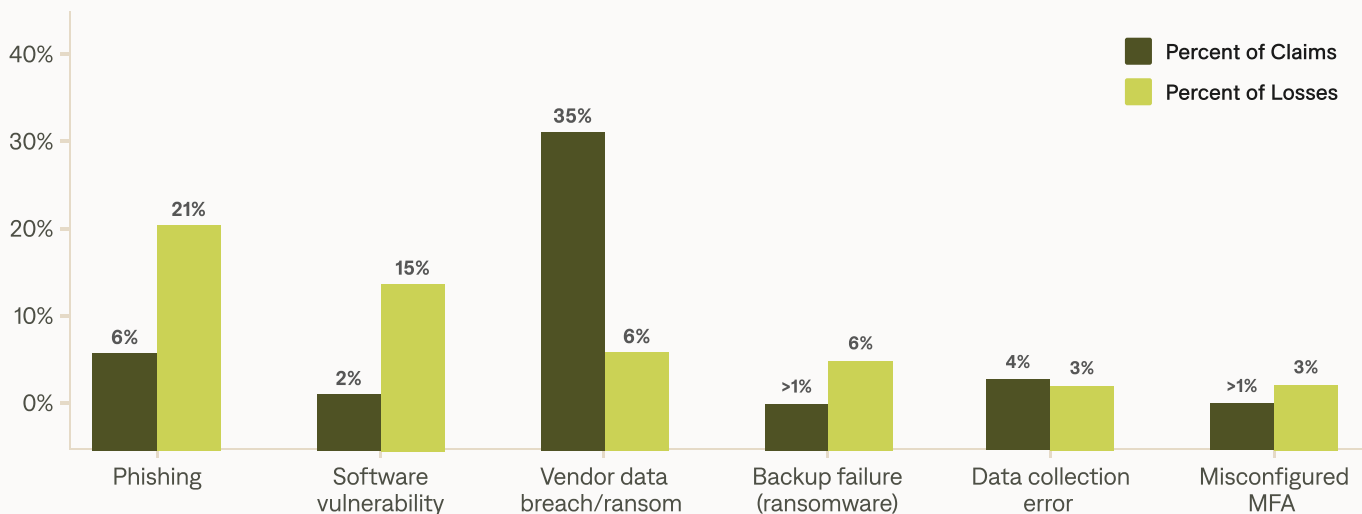
Points of Failure Analysis

An unpleasant fact is humans are the most likely point of failure in cybersecurity. It is time to point fingers. And yes, you're the problem, it's you.

Phishing leads our list of points of failure for incurred claims yet again this year proving that even a server with open file transfer protocol is safer than thousands of employees eagerly clicking away. Twenty-one percent of claims in 2023 involved reports of phishing as a point of failure. Those failures resulted most often in the deployment of ransomware or email compromise.

Software vulnerabilities, while only comprising 2% of claims in 2023, made up 15% of losses in our portfolio. These vulnerabilities were most often exploited using ransomware. Vulnerability management is the cornerstone of any security program, but leaner security teams may struggle to determine how to prioritize patching. Resilience works with clients to understand what they are running in their environments and is able to notify clients who might be affected by a new critical vulnerability.

Point of Failure for Claims, 2023



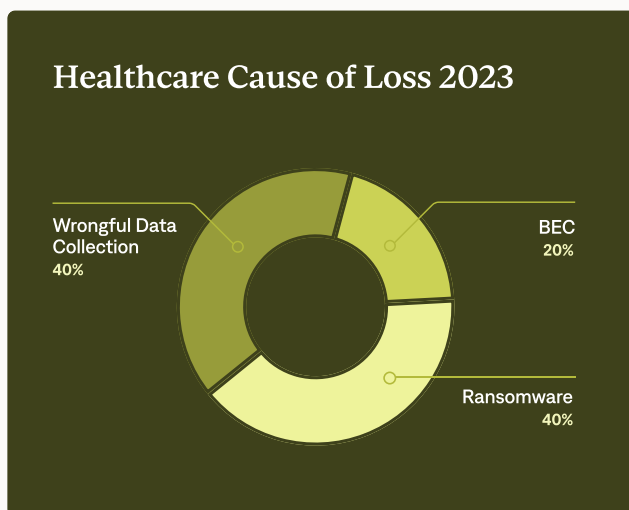
Employees and system users are not the only problem. So are your organization's vendors.

Thirty-five percent of all claims in 2023 were reported due to a vendor data breach or a vendor suffering a ransomware attack. In 2023 and so far in 2024, those claims have not resulted in material losses at the same rate as direct attacks, however, they are so far responsible for more than 5% of losses in our portfolio in 2023.

Industry Focus

In 2023, wholesale companies bore the brunt of cyber attacks. On a per-claim basis, 18% of incurred claims in our portfolio occurred at companies in this sector, with two-thirds of incurred claims relating to ransomware and a third to business email compromise.

Commonly held wisdom suggests that outside of nation state cyber activity, most threat actors are not intent on targeting a specific industry, but rather on targets that both lack controls and have significant value at risk. Wholesale companies may have experienced a higher level of ransomware due to the industry's late digital transformation as well as the distributed wholesale supply chain which presents a rich attack surface.



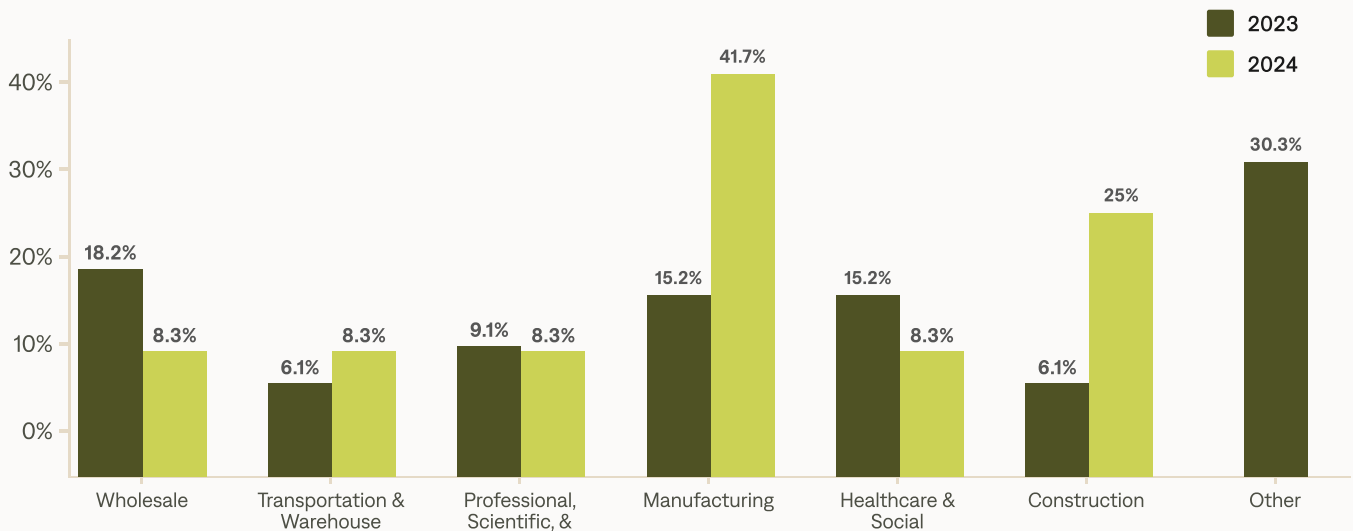
There was a slight increase of attacks in the healthcare sector in Q1 2024 compared to 2023 as ransomware groups such as BlackCat abandoned their “rules” to not target healthcare at the end of 2023; we can expect other ransomware groups to do the same, leading to a significant increase in healthcare attacks in 2024.

Healthcare was the second most affected industry. The losses in the sector in 2023 stemmed from ransomware (40%), BEC (20%), and wrongful data collection (40%). The wrongful data collection is unique to an issue involving wrongful data collection from marketing pixels mistakenly collecting information on healthcare sites. Manufacturing rounded out the top three industries affected in the Resilience portfolio in 2023. Manufacturing firms were hit by a wide range of attacks from malware to insider data breach, but like other industries, ransomware attacks led to the greatest losses.

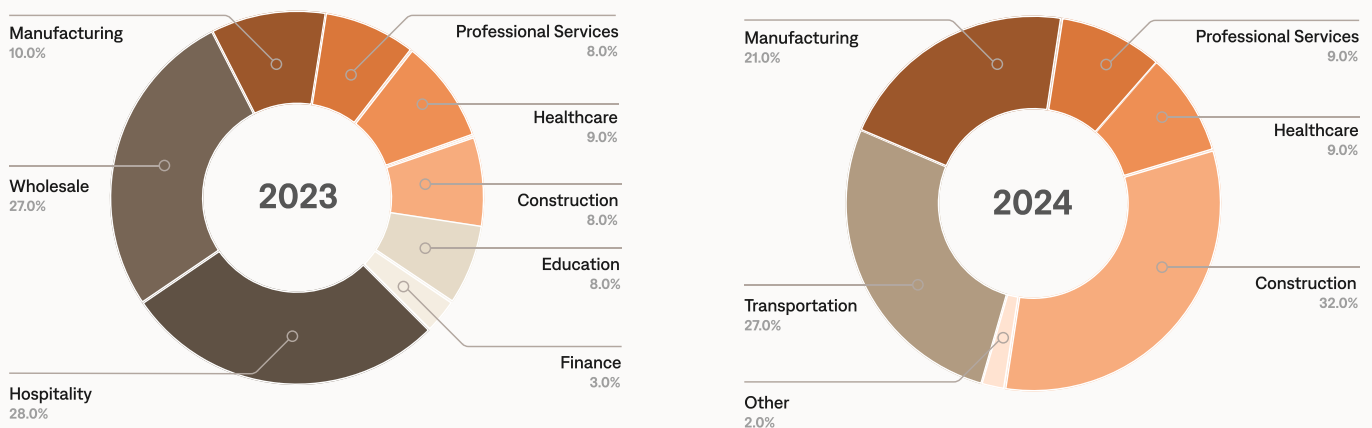
In 2024, claims within the manufacturing and construction space are on the rise, which tracks with industry data on attacks provided by our threat-hunting team. We can explain the growth in automotive attacks largely on the CDK Global issue from June, but construction warrants a close look. According to [SANS institute](#), attacks on construction was one of the fastest growing sectors for attacks in 2023. The growth of attacks throughout 2023 has escalated in 2024.

Like other highly targeted sectors, construction has lagged in digital transformation, and also on many systems and subcontractors access the same temporary networks on construction sites. Additionally, networks may be established without following security best practices in the push to start new projects. This can lead to a more permeable attack surface and a greater tolerance for anomalies.

Portfolio claims by industry (2023 vs. H1 2024)

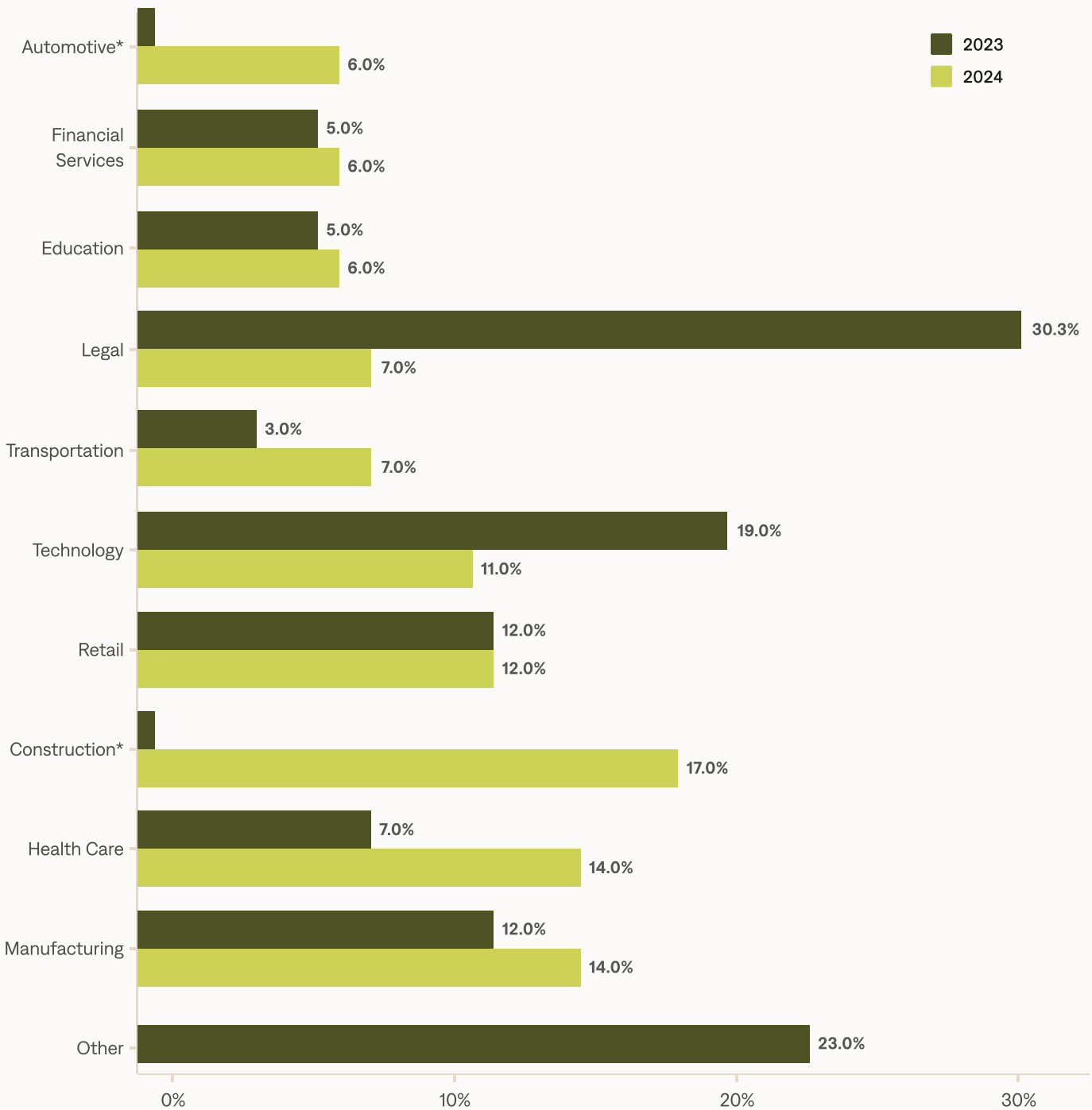


Resilience Portfolio Industries Affected by Ransomware (2023 vs H1 2024)



* Resilience has not recorded ransomware claims in the education, hospitality, and wholesale sectors thus far in 2024.

Global Ransomware Attacks by Industry (2023 vs. H1 2024)



* Construction and automotive claims are included in "Other" in 2023

YOUR RISK IS OUR RISK

Case Studies

This year's case studies illustrate the importance of understanding risks from other organizations. Change Healthcare shows the importance of cyber due diligence and cyber risk management during a merger or acquisition and its integration. The CDK Global hack and PanOS bug show how an attack on a trusted resource can impact entire industries.

The Change Healthcare Hack

Change Healthcare is one of the largest health payment processing companies in the world. It acts as a clearing house for 15 billion medical claims each year—accounting for nearly 40 percent of all claims in the United States. It was acquired by UnitedHealthcare in late 2022. In February of 2024 Change Healthcare came under attack by the notorious ALPHV/BlackCat group. Suddenly, the firm was unable to make payments or pre-approve treatment, creating serious issues for doctors, hospitals, and patients. Delays in medical payment threatened patient access to healthcare. The attack resulted in the theft of 6TB of data and the firm paid a \$22M ransom.

UnitedHealthcare is predicted to be saddled with up to \$1.6 billion in costs closely on the heels of acquiring Change Healthcare. It will take some time still to understand the impact to downstream healthcare companies that rely upon Change Healthcare.

Vendor-related risk is the fastest growing area of claims in our portfolio highlighting how the fragility of our technology ecosystem sometimes has outsized effects on its customers, and customer's customers.



The Change Healthcare hack illustrates the vulnerability that organizations are exposed to during the M&A process. Having recently acquired the processor, United Healthcare assumed the risk from a cyber incident without the opportunity to fully assess their cyber risk. While many companies conduct some sort of cyber due diligence on the intended acquisition target, the process is not guaranteed to protect the company from risk, just to help highlight where it exists.

The attack's impact landed UnitedHealthcare's CEO in front of Congress. During the hearing, the CEO admitted the organization did not use MFA on the system that was compromised in the attack. Later testimony revealed that Change Healthcare had appointed a CISO who lacked cyber risk credentials, one of many oversights that have led a Senator to call for enforcement action hold the CEO and board of directors responsible for "failure to use appropriate information security practices to protect consumers' personal information." (The Record).

CDK Attack Deals a Blow to Car Dealerships



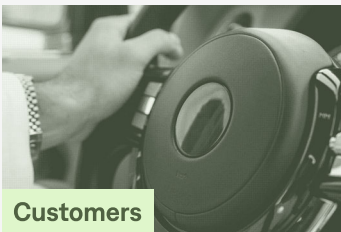
Car Dealerships

Reported disruptions, including an inability to access dealer management systems, difficulties tracking and ordering vehicle parts as well as new sales and offering financing.



Automakers

Dealer operations were directly impacted. Automakers were unable to track sales and inventory through their dealer networks.



Customers

Dealerships were unable to help customers complete purchases, or provide parts and servicing.

Approximately 15,000 car dealers across the US use CDK software to help dealerships manage daily operations, vehicle financing, insurance and repairs.

In June 2024, CDK was infected by ransomware, paralyzing and taking many of its systems offline. It is believed the attack was carried out by BlackSuit, a relatively new ransomware group that first emerged in April 2023.

Sales ground to a halt as dealers scrambled to sell cars by reverting to spreadsheets and paper contracts.

CDK has restored services and says the car dealerships are now up and running. However, thousands of companies were affected, and the ultimate costs and losses due to the CDK attack are yet to be fully determined. According to JD Power & Associates and GlobalData, new vehicle sales in the U.S. are projected to fall in June from a year ago, hurt by the cyberattack.

“

Vendor risk is one of the key topics we discuss with our insureds. Our team has drafted specific guidance to manage this risk, available to all our customers via our portal.



Amanda Bevilacqua
US Claims Operations Leader, Resilience

The PanOS Bug

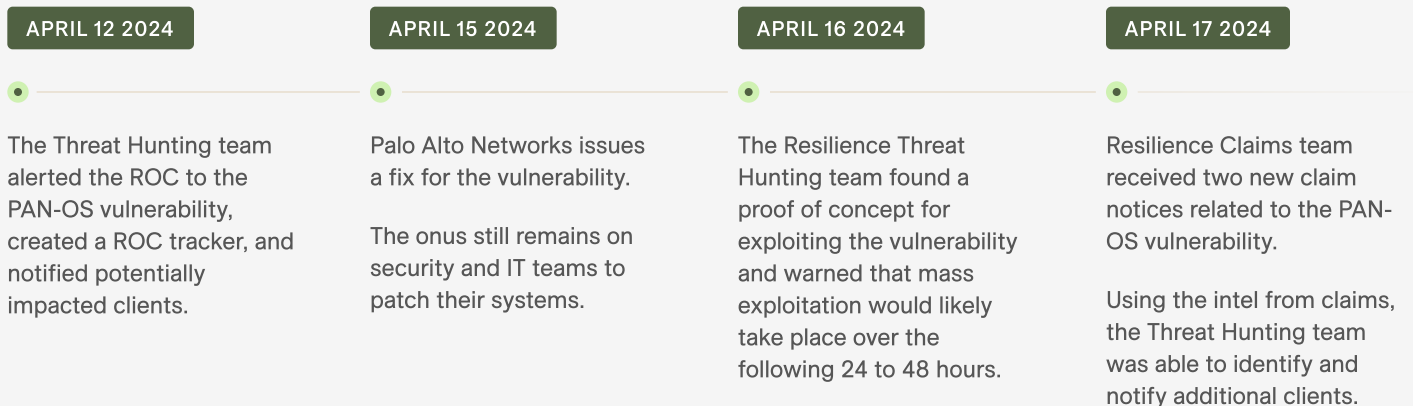
On April 11, Palo Alto Networks warned that threat actors were actively exploiting a zero-day vulnerability in PAN-OS Global Protect VPNs. The vulnerability was deemed a severity of ten or critical. The vulnerability hinged on whether a feature called “Global Protect” was enabled or not. Threat actors can exploit this vulnerability to gain arbitrary code execution with root privileges. In other words, fully control and movement on the affected network. Our threat-hunting team identified many customers with Global Protect enabled and notified them directly that they were at risk.

A patch for this vulnerability was released April 15, and Resilience continued to notify clients that a proof of concept had been posted for exploiting the vulnerability making it more likely to be exploited. Out of caution, the team also issued a

warning to all users of the product. Some clients reported potential signs of exploitation. They notified our team that they had been affected, and we used the information to tune our search and reveal several more clients who were at high risk. In the end, only 2% of potentially impacted clients reported being affected.

Resilience’s teams of security experts, threat hunters, and claims specialists worked to understand what clients were impacted directly and to reach out to them with targeted alerts. Each alert is reviewed by one of our specialists to ensure it is relevant to that client. Because our teams work closely on key incidents, they can enrich each other’s response process as the incident develops. This is one way we help you stay a step ahead of cyber criminals.

Timeline of PanOS Bug Incident



SPOTLIGHT

The Resilience Difference

Our team of cyber insurance experts, data scientists, and cyber security professionals provides a multi-disciplined approach that brings a higher level of diligence to cyber resilience. For our clients, it means being able to conduct their business with confidence. To our partners, brokers, and insurers, our team's total dedication and proven expertise is building long-term enduring relationships based on transparency, excellence, grit, and most of all... trust.

THE RESILIENCE SOLUTION

Most Effective Loss Prevention Solution



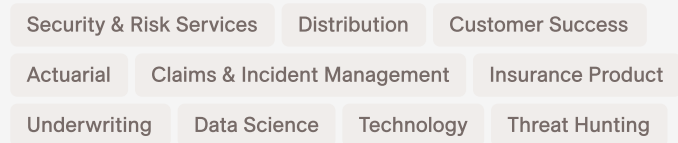
Backed by A+ Global Insurers

We've earned the trust of Intact Financial Group in North America, along with HDI Speciality Global and RSA in the UK & Europe, offering up to \$10M of cyber limit available per risk on a primary or excess basis.



In-house and Integrated Expertise

Our Insurance and Security teams handling every aspect of cyber resilience - Managed with seamless command, control and integration.



Best in Class Technical Cyber Underwriters

Our seasoned underwriters, with decades of experience in cyber and broader insurance industries, have helped protect our clients more effectively, resulting in a 12.9% blended incurred loss ratio over the last three years.



Priority Incident Management & Claims Handling

We provide clients with 24/7 in-house claims and incident management. Our experts have decades of experience handling the complex details of a cyber claim.



Cybersecurity Loss Prevention Specialists

Our 1:1 underwriter-to-cybersecurity expert ratio and advanced risk quantification models drive a 90% client renewal rate for our integrated cyber risk solution. Our Human-in-the-Loop partnership improves cyber hygiene throughout the policy term.



Global and Diversified Client Presence

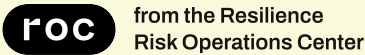
We work with clients with revenues up to \$10B and service them through our local presence in the US, Canada, UK, Spain, Ireland, Italy, Benelux and the Nordics and continue to expand our footprint.

“Many carriers and MGAs solely focus on selecting the best risks for their portfolio. We go beyond portfolio risk management to the individual account level to help enterprises become cyber resilient. Together with our partners, *our focus is to drive better outcomes for our policyholders and business partners – and this recognition from our industry peers reflects our passion and dedication.*”



Mario Vitale
President, Resilience




A precise approach to remediating threats

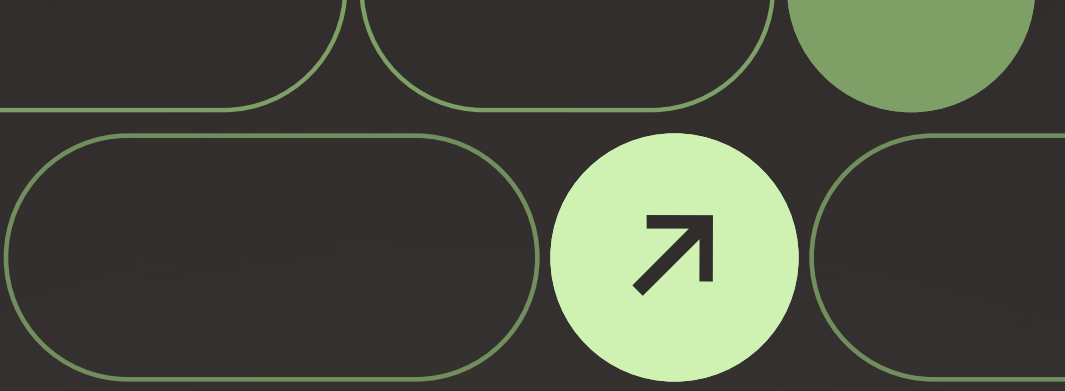


The Resilience Risk Operations Center (ROC) is a command center, a think tank, and a fighting force dedicated to cutting through the noise and helping clients proactively and precisely remediate the most financially damaging threats.

The ROC embodies a multidisciplinary team of, data scientists, claims and incident managers, cyber security experts, and insurance underwriters—all collaborating and corroborating threat information in real time. The result is timely, actionable, and precise information.

The ROC's multi-disciplinary approach includes:

-  **Proactive vulnerability hunting**
that searches for invasive attack behaviors and advanced threats that can bypass even the most cutting-edge security defenses.
-  **Collective intelligence**
that infuses multiple threat intel sources, our claims data, and is tailored to each client's risk profile.
-  **Portfolio insights**
allow us to swiftly identify threats by amplifying threat actor activities from our entire client base.
-  **Rapid action on containment recommendations**
using the most effective remediation insights from multiple sources including first hand knowledge of what worked and what didn't work for our clients.
-  **Financially driven results**
help IT security leaders understand the financial implications of cyber risks and prioritize the highest value threats.



See the latest trends and analysis in cyber claims



This material is provided for informational purposes only. Accordingly, this material should not be viewed as a substitute for guidance and recommendations of a trained professional. Additionally, Arceo Labs, Inc. d/b/a Resilience and its affiliates and subsidiaries (collectively, "Resilience") does not endorse any coverage, systems, processes, or protocols addressed herein. Any references to non-Resilience Web sites are provided solely for convenience, and Resilience disclaims any responsibility with respect to such Websites. To the extent that this material contains any examples, please note that they are for illustrative purposes only. Additionally, examples are not intended to establish any standard of care, to serve as legal advice appropriate for any factual situation, or to provide an acknowledgment that any factual situation is covered by Resilience.