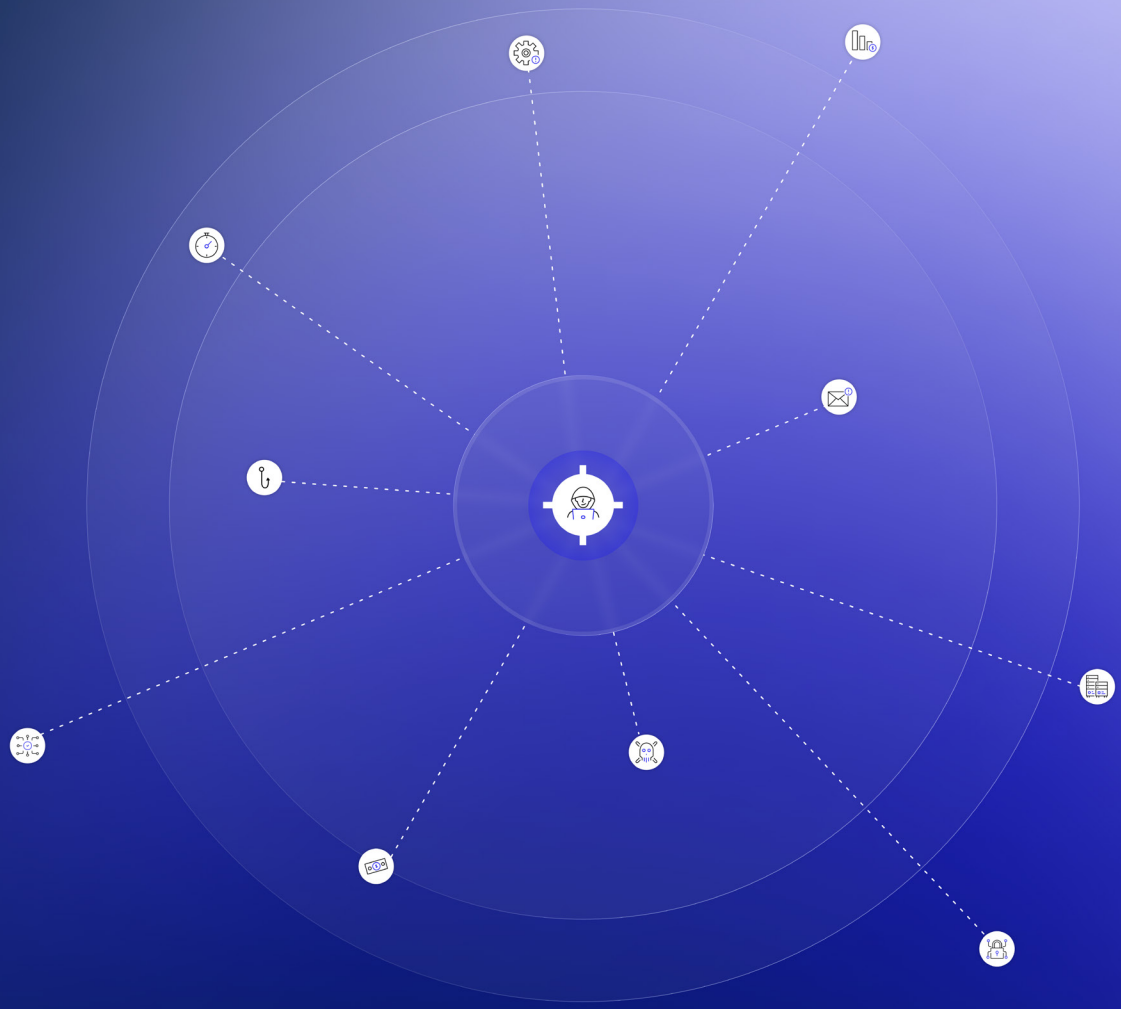


THE 2026

InsurSec Report

at bay

An analysis of At-Bay claims and cybercrime data

Table of Contents

Introduction

For this year's InsurSec Report, we looked beyond the headlines to document and reveal a more complete picture of the impact cyber attacks have on businesses.

In many ways, the story of 2025 appears similar to that of the previous two years: Overall claim frequency and severity continued to climb, both hitting all-time highs. Ransomware and financial fraud (the two most common and costly incident types) saw frequency remain elevated yet stable, while average severity increased significantly. Remote access, particularly VPNs, continued to drive massive risk for businesses.

These are headlines we've understood and shared for several years, but this year we went deeper to better communicate the full cost of a cyber incident, which often extends well beyond what most businesses anticipate when they think about their exposure — and what they can do about it.

For example, one in three ransomware victims suffered from business interruption, and when they did, their average claim severity was 3X higher. A company that survives a ransomware attack without business interruption faces a very different financial outcome than one that spends days or weeks trying to restore operations.

In financial fraud, the average stolen amount grew again, but the more urgent story is what happens after the fraud is reported. Businesses that notified At-Bay within three days recovered at least some of their funds 70% of the time. Beyond that, the likelihood of recovery dropped significantly. What determines the size of the loss, or whether there is a loss at all, is how quickly victims and their insurance partner work together to notify banks and law enforcement.

Third-party liability continues to be a growing concern. Businesses that experience a ransomware attack or data breach increasingly face a second wave of loss in the form of class action lawsuits that arrive long after the underlying incident has been resolved. The costs associated with a cyber incident are not always fully realized at the time of the event, but working with the right partner can make a significant impact on the outcome.

The ransom demand, the stolen funds, the price of rebuilding compromised systems: These are the immediate costs. But business interruption, clawback shortfalls, and class action lawsuits are what increase loss and determine the overall severity of an incident. They are also often the costs influenced by the partners and security readiness a business has in place before an incident occurs.

Beneath the surface, AI is becoming a growing force multiplier for cyber attacks. Increased financial fraud frequency, the accelerating pace of vulnerability exploitation, and direct evidence of AI tools being leveraged by attackers all signal a meaningful shift in the balance of power between attackers and defenders. Generative AI is already lowering the barrier to crafting convincing social engineering lures, enabling more attackers to execute more effective fraud campaigns at greater scale and across language barriers. We fully expect attackers to integrate AI further into their operations in the years ahead, and we are actively tracking this evolution.

We're publishing this report to document the full picture of cyber risk and to show that the right decisions made before an attack can meaningfully affect what happens after one. The findings in this report represent an analysis of more than 100,000 policy years of At-Bay cyber claims data.

Key Findings

Claim frequency increased 7% YoY.

The gains were driven in large part by increases in third-party liability claims, while ransomware and financial fraud remained stable YoY.

Email continued to be the most popular entry vector for attackers.

52% of all claims began with an email attack. Remote access continued to be associated with the highest severity ($433K on average).

Ransomware remained the most damaging incident type, more than twice the overall average.

Average severity for ransomware increased 16% YoY to $508K.

87% of ransomware claims began with the attacker entering through a remote access service.

1 in 3 ransomware claims started with SonicWall.

Akira was responsible for a 53% surge in ransomware claim frequency in H2 2025.

60% of Akira's victims had leading EDR solutions. The only Akira victims that avoided full encryption had a market-leading EDR tool backed by 24/7 monitoring via MDR.

1 in 3 ransomware claims suffered business interruption, and those that did saw 3X higher severity.

The largest single business interruption claim hit $5M, the coverage limit for that insured, but the actual business interruption cost in that case was likely much higher.

Financial fraud continued to be the most common incident, accounting for 30% of all claims.

The average amount of stolen funds ($285K) increased 16% YoY, with the single largest amount stolen hitting $9.7M.

Insureds' vendors and customers accounted for 14% of all claims.

Severity for these claims was $145K on average, a troubling amount considering that the losses occurred without insureds suffering a security failure in their own environments.

Third-party liability saw the highest jump of any incident type, increasing 70% YoY.

This category includes claims related to the California Invasion of Privacy Act (CIPA) and class action lawsuits, driven by an increasingly aggressive plaintiffs' bar.

The Cyber Threat Landscape

CHAPTER

01

Overall Claim Frequency & Severity **Hit Record Highs**

In 2025, cyber risk reached a new high-water mark. Claims frequency increased 7% year-over-year to the highest rate At-Bay has recorded since 2021. This marks the third consecutive year of increase following a brief dip in 2022.

The 2022 decline, which we have previously attributed in part to the disruption of Russia and Ukraine-based cybercriminal groups following the outbreak of the war in Ukraine, now reads clearly as a temporary interruption rather than a legitimate inflection point. By 2023, frequency had recovered past 2021 levels, and the upward trend has continued unabated.

At the same time, average claim severity climbed to an all-time high of $221K. The combination of more incidents and higher costs signals a continuation of the progressive worsening of the cyber threat environment, one defined not by a single dramatic event, but by a broad, sustained expansion of risk across industries, company sizes, and attack types.

FIGURE 1

Overall Claim Frequency Increased 7% in 2025

Indexed Claim Frequency by Year

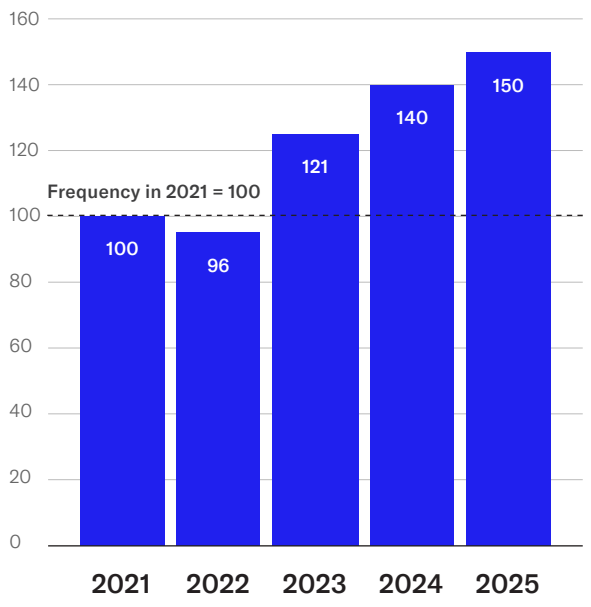
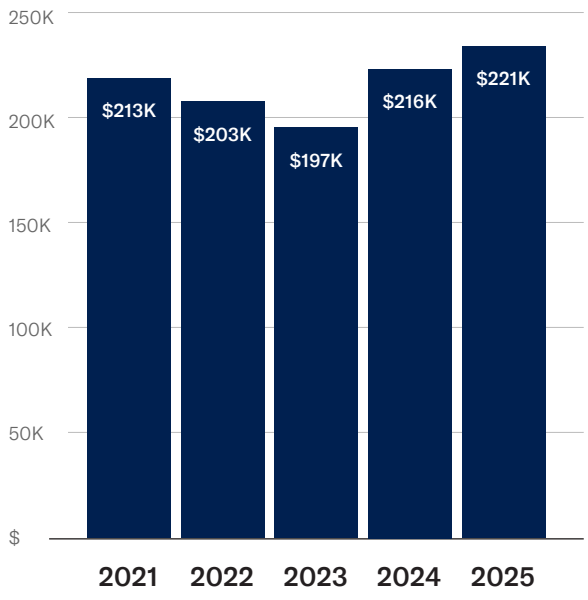


FIGURE 2

Average Severity Climbed to All-Time High of $221K

Average Claim Severity by Year



Claim Frequency and Severity by **Incident Type**

Financial fraud remained the largest category of claims in 2025, accounting for roughly 30% of all incidents for the third consecutive year. The consistency of this figure reflects the enduring effectiveness of email-based fraud tactics, which have only become more potent as generative AI enables attackers to craft more convincing and contextually appropriate messages.

Ransomware continued its recovery from the 2022 trough, with frequency rising again in 2025. The second half of the year was particularly active, driven by a sustained campaign of Akira ransomware attacks exploiting companies operating SonicWall appliances. We cover Akira in depth in Chapter 2.

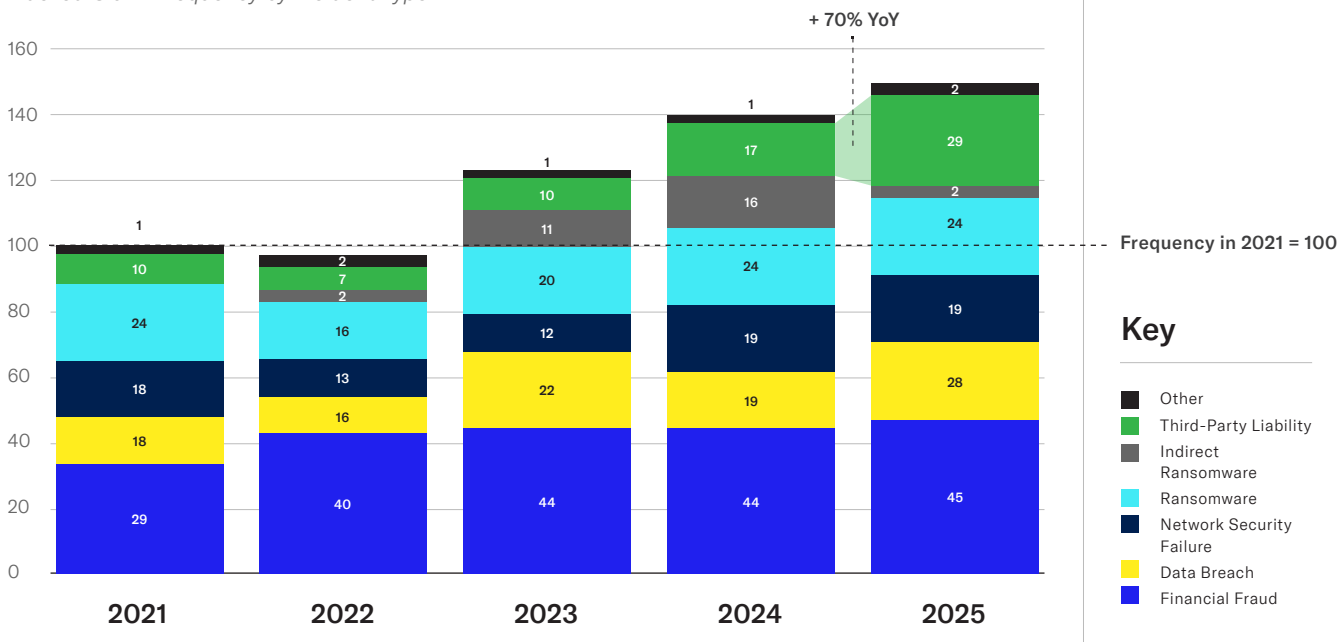
Indirect ransomware, or a ransomware attack on an insured's vendor or customer that results in damages to the insured, declined significantly with the absence of a large-scale aggregate event like the mass exploitation of companies operating the MOVEit file transfer software in 2023 or the ransomware attack against auto dealer software maker CDK Global in 2024.

Two incident types posted especially sharp increases. Data breach claims jumped 47%, which included a group of claims attributable to the 700Credit breach. Third-party liability claims surged 70%, and mainly include claims arising from class action lawsuits and litigation related to CIPA. These legal campaigns, which we discuss in Chapter 5, represent a distinctly different risk category: not security failures, but exposure to industrialized litigation.

FIGURE 3

Ransomware and Financial Fraud Incidents Remained Elevated, Third-Party Liability Claims Jumped 70%

Indexed Claim Frequency by Incident Type



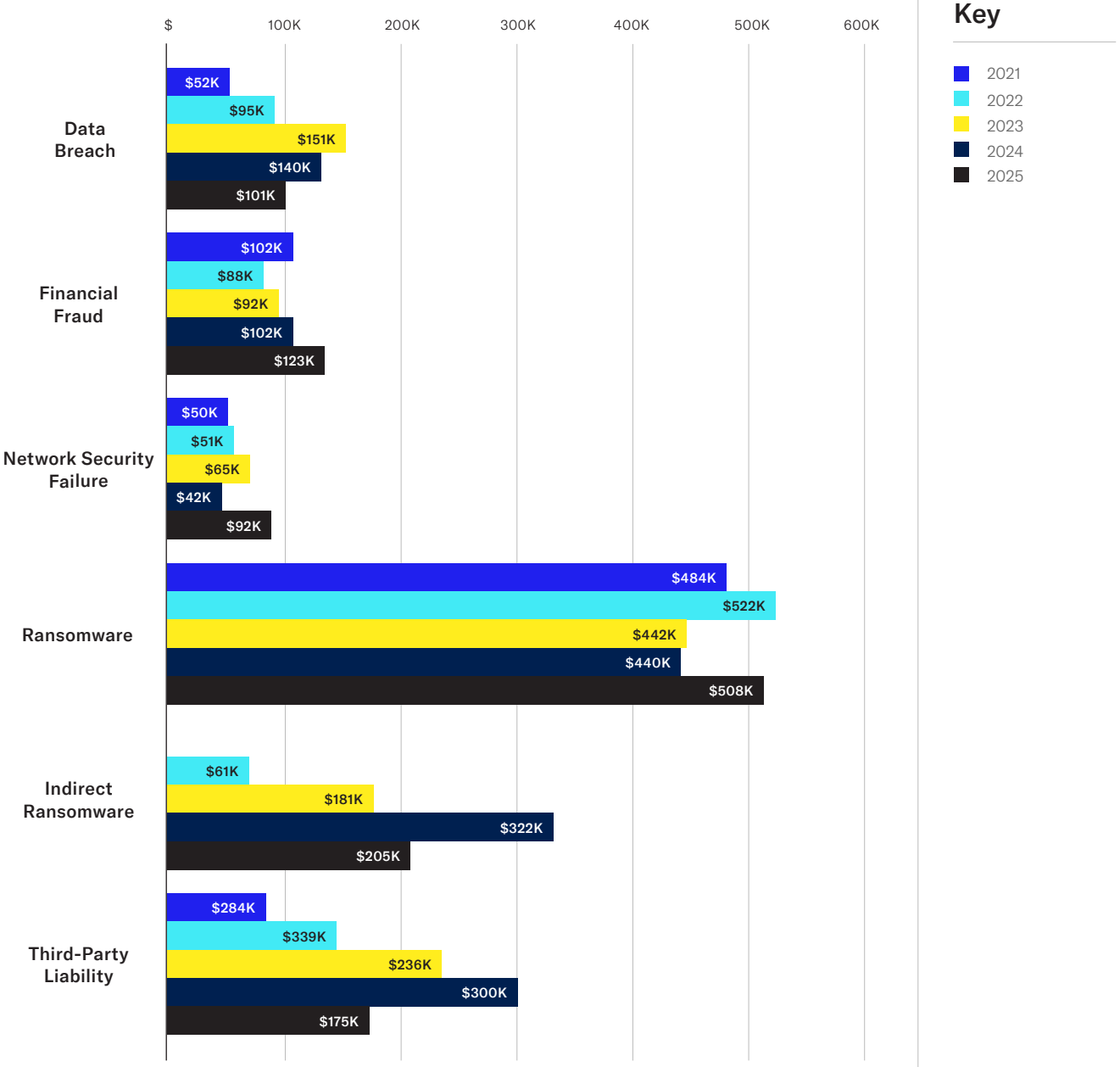
Ransomware remained the costliest incident type by a significant margin in 2025, with average severity of $508K, up 16% year-over-year. Financial fraud severity saw the largest increase, rising 21% year-over-year to $123K, a concern given financial fraud frequency continues to grow.

Average severity for third-party liability dropped, signaling a higher volume of less-damaging claims. However, businesses must be aware that class action lawsuits often arrive months after systems are back online and can add a year or more of legal proceedings, defense costs, and public scrutiny on top of the immediate costs of an incident a company thought it had already survived.

FIGURE 4

Ransomware Severity Up 16%, Financial Fraud Costs Accelerated

Average Claim Severity by Incident Type



Claim Frequency and Severity by **Revenue Band**

Across all three revenue bands, claim frequency increased in 2025. The largest companies (those with revenues between $100M and $500M) saw the most pronounced jump, with indexed frequency up 14% from the prior year.

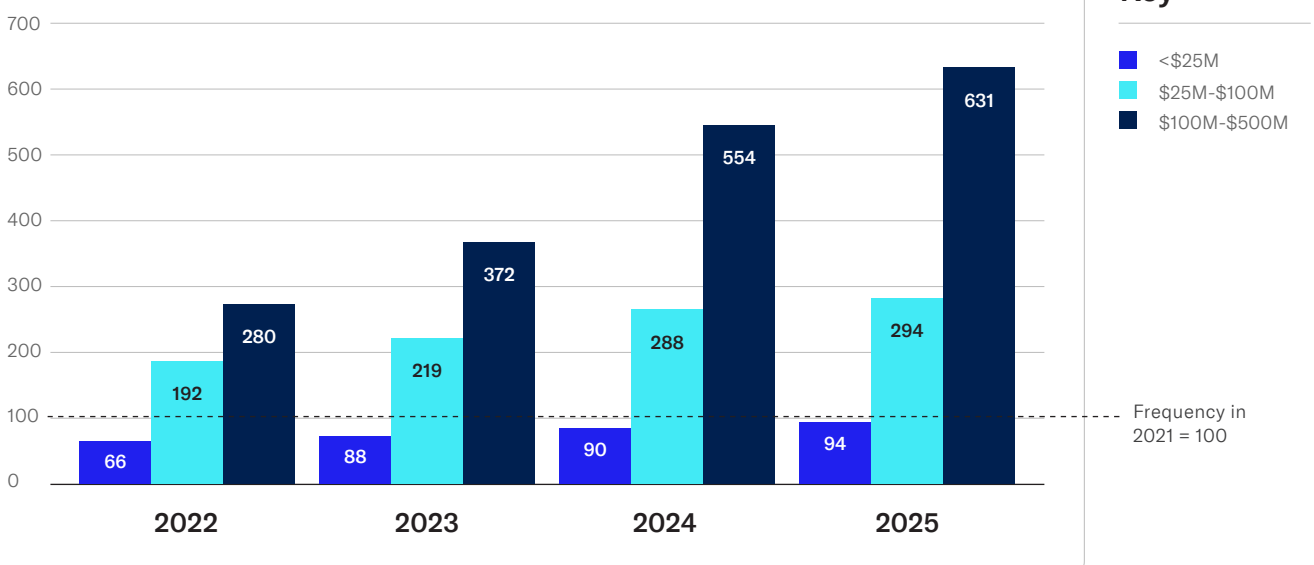
This pattern reinforces what we already know. Larger organizations have more attack surface: more employees, more vendors, more exposed systems, and more data worth targeting. They also tend to carry higher limits, making them more attractive targets for ransomware groups that calibrate ransom demands based on revenue.

Average claim severity increased to $221K in 2025, up from $216K in 2024, a new high for our dataset. The most striking severity story in 2025 was the continued escalation for companies under $25M in revenue. This segment saw a 26% increase in average severity year-over-year (the largest gain of any revenue band), reaching $180K. This is part of a sustained trend: The smallest companies in our portfolio have seen severity creep upward in each of the past three years, even as the largest segment has seen declines since 2023.

FIGURE 5

Claim Frequency Increased Across All Revenue Bands

Indexed Claim Frequency by Revenue Band



The increasing severity at the small end of the market reflects the ongoing shift in how attackers operate. Ransomware groups are casting wide nets based on the opportunities they find, scanning for vulnerable infrastructure at scale and deploying ransomware against whatever they discover.

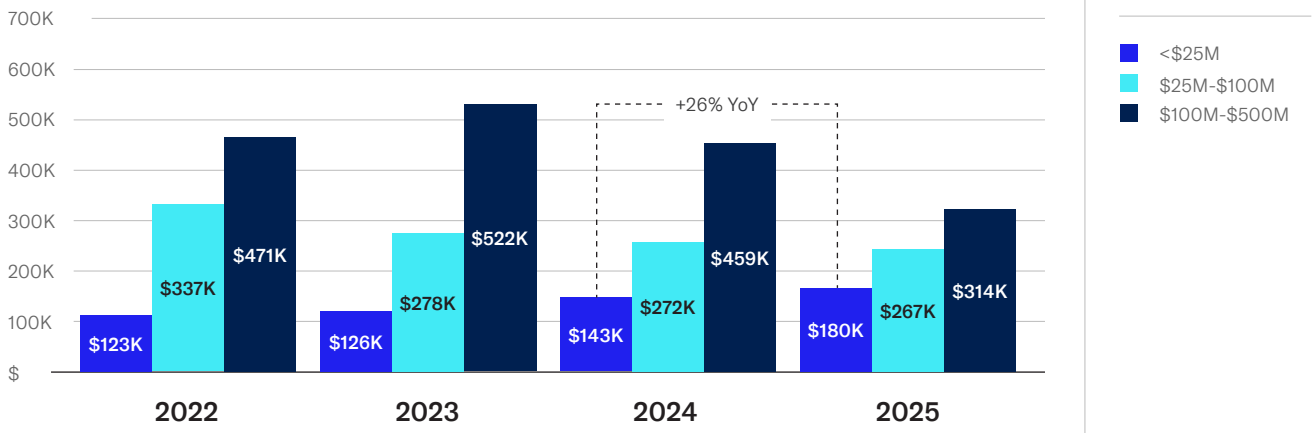
The Akira group's exploitation of SonicWall devices is a clear example: Attackers didn't seek out small businesses, they simply found exposed appliances and struck indiscriminately. When a $10M company and a $200M company share the same remote access tools, they share the same risk. The result is that smaller organizations, who have historically assumed that they were below the threshold of attacker interest, are now caught in the same ransomware campaigns as larger companies.

The increasing severity is also likely the result of under-investment in security controls among smaller companies. These organizations are less likely to purchase market-leading security tools or to have dedicated IT and security specialists who can consistently maintain the tools that they do purchase, and attackers are increasingly able to take advantage of the gaps in risk management that this creates.

FIGURE 6

Smallest Companies Saw a 26% Increase in Severity

Average Claim Severity by Revenue Band



Claim Frequency & Severity by **Industry**

Education, manufacturing, technology, and retail trade held their positions as the top four industries by claim frequency in 2025. The gap between this leading cohort and the remaining industries was substantial, reflecting structural differences in attack surface, technology maturity, and attacker preference.

Manufacturing companies, for example, tend to have a combination of operational technology, lean IT staff, and high-value production processes, making them attractive targets for ransomware groups that can extract meaningful leverage from business interruption. Ransomware frequency in manufacturing was 2.2X the average across all industries in 2025 (see Chapter 2).

Technology topped overall claim severity in 2025 at $271K (Figure 8), driven by the highest average severity for ransomware claims. Healthcare ($250K) and manufacturing ($248K) followed. All three exceed the $221K portfolio average and share a common vulnerability profile: connected operations, sensitive data, and high cost of disruption.

FIGURE 7

Education, Manufacturing, and Technology Remained Most Exposed

Indexed Claim Frequency by Industry, 2025

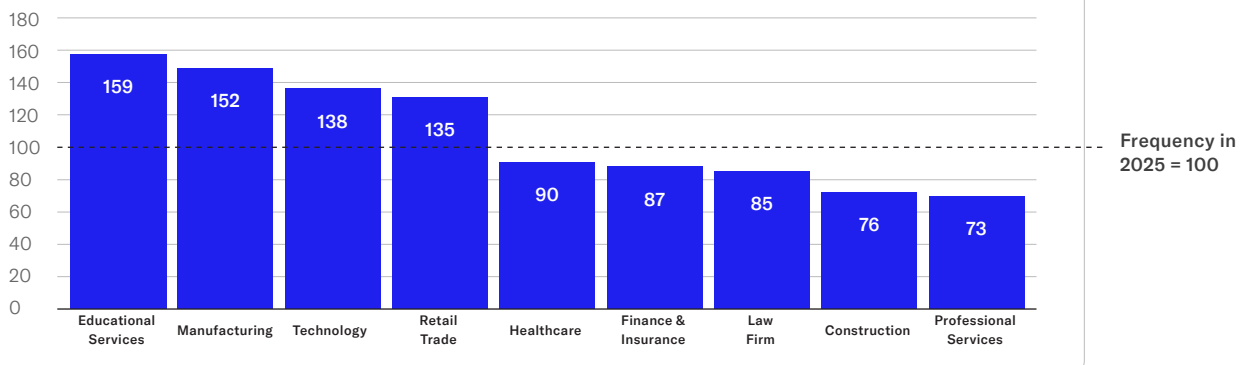
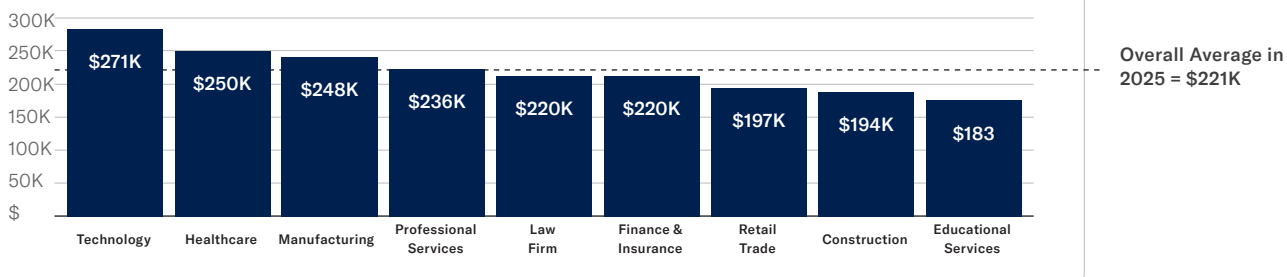


FIGURE 8

Technology Companies Had Highest Severity in 2025

Average Claim Severity by Industry, 2025



How Attackers Got In — and What Happened Next

Email remained the most common initial entry vector in 2025, accounting for 52% of all cyber-related claims. This reflects the critical role of email in enabling financial fraud, which continued to dominate claim volume. Remote access, including VPN and RDP, was the second most frequent entry vector at 24%, followed by the insured's vendor or client at 14%.

The vendor and client entry vector, accounting for roughly one in six incidents, is worth highlighting as a leading indicator of third-party risk exposure. As more companies connect their operations to vendors and partners through shared platforms and integrations, the attack surface created by those relationships continues to expand.

Remote access intrusions incurred the highest average severity at $433K, more than double the $212K overall average. This premium reflects the nature of corporate system attacks: These incidents are more likely to involve ransomware deployed after lateral movement inside the perimeter, resulting in widespread encryption, extended downtime, and higher response costs.

Email-based incidents, while frequent, averaged $109K in severity, consistent with their primary association with financial fraud. Incidents involving the insured's vendor or client averaged $145K, which is costly considering these incidents start outside of the insured's environment and are therefore virtually impossible to prevent.

FIGURE 9

Email Was Still the Most Common Entry Vector

Claims by Initial Entry Vector, 2025

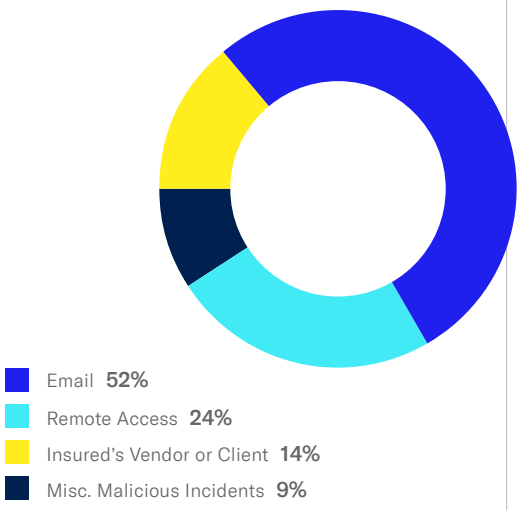
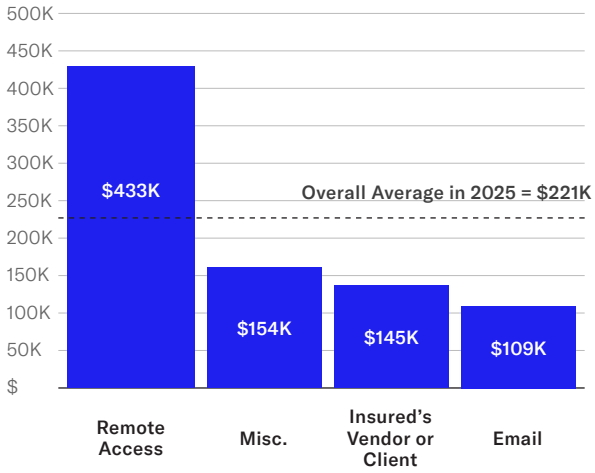


FIGURE 10

Attacks on Remote Access Were 2X Costlier Than Average

Claim Severity by Initial Entry Vector, 2025



**For the purposes of this analysis, we have excluded incidents unrelated to cyber attacks where no true entry vector existed, such as claims related to litigation or copyright infringement.*

Ransomware

CHAPTER

02

Ransomware Frequency & Severity Both **on the Rise**

Ransomware returned to the center of the cyber threat landscape in 2025, not because the threat fundamentally changed, but because one group arrived with a playbook that was industrially efficient and remarkably effective. Akira ransomware accounted for more than 40% of all ransomware claims in At-Bay's portfolio, making it the single most dominant strain we have ever tracked in a single year.

The story of ransomware in 2025 is, in large part, the story of Akira. But it is also a story about the continuing vulnerability of remote access infrastructure (particularly VPNs), the growing financial consequences of ransomware for businesses of all sizes, and our continued observation of threat groups that prioritize exfiltration over encryption as their preferred mechanism for extorting ransoms.

Ransomware frequency in 2025 reached near-parity with the 2021 baseline, continuing a steady climb that has now extended for three consecutive years after the sharp dip in 2022, then surging in Q3 and Q4 driven almost entirely by Akira. Average ransomware severity reached $508K in 2025, a 16% increase year-over-year.

FIGURE 11

Ransomware Frequency Returned to 2021 Levels

Indexed Ransomware Frequency by Year

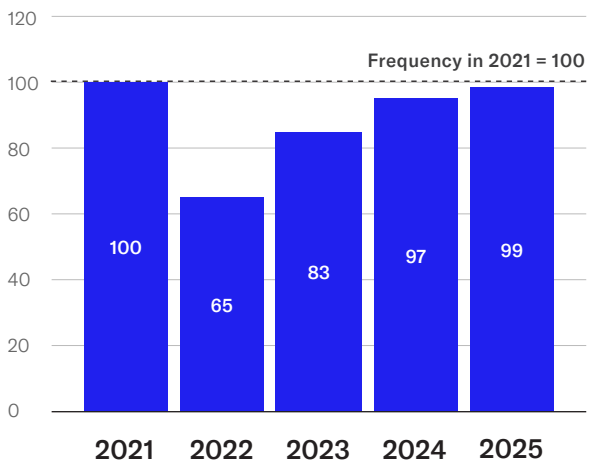
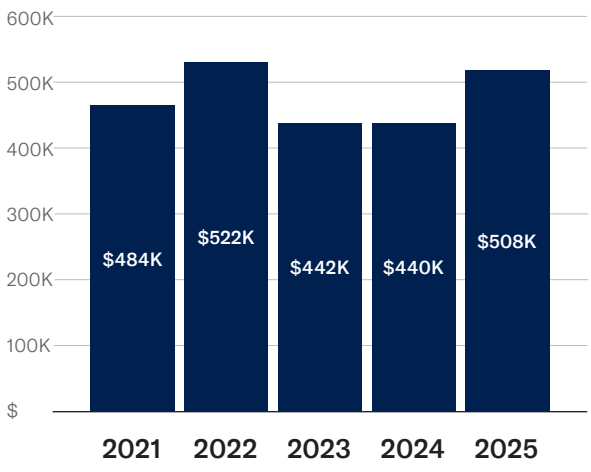


FIGURE 12

Average Ransomware Severity Climbed to $508K, a Three-Year High

Ransomware Severity by Year



Ransomware Trends by **Revenue and Industry**

Companies with under $25M in annual revenue saw a 21% year-over-year increase in ransomware claim frequency, the largest jump of any segment and a meaningful reversal from recent years when mid-market companies bore the brunt of frequency increases.

This shift reflects most threat actors' (including Akira's) infrastructure-driven targeting model. Akira identifies companies operating a specific technology stack (SonicWall appliances in 2025) and attacks them in an industrialized manner, regardless of size or segment. This data should dispel any lingering sense that smaller businesses are below the radar.

Severity by revenue band mirrors the frequency story. Companies under $25M in revenue saw a 40% increase in average ransomware severity ($422K), the largest jump of any segment.

FIGURE 13

Smallest Businesses Saw the Largest Jump in Ransomware Frequency (21% YoY)

Indexed Ransomware Frequency by Revenue Band

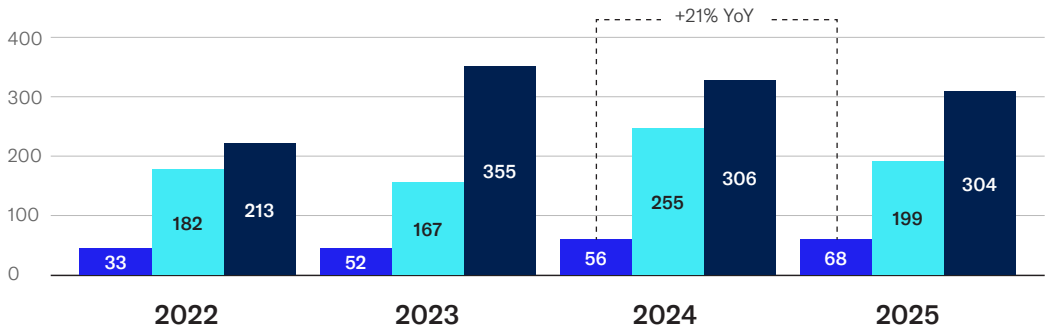
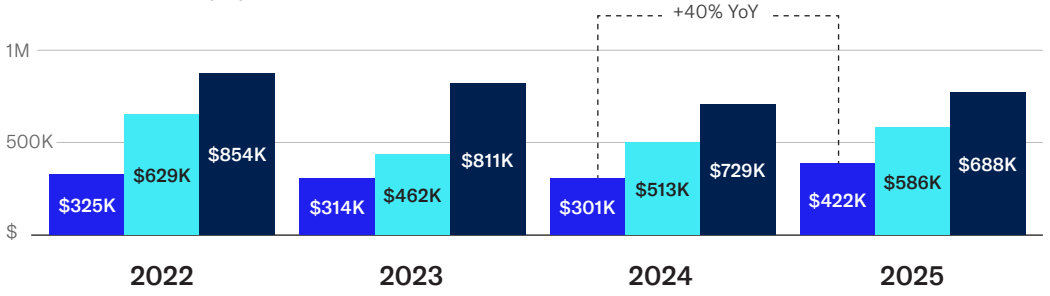


FIGURE 14

Smallest Businesses Also Saw the Steepest Severity Increase (+40% YoY)

Ransomware Severity by Revenue Band



Technology topped the 2025 ransomware severity rankings with an average of $875K per claim, 72% higher than the $508K average. Finance and insurance ($731K) and health care ($675K) followed. Although manufacturing ($451K) and law firms ($418K) ranked fifth and sixth respectively, the average severity for these industries was in line with those from prior years. Neither industry got safer — the rest of the market simply got more exposed.

FIGURE 15

Ransomware Attacks Hit Manufacturing the Hardest, 2.2X the Average

Indexed Ransomware Frequency by Industry, 2025

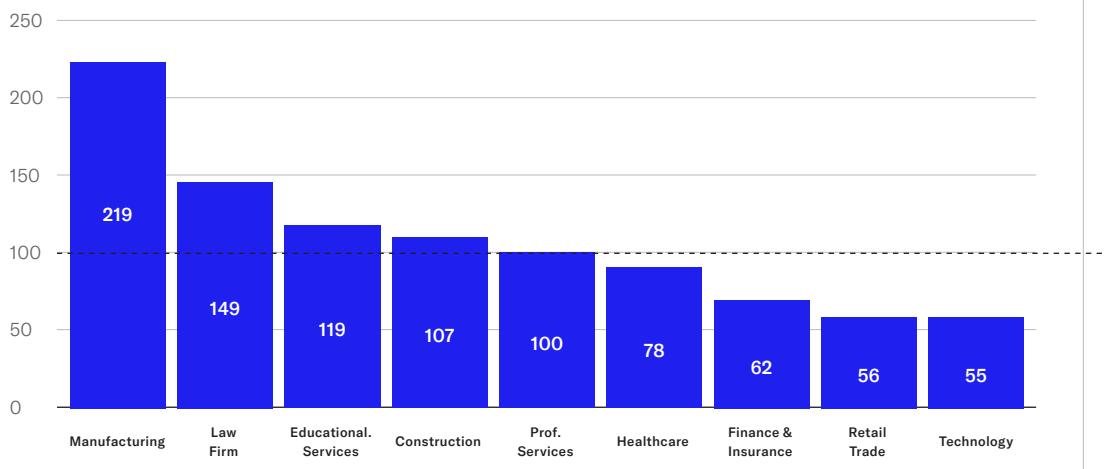
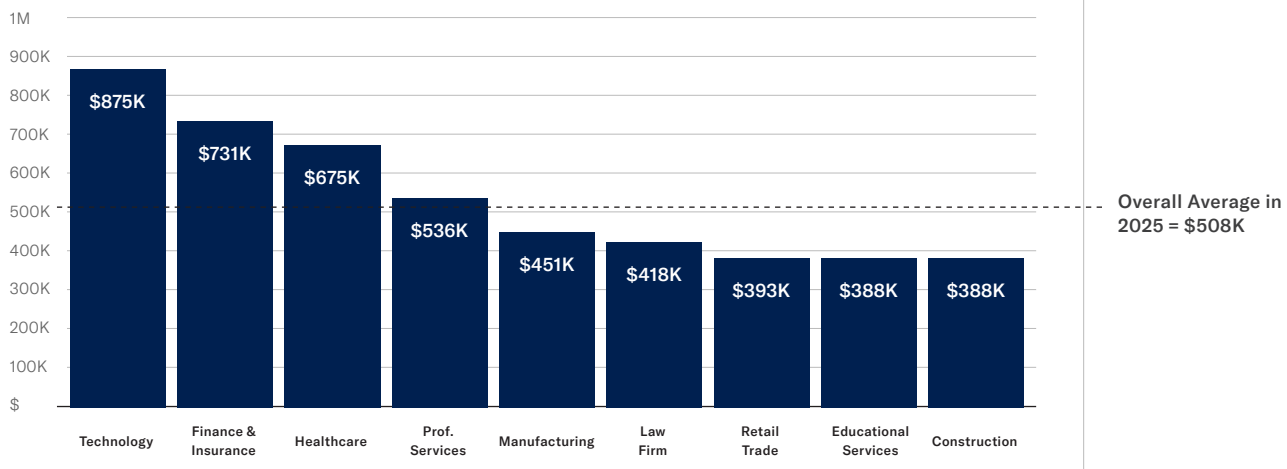


FIGURE 16

Technology Industry Saw 72% Higher Ransomware Severity Than Average

Ransomware Severity by Industry, 2025



Ransomware's Stranglehold on Remote Access

The shift in ransomware entry vectors over three years represents one of the most significant structural changes in the threat landscape. VPNs accounted for 38% of ransomware attacks with an identified entry vector in 2023. In 2024, that share rose to 66%. In 2025, it climbed to 73%.

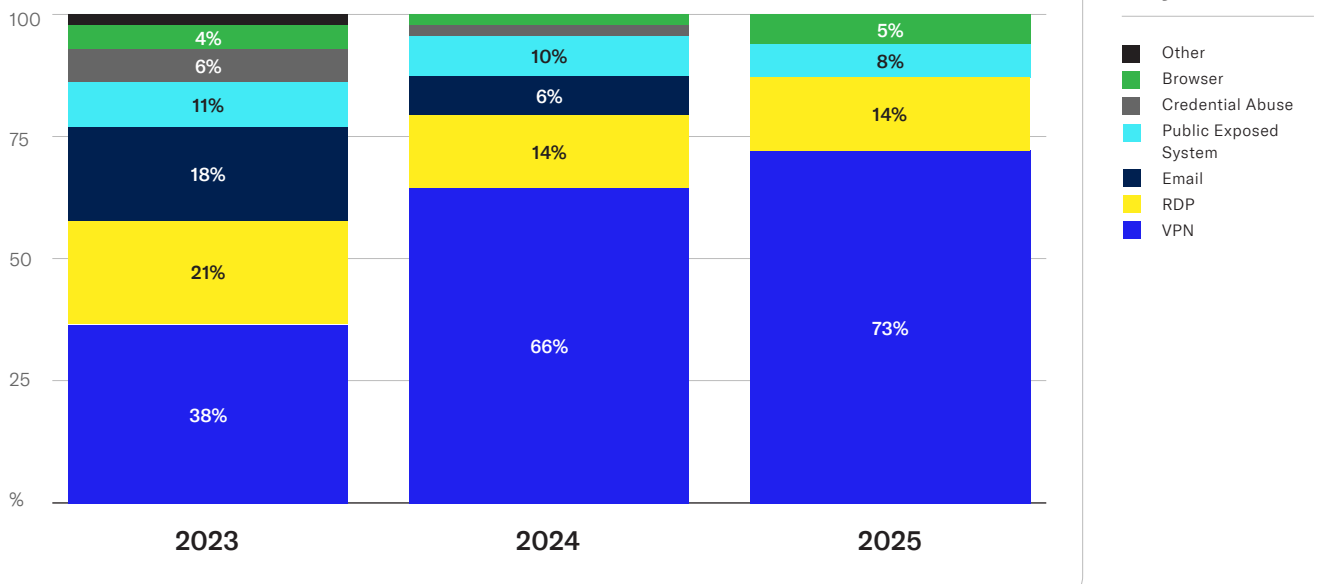
VPNs and RDP combined accounted for 87% of all ransomware claims in 2025, up from 80% the prior year. Also of note: Email did not lead to a single ransomware claim for At-Bay in 2025. This is a reflection of the improved effectiveness of email solution providers at detecting and removing overtly dangerous content from inboxes.

For this vector to have disappeared entirely from the ransomware column also reflects a decisive attacker pivot toward tactics that are more likely to succeed. Attackers go where the openings are. In 2025, those openings were almost exclusively in remote access infrastructure. When remote access was the entry vector, 55% of those incidents involved a SonicWall device (Figure 18), a direct result of Akira's mass exploitation of those devices in Q3 and Q4 of 2025. Akira's share of more than 40% of all ransomware claims in 2025 is extraordinary by historical standards (Figure 19). In prior years, the largest single strain rarely exceeded 20-25% of claims.

FIGURE 17

VPNs Accounted for Nearly Three-Quarters of All Ransomware Entry

Ransomware Initial Entry Vector by Year

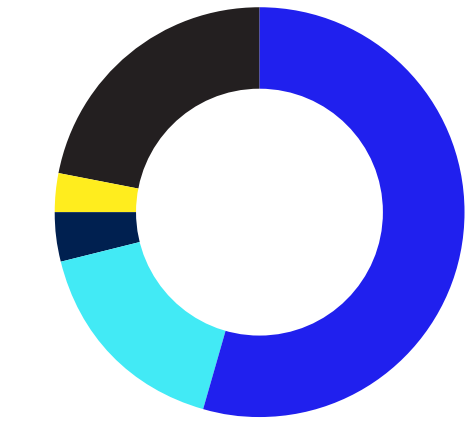


1 in 3 ransomware claims started with SonicWall

FIGURE 18

SonicWall Was the Entry Point for 55% of All Remote Access Ransomware Incidents

% of 2025 Ransomware Claims by Remote Access Vendor



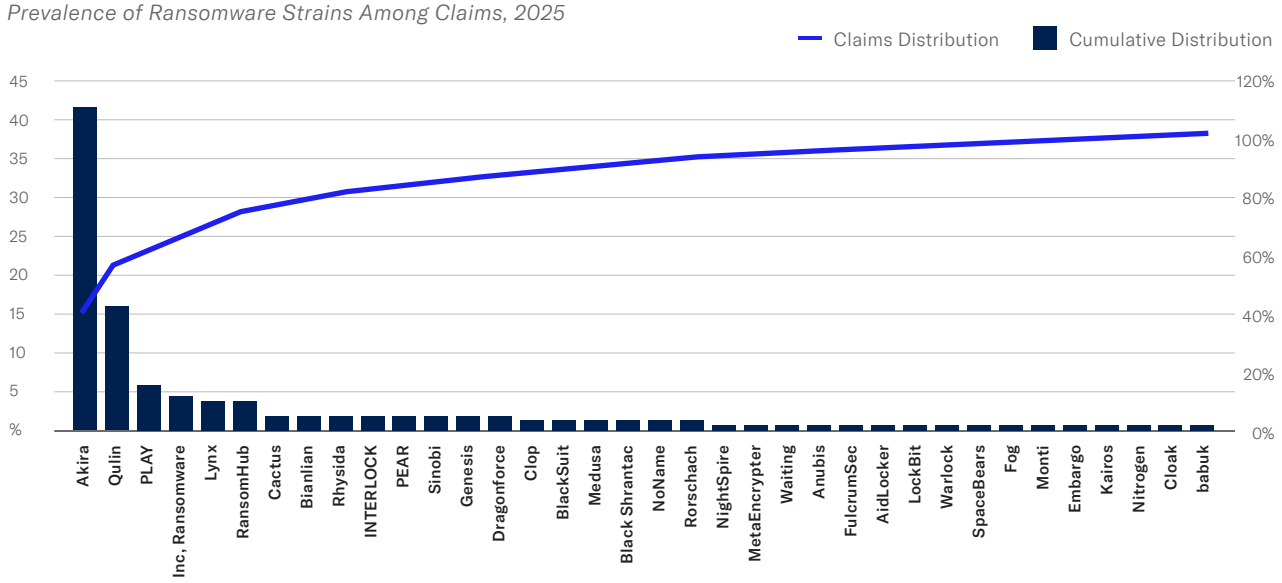
Beyond Akira, the 2025 ransomware ecosystem reflects continued fragmentation. At-Bay observed dozens of distinct groups among our claims. The fragmentation matters for victims. With a large and growing number of groups operating, the norms around negotiation, data deletion after payment, and decryptor delivery have continued to erode. Victims can be less certain of who they are dealing with and what promises will be honored, if any. The progressive fragmentation will also erode the ability of global law enforcement to reliably track groups over time, likely resulting in decreased enforcement activity.

Notably, pure exfiltration actors continue to be a growing presence. These are groups that steal data without deploying encryption ransomware, operating under the threat of publication rather than operational disruption. One such group, PEAR (Pure Extraction and Ransom) Team, emerged in June 2025 and has already claimed 63 victims via exfiltration with no encryption. The group relies purely on data theft and the threat of public exposure to extort its victims. This prevalence in exfiltration tactics is a trend we flagged in our 2024 report.

FIGURE 19

Akira Led All Ransomware, but the Ecosystem Is Wide and Fragmented

Prevalence of Ransomware Strains Among Claims, 2025



[1] Source: PEAR Site (as of 3/11/2026)

Spotlight on Akira Ransomware

At-Bay's largest cyber risk event of 2025 involved the alignment of remote access risks with a threat group ready to take advantage of the opportunity they presented. While the elevated risks of on-premise VPN appliances have been an issue of concern for At-Bay since mid-2023, we have not previously seen strong evidence that cyber criminals were making a deliberate effort to target specific makes or models of devices. This changed in July 2025.

Akira has operated since 2023 as a ransomware-as-a-service (RaaS) operation, but 2025 was a breakout year. The campaign drove a 53% increase in ransomware frequency and a 364% increase in Akira ransomware frequency in Q3-Q4 and was almost entirely focused on attacking SonicWall devices. According to our claims data for all of 2025, 86% of Akira attacks occurred in environments where a SonicWall device was present.

These attacks also occurred much faster than average. While deployment of ransomware often occurs days or weeks after initial entry, many Akira events observed by At-Bay occurred within hours or minutes. This timeline supports our assessment that these attacks were specifically targeted, and the presence of a SonicWall device was the inferred targeting criteria for victim selection. Finally, ransom demands from Akira were more than twice what we saw from the group prior to the second half of 2025. Taken together, these factors paint a picture of a threat group operating confidently with tactics they clearly knew would be game-changers.

FIGURE 20

Akira Drove Massive Ransomware Surge in Q3 and Q4

Indexed Ransomware Frequency by Quarter, 2025

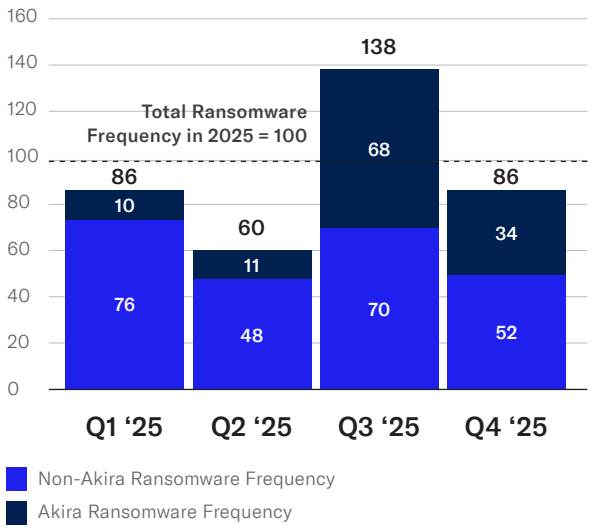
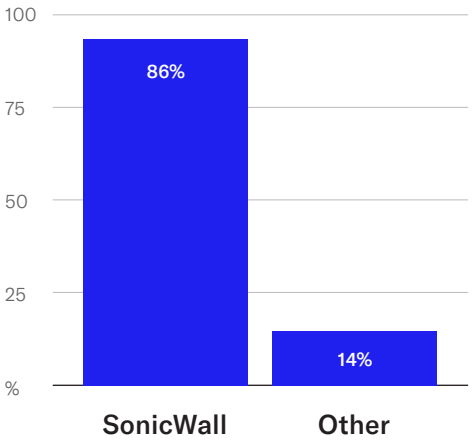


FIGURE 21

86% of Akira Attacks Had a SonicWall Device Present

Percentage of Akira Ransomware with SonicWall Present, 2025



Akira Hit Larger Companies and Manufacturers Disproportionately Harder

Akira's targeting was driven by infrastructure, not by deliberate industry or size selection. The campaign exploited SonicWall devices wherever they existed. In this case, we saw the largest spikes in mid-market companies and across manufacturing, construction, law firms, and professional services. Manufacturers were hit almost 2X any other industry.

FIGURE 22

Akira Impacted Companies Over $25M in Revenue Disproportionately

Akira Ransomware Claims Frequency by Revenue Band, 2025

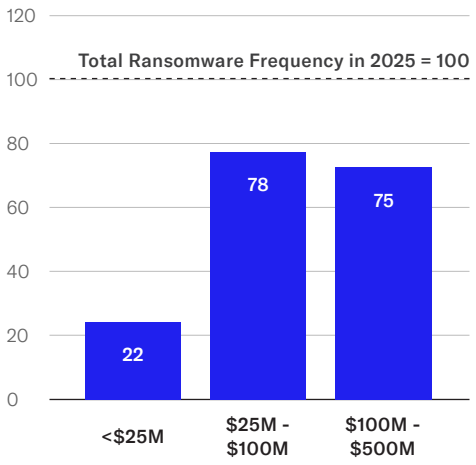
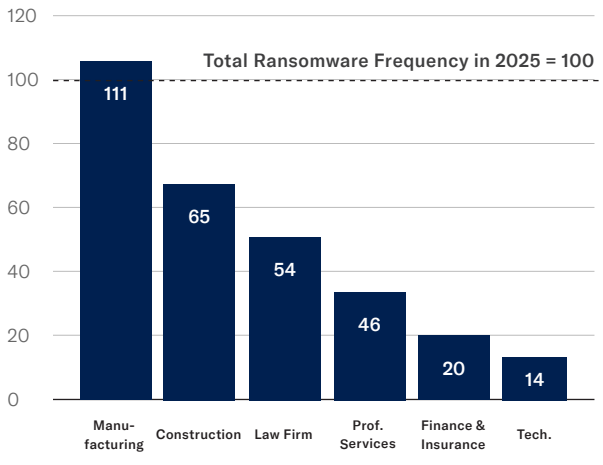


FIGURE 23

Manufacturers Hit by Akira Nearly 2X Any Other Industry

Akira Ransomware Claims Frequency by Industry, 2025



> Of the businesses that were **not** encrypted by Akira, all of them had high-fidelity 24/7 Managed Detection and Response

Akira Ransom Demands Were More Aggressive Than Other Ransomware Attacks

An Akira attack was significantly more expensive than a typical ransomware incident in 2025. Average Akira ransom demands came in at $1.2M, 50% higher than the average non-Akira demand of $824K. Average Akira payments reached $452K, compared to $332K for non-Akira incidents, a 36% difference.

Severity by revenue band for Akira claims further confirms the scaling dynamic and also explains the significant increase in ransomware severity for companies with less than $25M in revenue. The average Akira ransomware severity for these companies was $419K, a sizeable jump from the $301K average ransomware severity in 2024.

FIGURE 24

Akira Ransom Demands Were 50% Higher Than Other Ransom Demands

Average Akira Ransom Demand and Payment vs. Non-Akira Ransomware, 2025

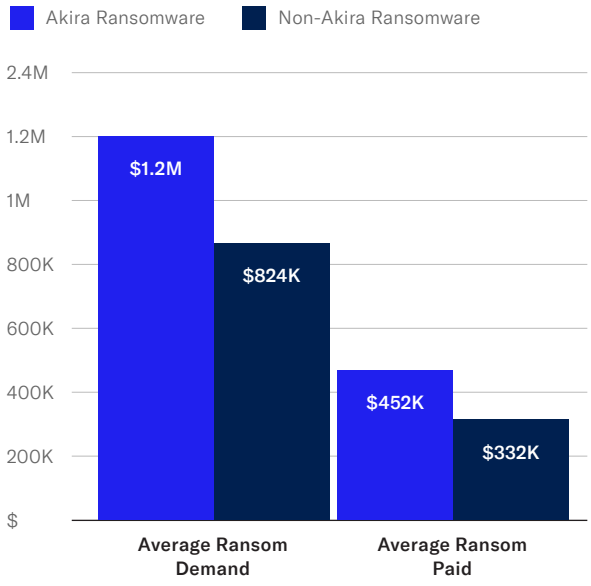
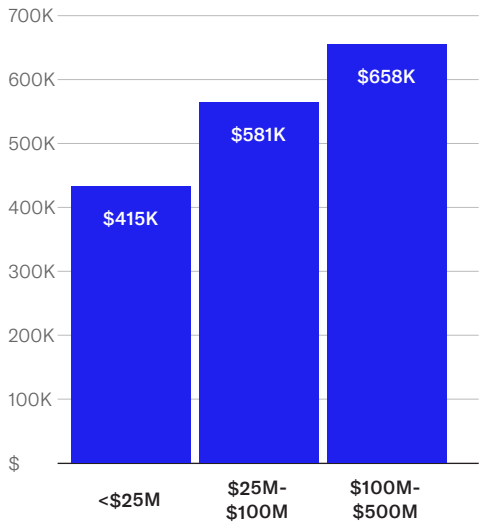


FIGURE 25

Average Akira Claims Severity Increased as Company Revenue Size Increased

Average Severity of Akira Claims by Revenue Band, 2025



Most Akira Attacks Happened on Nights and Weekends

Two-thirds of Akira attacks occurred outside normal business hours on nights or weekends. Although this may simply be a function of the threat actors' location, the timing of attacks made it conveniently inconvenient for businesses to detect and respond quickly enough to prevent damage. Organizations without 24/7 monitoring had little opportunity to interrupt the attack chain once Akira began its final stage.

However, we did identify one bright spot. Of the businesses that were not encrypted, all had high-fidelity Managed Detection and Response (MDR) monitoring and securing their environments 24/7. Notably, not a single At-Bay MDR customer filed an Akira claim in 2025.

How At-Bay MDR Stopped Akira in Its Tracks

The Threat

Akira ransomware attackers targeted a company by leveraging stolen VPN credentials to probe 126 hosts with automated tools at 2:10 AM in the morning.

The Remediation

Due to fast action and eradication, the threat actor was unable to complete pre-ransomware reconnaissance, and our client ended the day more resilient.

<15 minutes for At-Bay MDR to contain and remediate threat.*

Within **10 minutes**

Attacker presence indicated by network discovery attempts identified by At-Bay's MDR Team

Within **15 minutes**

At-Bay MDR completely contained compromised SonicWall credentials and the attack before any systems were able to be accessed

At-Bay Stance™ MDR offers enterprise-grade, AI-powered security with 24/7 monitoring, expert-led response, and full remediation, all at a fraction of the cost of an in-house SOC. Our MDR protects the entire IT environment, delivering a 99.999% incident avoidance rate.**

Not a single **At-Bay MDR customer** experienced an Akira-driven claim in 2025

**Response timelines differ. Past results do not guarantee future outcomes. This content is provided for information purposes only and is not intended to define any Policy commitment. No warranty is given or liability accepted regarding this information.*
***Based on At-Bay MDR portfolio performance data from inception through December 15, 2025.*

The Cost of Ransomware

Across all ransomware claims in 2025, the average ransom demand was $980K. The average ransom payment was $370K, representing 38% of the demand. Both of these numbers were up from last year, when the average ransom demand was $953K and the average ransom payment was $312K.

Ransom was only paid in 32% of incidents where there was a demand, consistent with the prior year. The 68% payment avoidance rate is the product of effective incident response: functioning backup infrastructure, skilled negotiation, and the involvement of experienced claims professionals who understand how ransomware groups actually operate.

FIGURE 26

At-Bay Response & Recovery Team Avoided $91M in Ransoms

*Total Ransom Demanded vs. Actual Ransom Paid, 2025**

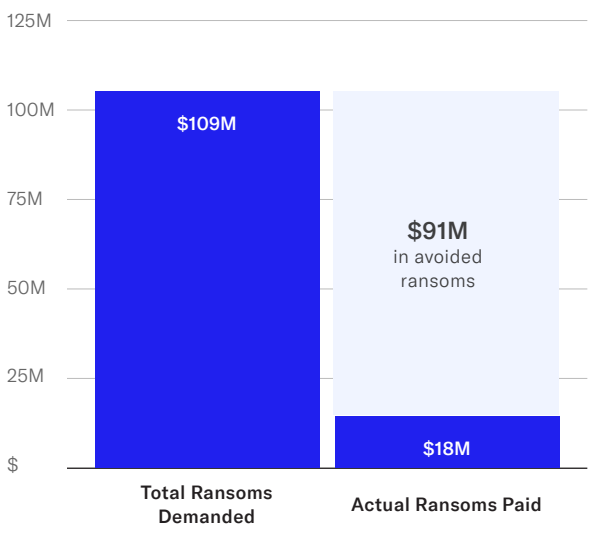
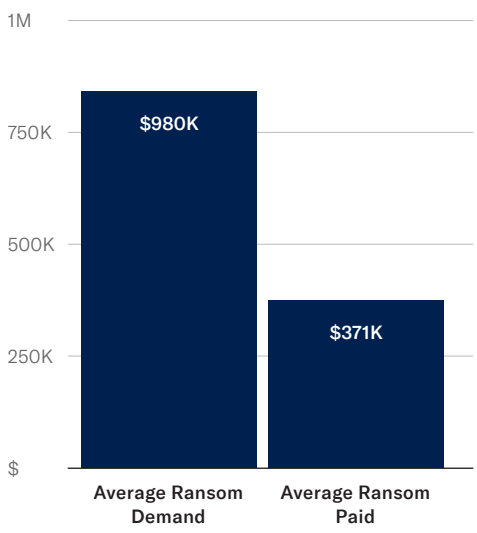


FIGURE 27

Average Ransom Payment Was $370K, 62% Lower Than Demand

Average Ransom Demand and Payment, 2025



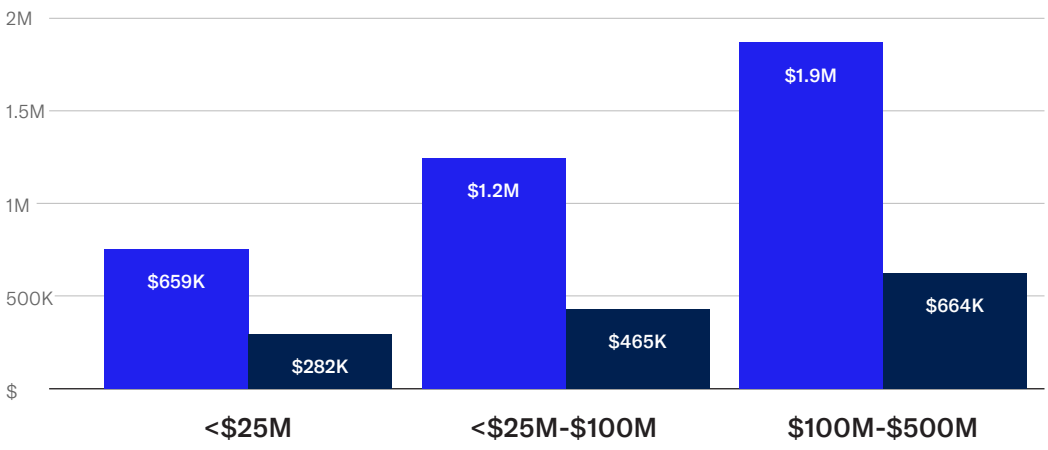
> At-Bay's Response & Recovery team helped policyholders **avoid $91M in ransoms in 2025**

*Only includes claims where At-Bay Response and Recovery was engaged as DFIR vendor

FIGURE 28

Ransom Payments and Demands Scaled With Revenue

Average Ransom Demand and Payment by Revenue Band, 2025



Key

- Average Ransom Demand
- Average Ransom Paid

The gap between demand and payment reflects an important strategic dynamic. Ransomware groups set opening demands with negotiation in mind. The initial demand is rarely the expected outcome. Understanding this is a core element of effective incident response, and it reinforces the value of having experienced professionals involved from the first hours of an incident.

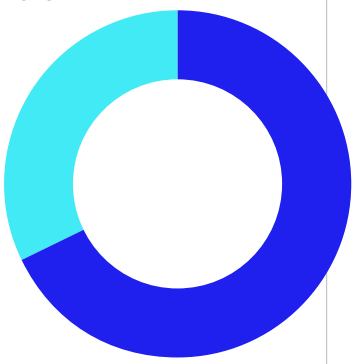
Ransom demands and payments scale with victim revenue. The highest revenue band faced an average demand of approximately $1.9M and an average payment of $664K, roughly 1.8X the overall average payment.

Meanwhile, a $282K average payment is not a modest line item for a business with under $25M in annual revenue. It represents a potentially existential expense, layered on top of business interruption costs, incident response fees, and legal expenses.

FIGURE 29

Only 32% of Ransom Demands Resulted in an Actual Ransom Payment

Ransomware Claims with Ransom Paid vs. Not Paid, 2025



No Ransom Paid **68%**

Ransom Paid **32%**

BUSINESS INTERRUPTION:

The Hidden Multiplier

Ransom payments get headlines. But for many businesses hit by ransomware attacks, significant additional damage comes from simply being unable to operate.

Business interruption coverage compensates policyholders for lost revenue and extra expenses when a cyber incident shuts down or disrupts operations and can make ransomware severity skyrocket.

Claims that involved a business interruption payment averaged $510K in severity, compared to just $168K for ransomware claims without one. That's a 3X difference, driven by the cost of lost revenue, emergency operations, and system rebuild while the business is offline.

1 in 3 ransomware claims triggered business interruption coverage

Most disruptions resolve within a month, but roughly one in ten ransomware incidents causes downtime exceeding 30 days.

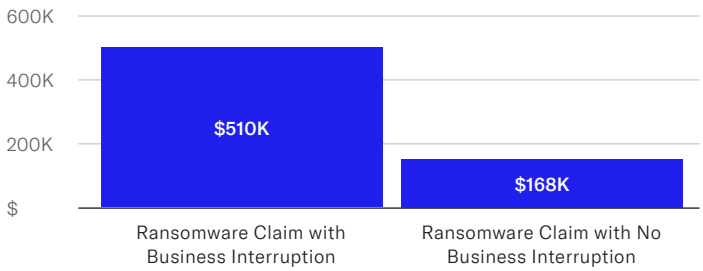
The largest single business interruption claim hit $5M, the coverage limit for that insured, but the actual business interruption cost in that case was likely much higher.

Containment is key. An intrusion that's detected and isolated early, before encryption propagates across critical systems, has a better chance of resolving without major damage.

FIGURE 30

Ransomware With Business Interruption Was 3X More Severe

Average Ransomware Claim Severity With Business Interruption vs. No Business Interruption, 2025



Why 24/7 Monitoring Changes the Math

Ransomware doesn't encrypt an entire environment instantly. Threat actors move through a network — sometimes over hours, sometimes over days — before deploying their payload. That window is the opportunity.

An organization with 24/7 Managed Detection and Response (MDR) in place can catch lateral movement before it reaches critical systems, containing the incident before operations go down. One without it may not find out until the business is already dark. Early detection can compress the blast radius, and as the data shows, that compression can potentially be worth several hundreds of thousands of dollars.

At-Bay MDR has a 99.999% incident avoidance rate thanks to a combination of 24/7 monitoring and enterprise-grade security. **Learn more at [at-bay.com/mdr.](at-bay.com/mdr)**

Financial Fraud

CHAPTER 03

Financial Fraud Continued Its Climb

Financial fraud was the most common incident type once again. Financial fraud claim frequency has risen every year since the 2021 baseline, reaching its highest levels this year.

Unlike ransomware, which requires technical capability to execute, financial fraud requires only a convincing email and a moment of inattention. The continued growth in frequency reflects the increasing availability of generative AI tools that lower the barrier to crafting effective social engineering lures, making it possible for more attackers to execute more convincing fraud campaigns at greater scale, even across language barriers.

Email was the initial entry vector for 82% of financial fraud claims in 2025. Despite continued investment in email security, attackers have found ways to craft messages that evade detection using social engineering techniques like business email compromise, vendor impersonation, invoice manipulation. In our last InsurSec Rankings Report, we detailed how legacy email security solutions, in general, have been decreasing in effectiveness against modern fraud attacks.

FIGURE 31

Financial Fraud Frequency Remained Elevated

Indexed Financial Fraud Frequency by Year

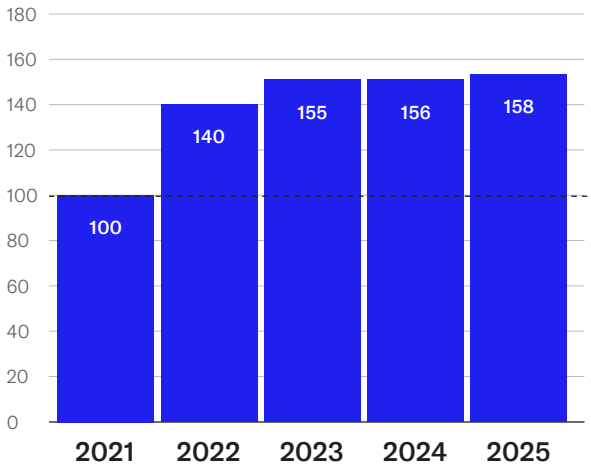
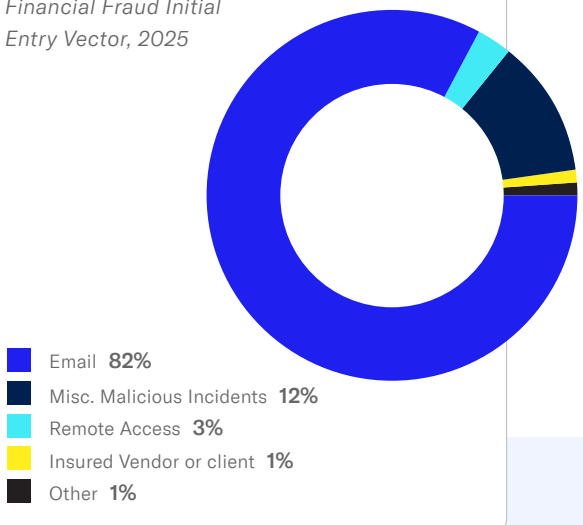


FIGURE 32

8 in 10 Financial Fraud Incidents Began With Email

Financial Fraud Initial Entry Vector, 2025



Stance Fraud Defense One Year In

In 2025, At-Bay launched Stance Fraud Defense to address attacks that legacy email security solutions consistently miss. Thousands of fraudulent emails that cleared existing email security filters have been flagged by the solution, and 40% of enrolled accounts were protected against an active attack. Fraud Defense is available at no additional cost to At-Bay Cyber and Tech E&O policyholders[1]: **stance.at-bay.com**.

[1] *Access to Stance Fraud Defense is available to insureds with policies placed through At-Bay Insurance Services, LLC that include an Embedded Security Endorsement.*

The Emergence of Abused Infrastructure

From September 2025 to March 2026, At-Bay's MDR for Email team triaged and analyzed over a million email security alerts, allowing us to identify emerging attacker trends and feed those insights back into our operations to improve security.

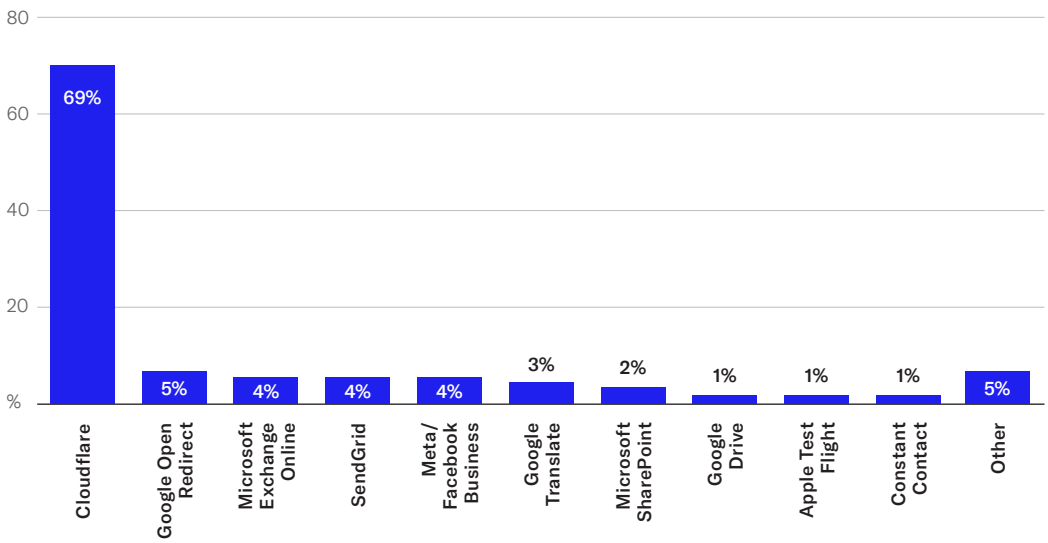
Although we know eight in ten financial fraud incidents begin with email, the tactics continue to evolve. Attackers are moving away from self-hosted, easily identifiable infrastructure in favor of hijacking legitimate cloud platforms.

By embedding attacks within standard business workflows (i.e., routing them through services like Cloudflare, Microsoft Exchange Online, TikTok, Canva, and Dropbox), they inherit the trust those platforms carry. Employees are accustomed to receiving real emails from these services, so messages sent through them don't trigger the same suspicion, or the same filters, as emails from spoofed or newly registered domains. This creates a detection gap that legacy email security solutions aren't designed to close. A filter that scans for known-bad domains won't flag a link sent through a legitimate Cloudflare domain, for example.

FIGURE 33

69% of Abused Infrastructure Alerts Were Associated With Cloudflare Links

Percentage of Abused Infrastructure Alerts by Vendor, September 2025-March 2026



How Attackers Are Using Cloudflare

Most email security tools work by automatically scanning links before they reach your inbox. Attackers have found a way around this by routing malicious links through Cloudflare, a widely trusted internet infrastructure provider. Because the link appears to come from Cloudflare, security scanners give it a pass. When those scanners try to investigate further, Cloudflare's own anti-bot protections block them, the same way it would block any automated traffic hitting a legitimate website.

The result is a malicious link that looks clean, hides where it actually leads, and is designed to steal credentials. Once an attacker has those credentials, they can monitor your email, learn your vendors and payment patterns, and either send fraudulent invoices or redirect wire transfers. Increasingly, we're also seeing attackers take a slower approach: quietly exfiltrating sensitive data and later threatening to publish it unless they're paid — a threat that doesn't go away once systems are restored.

Other Campaign Trends

We've observed significant increases in specific brand and service impersonation tactics that can change as frequently as week to week. Two surging campaigns we've recently observed:

Meta Brand Impersonation:

Meta or Facebook for Business emails primarily requesting marketing and social media administrative credentials to hijack corporate identity.

ADP & Payroll Logistics:

Using payroll and HR-themed emails to solicit credentials during time-sensitive financial windows.

How At-Bay MDR for Email Protects Businesses

At-Bay's MDR team manually reviews potentially threatening emails to identify emerging tactics then builds detections and automations that are deployed across all customers, so a pattern caught for one client becomes protection for thousands. 100% of customers who have deployed Stance MDR for Email have had an active threat detected and blocked, and 92% of monitored clients received high-severity detections over the past year. Read more about At-Bay MDR for Email's 24/7 monitoring and enterprise-grade email security technology at **at-bay.com/mdr.**

The Cost of Financial Fraud

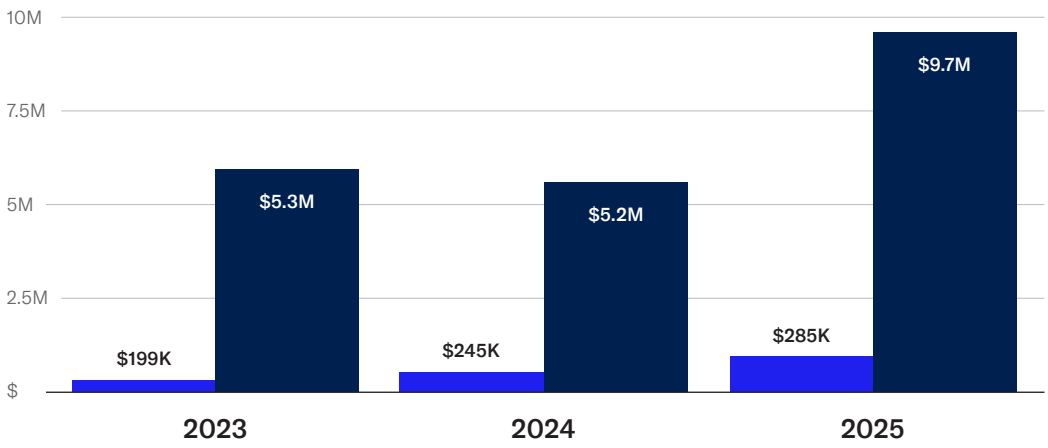
The average amount stolen in a financial fraud incident reached $285K in 2025, up 16% from $245K in 2024 and up significantly from $199K in 2023. This three-year trajectory reflects not just more fraud, but more effective fraud. Attackers are getting better at identifying higher-value targets and calibrating their social engineering to match.

The single largest amount of funds stolen from an At-Bay policyholder in 2025 was $9.65M, the highest we have recorded. That a company can lose nearly $10M to a single fraud incident is a reminder that financial fraud, while often treated as a lower-stakes threat than ransomware, can produce catastrophic outcomes.

FIGURE 34

Average Funds Stolen Rose 16%, and the Worst Cases Got Worse

Average and Max Funds Stolen by Year



Key

- Average Funds Stolen
- Max Funds Stolen

> Financial fraud, while often treated as a lower-stakes threat than ransomware, **can produce catastrophic outcomes.**

Financial Fraud Losses by **Revenue**

Mid-sized companies ($25M-$100M) saw the steepest increase of financial fraud frequency at 32% year-over-year. These businesses tend to have enough revenue to make fraud worthwhile yet lack the formal financial controls (dedicated accounts payable/receivable oversight, multi-approval wire processes, vendor change verification protocols) that larger enterprises build into their operations.

Average funds stolen generally scale with revenue, but the maximum loss figures by revenue band tell a more unsettling story. The single-largest fraud loss in the under-$25M segment reached $6M. In the $25M-$100M segment, the maximum was $9.65M. These are not statistical outliers to be footnoted, they are existential events for the businesses that experience them.

FIGURE 35

Mid-Market Companies Saw a 31% Jump in Financial Fraud Frequency

Indexed Financial Fraud Frequency by Revenue Band

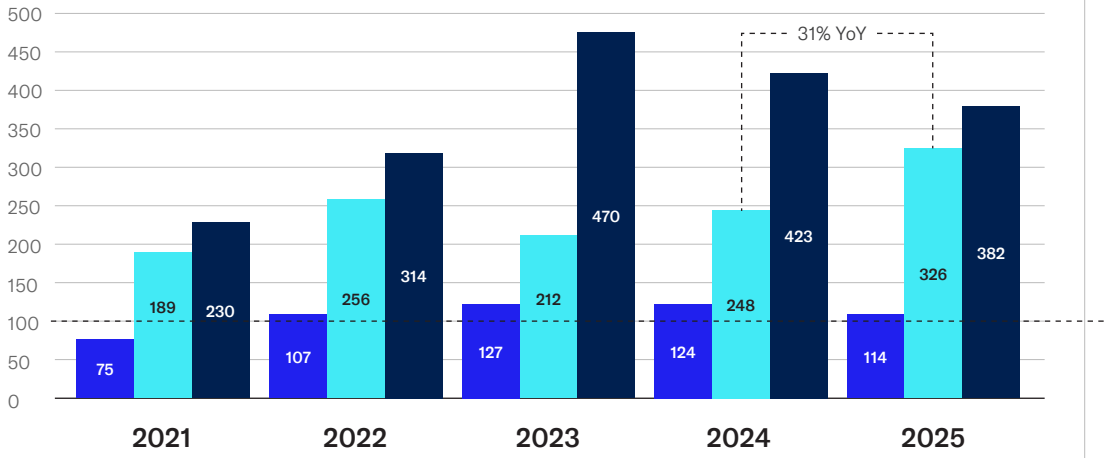
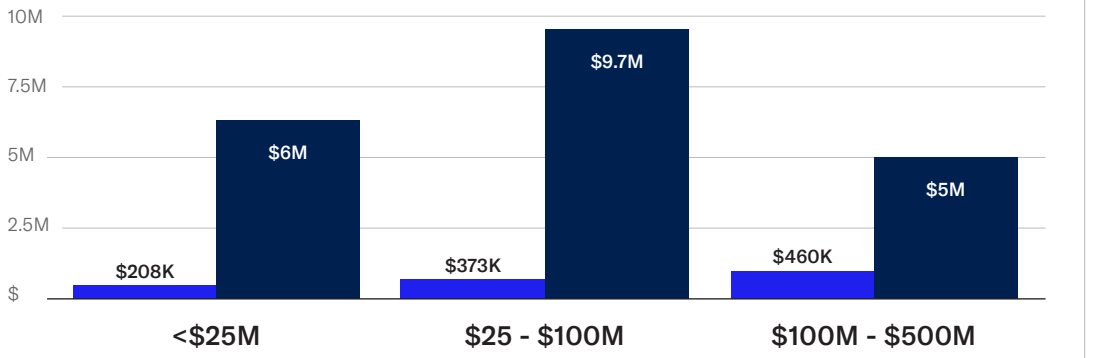


FIGURE 36

Larger Companies Faced Higher Average Losses

Average and Max Funds Stolen by Revenue Band, 2025



Financial Fraud Trends by **Industry**

Manufacturing topped the financial fraud frequency rankings, mirroring its position for ransomware frequency with one key difference. In ransomware, manufacturers are targeted because they disproportionately run vulnerable IT infrastructure. In financial fraud, manufacturers are targeted because of the nature of their procurement activity: large, routine purchase orders with numerous vendors, significant invoice volumes, and, in many cases, less mature financial controls than regulated industries like finance and insurance.

Real estate rental and leasing is a notable addition to the top tier. This sector processes frequent high-value transactions (lease payments, vendor invoices, capital improvement payments) and typically involves multiple parties and intermediaries, creating natural friction points that fraudsters can exploit through impersonation. Construction shares a similar profile: project-based billing, numerous subcontractors, and substantial wire transfers are the norm.

FIGURE 37

Manufacturing Led Financial Fraud Frequency, 1.5X Average

Indexed Financial Fraud Frequency by Industry, 2025

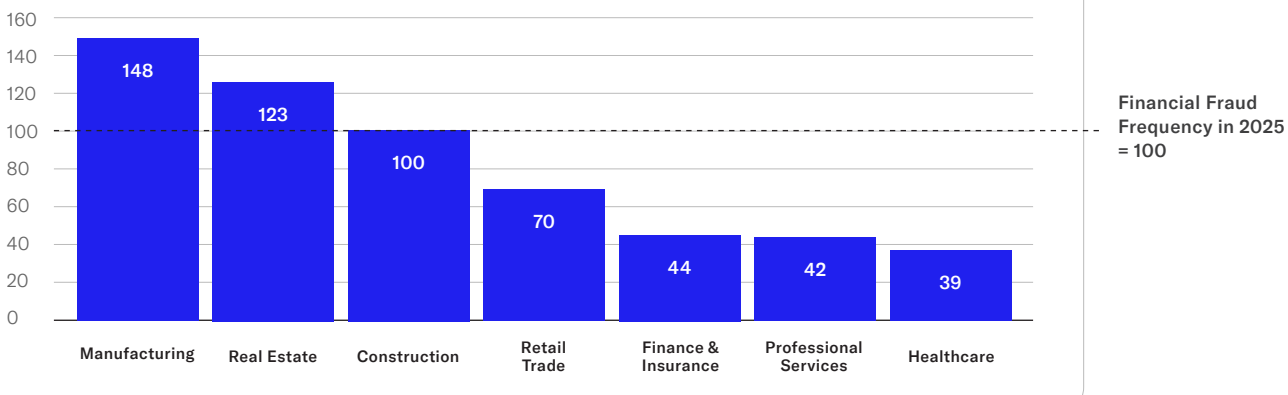
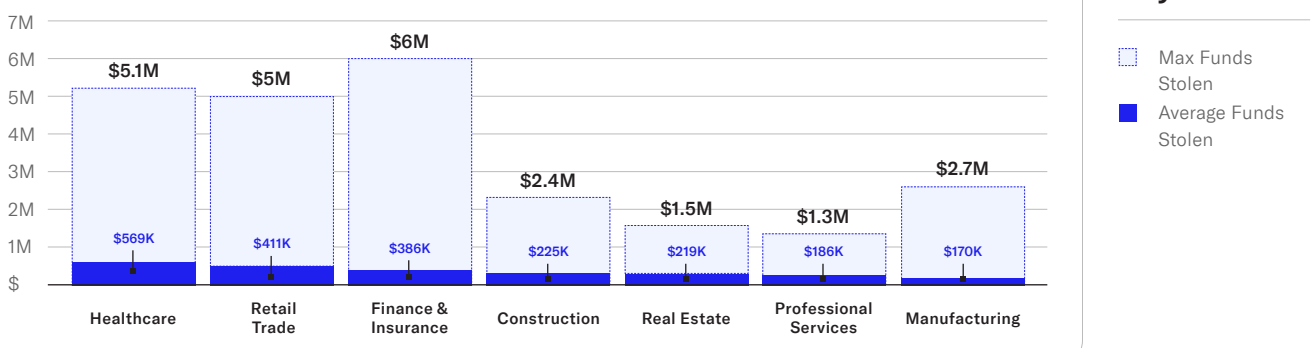


FIGURE 38

Healthcare Faced the Highest Average Funds Stolen

Average and Max Amount of Funds Stolen by Industry, 2025



THE COST OF WAITING:

How Time Impacts Fund Recovery Rates

Financial fraud recovery depends largely on how quickly the victim alerts their insurance provider. When a fraud incident occurs, there is a narrow window to intercept funds before they move beyond reach. The moment At-Bay is notified, our Claims team initiates our recovery process. This is a highly coordinated effort to trace, freeze, and recover misdirected funds through banking channels and law enforcement partners (see 'How a Clawback Happens' on the next page). In general, the faster we're alerted, the more likely some funds can be returned.

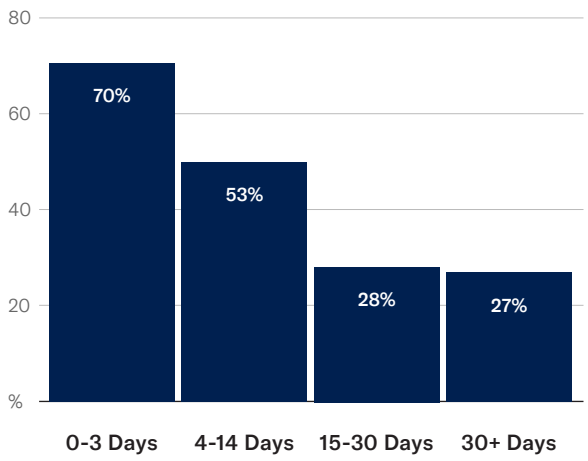
Every day that passes gives the threat actor additional time to move the stolen funds, convert them to cryptocurrency, or transfer overseas — increasing the threat actor's chances of cashing out and decreasing the victim's chances of recovering.

The practical implication: Businesses should treat suspected fraud with the same urgency as a ransomware attack. The instinct to investigate internally before escalating costs time and money.

FIGURE 39

70% of Clients Who Alerted At-Bay Within 0-3 Days Saw Some Funds Recovered

Percentage of Financial Fraud Victims with Some Funds Recovered, 2024-2025



At-Bay Recovered **$56M** in Stolen Funds in 2025

Financial fraud hit businesses hard in 2025, but just because money goes out the door doesn't mean it can't be recovered. In 2025, At-Bay's Claims team helped policyholders recoup a significant amount of financial fraud losses. To increase the odds of recovering funds, it's critical to work with a partner with a proven track record and defined process, because speed is everything.

Amount of Funds Recovered by At-Bay in 2025

$56M

Average Funds Recovered by At-Bay in 2025

$275K

Likelihood of a Full Financial Fraud Recovery with At-Bay in 2025

1 in 5

Overall Recovery Rate

42%

SPOTLIGHT:

How a Clawback Happens

Here's what to expect when working through a financial fraud clawback.

Fraud Reported to At-Bay

STEP 01

Policyholder contacts At-Bay. The Claims team is activated immediately and provides instructions on exactly what the policyholder needs to do for the Claims team to initiate the recovery process.

Banks and Law Enforcement Notified

STEP 02

The adjuster works directly with the insured to collect all the necessary information required to notify any/all banks involved in the fraudulent transfer, as well as any relevant law enforcement agencies. Time elapsed since transfer is the single most important variable at this stage. The sooner the insured can provide At-Bay with the transaction details, the better the chance of recovery.

Bank Intervention and Investigation

STEP 03

Proactive follow up with the banks ensures that the banks prioritize the efforts necessary to trace, identify, and freeze the stolen funds. If funds have moved, the team traces the chain of transfers through coordination with receiving banks, correspondent banks, and, where applicable, international banks and law enforcement agencies.

Recovery or Escalation

STEP 04

Frozen funds are recovered and returned to the insured. Legal counsel may be engaged if litigation is needed to compel recovery.

Resolution

STEP 05

Claim is resolved with full, partial, or no recovery. Remaining losses, including unrecovered lost funds, are covered per policy terms. The faster fraud is reported the higher likelihood that some funds will be recovered (see Figure 39).

Third-Party Liability

CHAPTER

04

Third-Party Liability Exploded in 2025

Litigation is emerging as a threat in its own right, sometimes trailing a ransomware attack or data breach, sometimes arriving with no underlying incident at all for defendants. Third-party liability claims jumped 70% in 2025, the largest increase of any incident type we track.

In 2025, we continued to see two primary themes: Lawsuits related to California's Invasion of Privacy Act (CIPA) were a persistent cause for claims, and class action lawsuits became more common and more aggressive.

CIPA: A Catalyst for Claims

California's Invasion of Privacy Act (CIPA) accounted for 34% of third-party liability claims in 2025, up from 26% in 2024 and 7% in 2023. CIPA liability typically arises from tracking technologies embedded in websites that capture user data without proper consent. Many companies believe their cookie banners and opt-in mechanisms are compliant. Attorneys are informing them otherwise.

FIGURE 40

Claims Related to CIPA Are a Persistent Presence in Our Dataset

Percentage of Third-Party Liability Claims Related to CIPA

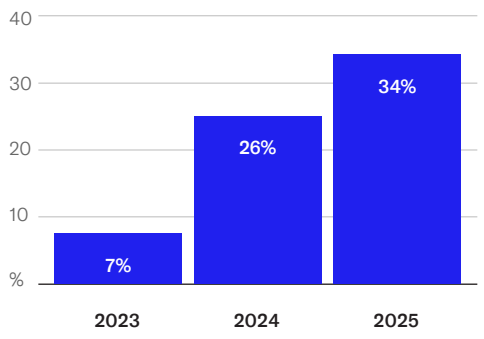
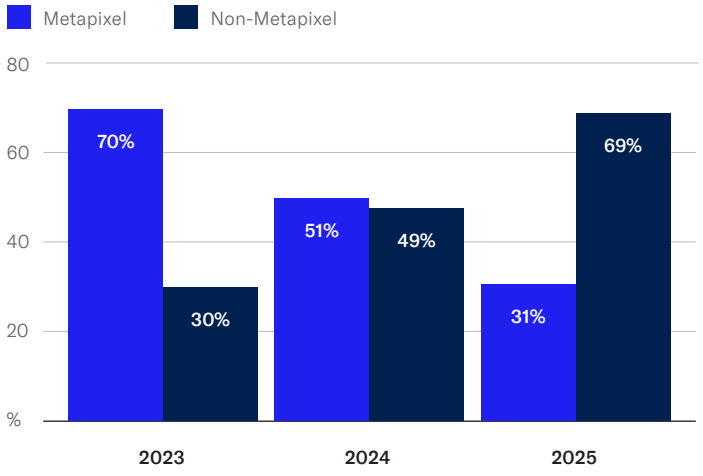


FIGURE 41

Higher Percentage of CIPA Claims Unrelated to Meta Pixel in 2025

Percentage of Meta Pixel Claims vs. Non-Meta Pixel Claims



The risk first emerged in late 2023 through Meta Pixel, a website analytics and advertising tool used to track visitor behavior, which was found capturing sensitive user data without adequate disclosure. Since then, the playbook expanded to LinkedIn, TikTok, and other tracking tools throughout 2025, shifting from 70% Meta Pixel-related cases in 2023 to 69% non-Meta Pixel in 2025. More tracking tools mean more exposure.

This isn't going away. Plaintiffs' attorneys have found a reliable mechanism to extract settlement payments from companies using these technologies and will keep using it. For businesses, it's good practice to ensure the technology is properly configured and operating as intended.

Class Action Lawsuits

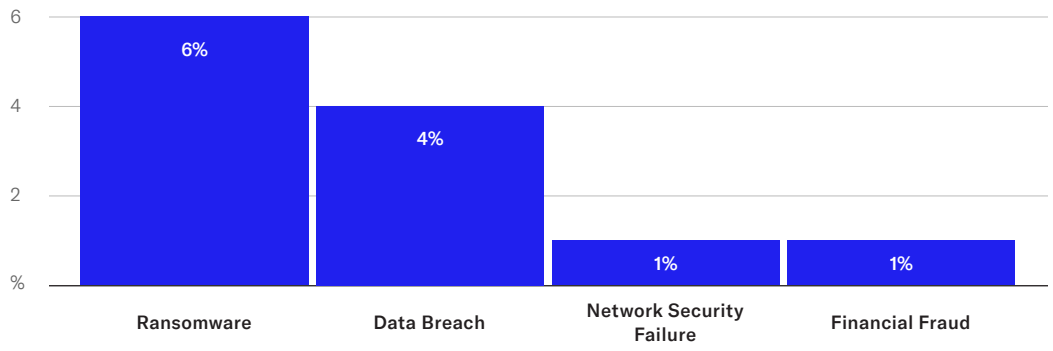
Class action lawsuits were an ongoing driver of third-party liability claims in 2025, and we expect the number to grow well into 2026. Unlike a cyber attack, class actions often have a delayed fuse and arise after the initial cyber threat has resolved.

Class actions are becoming more common and more aggressive. The threshold for filing has dropped. Plaintiffs' attorneys are organizing faster, and cases that once included tens to hundreds of thousands of impacted individuals are now being filed with far fewer, according to our claims data. Often, multiple class actions are filed simultaneously for the same incident, driving up costs and complexity, which impacts the cost. Often, the more class actions filed per incident, the more expensive they are to resolve.

FIGURE 42

Ransomware Incidents Saw the Highest Percentage of Class Action Lawsuits

Percentage of Class Action Lawsuits by Incident Type, 2023-2024



Due to the length of time these claims take to develop, we looked at 2023 and 2024 claims data to understand which incident types are the most likely to trigger a class action lawsuit. Ransomware and data breach topped the charts, with 6% of ransomware claims and 4% of data breach claims eventually seeing such legal action. While these numbers may not be large, class action litigation is notoriously high stakes because of the significant costs and losses at play.

What makes this particularly brutal for businesses is the timing. A company that has already spent months rebuilding systems, notifying customers, and managing reputational fallout after an attack can find itself served with a class action just as business is finally getting back to normal. Litigation is a multi-year process marked by significant defense costs, distraction within the business, and public scrutiny.

Insurance is a safety net, not a shield. While having the right insurance coverage can help make businesses financially whole after an attack, it may not help them avoid a cyber incident-related class action lawsuit that can prolong the pain and cost. The only true prevention is avoiding a cyber incident altogether.

Anatomy of a Data Breach Class Action

Breach Occurs

PHASE 01

Systems are compromised.
Data (customer records, PII, payment information) is accessed or exfiltrated.

Investigation

PHASE 02

The forensic investigation helps determine which individuals require notification. Regulators and affected individuals are notified in accordance with state and federal requirements. Often, plaintiffs' attorneys learn of the breach for the first time via State Attorney General websites.

Attorneys Mobilize

PHASE 03

Plaintiffs' firms often rely on Attorney General websites and utilize social media to recruit affected individuals and file suit. Generally this means investigation and notifications precede mobilization.

Lawsuit Filed

PHASE 04

A class action complaint is filed, typically alleging negligence, failure to safeguard data, and/or statutory violations. If media coverage follows, and/or multiple class actions are filed, the complexity and cost increases. Courts consolidate claims with multiple class actions into one lawsuit.

Motion Practice and Initial Discovery

PHASE 05

If a motion to dismiss succeeds, the case ends. However, plaintiffs commonly refile the case after curing defects pointed out by the court in its dismissal. Parties often discuss early settlement/ mediation with informal discovery to confirm the class size.

Settlement Negotiations or Continued Litigation

PHASE 06

Most cases settle after several rounds of discussions. This can take six months to several years. Settlement amounts are driven by class size, data sensitivity, and the defendant's perceived security failures. Absent early settlement, varied motion practice, and broad discovery, (including additional motion practice, document production, depositions, and expert witnesses) occur in earnest, driving up significant legal fees that reflect the level of activity in the case.

Resolution

PHASE 07

All class action settlements require Court approval. Costs include ongoing defense fees, administrative costs to process the settlement including the enrollment process for class benefits, settlement payout, and ongoing reputational damage. The resolution process once settlement is reached spans months. These lawsuits can stretch on for years, incurring costs and fees until they are closed.

What the Data Tells Us

CHAPTER

05

What the Data Tells Us

The data in this report points in one direction: Cyber risk is getting harder to avoid and more expensive to absorb. Claims frequency has now risen for three consecutive years. Average severity hit an all-time high. Ransomware and financial fraud continue to wreak havoc.

Looking ahead, we don't expect meaningful relief. The conditions that drove 2025's claims environment are structural, not episodic.

Akira was 2025's defining story in ransomware, but the underlying weaknesses they exploited are not distinct to the SonicWall devices that they appear to have targeted.

The shift toward infrastructure-based, automated exploitation has been building for several years. Organizations that haven't addressed their remote access exposure will continue to see elevated risks, regardless of the maker of the network devices they're operating.

In financial fraud, the AI-assisted sophistication of phishing and business email compromise is not a future concern, it is the present one.

The 16% increase in average stolen funds reflects attackers who are getting better at identifying high-value targets, crafting contextually appropriate messages, and moving funds faster before anyone can intervene. The fraud campaigns we see in the years ahead will be harder to distinguish from legitimate communications than the ones we see today.

In third-party liability, the legal ecosystem around data privacy and breach notification is still accelerating.

Class action thresholds are dropping. Plaintiffs' attorneys are organizing faster. Businesses that haven't audited their tracking technology stack for compliance are building undisclosed liability while their finance teams budget for other risks.

Against this backdrop, we believe the most important strategic decision a business can make isn't which specific control to deploy first, but whether they have the right partners in place to respond.

The data in this report shows what that looks like in practice. Every business in our portfolio that faced an Akira attack but was not encrypted shared one thing in common: They had high-fidelity Managed Detection and Response monitoring their environment around the clock. By high-fidelity, we mean actual human experts watching the network, identifying lateral movement at 1 a.m. on a Saturday, and responding before encryption could complete. That is what converts an existential threat into a minor nuisance.

The same logic applies to financial fraud. Our Claims team recovered $56M in stolen funds in 2025, but nearly all of it came from incidents reported quickly where we could put our proven process to work to recover funds. Partnering with an insurance provider who has a dedicated clawback team, established banking relationships, and defined escalation protocols is the deciding factor.

And for the businesses that suffer an attack and then face litigation, having experienced legal counsel embedded in the claims response from the start can mitigate exposure meaningfully.

The consistent theme is that outcomes are not randomly distributed. They are shaped by the decisions that organizations make before a crisis begins: about which tools they run, about who will maintain and operate those tools, about who they call first when something goes wrong, and about how quickly they escalate. The businesses that fare best among our insureds are not the ones that simply got lucky, they are the ones that took steps to ensure their cyber resilience wouldn't fail.

Cyber risk is not going away. But it is manageable. The evidence in this report shows that key activities, when managed well, largely counteract the effectiveness of sophisticated adversaries operating at scale. That is the case for investing in the right controls, the right partnerships, and the right insurance.

Methodology

At-Bay's analysis is based on claims data for policies placed through and serviced by At-Bay Insurance Services, LLC from 2021 through the first quarter of 2026. By analyzing actual claims data, the At-Bay Research team set out to answer these questions:

- *How have cyber attacks and threat actors evolved?*
- *What is the actual cost of a cyber incident for businesses?*
- *Where can businesses focus their efforts to better protect their livelihoods?*

This data was collected from At-Bay policyholders during initial underwriting, throughout the policy year, as well as when their claims were processed by our team in the wake of an incident.

A Note About Our Revenue Bands

While At-Bay helps place insurance for businesses with up to $5B in revenue, and these insureds are included in the data, labeling the largest revenue band group "$100M-$500M" more accurately captures the size of risk represented.

How We Calculate Severity For This Report

Severity calculations include the total incurred loss of a ransomware claim, with development to ultimate selected using actuarial methods leveraging historical experience. The losses considered can include, but are not limited to, ransom paid, recovery and restoration costs, such as procuring new servers, computers, or deploying entire new network architectures; third-party consultancy costs like digital forensics and incident response professionals; business interruption expenses; and legal expenses, particularly if personally identifiable information was compromised.

Contributors

Adam Tyra
CISO for Customers

Ayelet Kutner
Chief Technology Officer

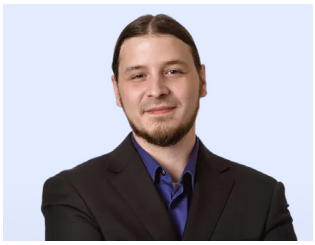
Cameron Pitts
Senior Content Marketing Manager

Chin Chang
Senior Manager, Risk Analytics

Laura Hawkins
AVP, Claims

Laurie Iacono
Director, Threat Intelligence

Michael Lowe
Head of Marketing



Mike Scutt
Vice President, MDR Security Operations

Rebecca Jarrett
Head of Claims Operations at At-Bay

Ronit Suzan
Product Specialist

Samantha Wong
Senior Risk Analyst

About At-Bay + InsurSec Report

At-Bay is the InsurSec provider for the digital age, helping businesses mitigate cyber risk and avoid incidents by continuously analyzing data from security scans and collecting cyber threat intelligence and the relevant details of security incidents reported by insureds. Because we can correlate information about a significant number of real-world incidents with data about the victim's technology environment before the incident occurred, this enables us to reliably identify trends and relationships that other companies and security vendors cannot. We're able to clearly identify security controls t hat mitigate risk, differentiate them from security controls that don't mitigate risk, and prove our case with empirical data from actual incidents where those security controls were in place.

Our goal is to share our findings on the respective impacts of a range of security controls with the public at large. We believe we can use facts and evidence to cut through the noise of a crowded cybersecurity marketplace and enable organizations to deploy scarce cybersecurity resources for maximum impact. We regularly develop and share a slate of statistically provable leading practices for security that can be readily consumed by organizations regardless of headcount or the size of their security budget.

The information contained is for general guidance on matters of interest only and is not intended to construe or the rendering of professional services of any kind. If professional advice is required, the services of a professional should be sought. All information is provided as is with no guarantee or warranty of any kind, express or implied, concerning the completeness, accuracy, usefulness, timeliness of the information provided. At-Bay is not responsible for any errors or omissions, or for the results obtained from the use of the information provided in these materials. This report post includes links to third-party websites. These links are provided as a convenience only. At-Bay does not endorse, have control over, or assume responsibility or liability for the content, privacy policy, or practices of any such third-party websites. At-Bay Insurance Services LLC, a wholly owned subsidiary of At-Bay, Inc., is a licensed insurance agency and surplus lines broker in all fifty states and the District of Columbia.

©4/2026 At-Bay. All Rights Reserved.