at bay

The 2025

InsurSec Report

All Claims Edition

at-bay.com

An analysis of At-Bay claims and cybercrime data

Table of Contents

Introduction	4
Key Findings	5
Chapter 1: The Cyberthreat Landscape	6
Chapter 2: Ransomware Continues to Rise	12
Chapter 3: Third Party Risks Are Here to Stay	19
Chapter 4: Financial Fraud Still the Most Frequent Incident	23
Looking Ahead	27
Methodology	29
Contributors	30

Introduction

In this year's edition of At-Bay's InsurSec report, our intent is to use our distinctive insights derived from cyber incidents suffered by insureds with policies placed by At-Bay to illuminate the relationship between technology choices and underlying risk. Our hope is that we will drive better security outcomes for businesses by clearly connecting these two concepts and showing how they contribute to losses.

To this end, our data contains two clear takeaways. First, the technologies that businesses choose to deploy have a direct impact on the attention that attackers will (or won't) devote to them. Poor choices here will significantly increase the likelihood of a direct attack and will also increase the probability that a business will suffer losses from cyber incidents of all types in a given year.

Note that the set of technology choices that matter also includes decisions about whether or not to do business with other companies that will bring the consequences of their own technology choices into the relationship.

To help explain this, we've expanded on the analysis of indirect ransomware attacks from last year's report to now also consider a variety of loss scenarios attributable to third party relationships collectively addressed in this year's report as third-party risks.

The second takeaway from our data is that security controls work. When demonstrably effective controls are selected, configured appropriately, deployed comprehensively throughout the environment, and maintained over time, there is a clear reduction in the losses experienced by the businesses that are operating them.

We hope that this second point will be vindicating for many of our readers while also reducing the anxiety of others. While the pace of technology development exceeds the ability of many business leaders to understand the future impact to their organizations (e.g., what will happen as generative AI becomes pervasive), old ideas in cybersecurity still work just fine when faithfully implemented. Strong encryption still protects data from disclosure. Multi-factor authentication still prevents attackers from making use of compromised credentials. And, market-leading Endpoint Detection and Response (EDR) tools managed by competent professionals are still highly effective at detecting and stopping malicious activity when other controls have fallen short.

For our second annual InsurSec Report, we've analyzed a year's worth of real-world claims data to understand these and other issues. We've blended our claims and loss data with independent threat research conducted by our in-house cybersecurity teams. And, we've done our best to craft the collected insights into an actionable story that can help readers apply the lessons of 2024 to create a more resilient 2025 and beyond.

Key Findings

1 **OVERALL CLAIM FREQUENCY INCREASED BY 16% IN 2024.**

Financial fraud continued to be the most common cyberattack, keeping frequency high. However, lower severity financial fraud claims pushed down average severity by 5% to $166K.

2 **EMAIL CONTINUES TO BE THE MOST COMMON INITIAL ENTRY VECTOR, TRIGGERING 43% OF CLAIMS.**

83% of financial fraud claims began with an email attack, while email was only exploited in 6% of ransomware cases.

3 **DIRECT RANSOMWARE CLAIM FREQUENCY RETURNED TO 2021 LEVELS, AN INCREASE OF 19% YOY.**

Companies with $25-$100M in revenue were hit the hardest, seeing a 46% increase in frequency and 47% increase in severity.

4 **REMOTE ACCESS TOOLS WERE THE INITIAL ENTRY VECTOR FOR 80% OF DIRECT RANSOMWARE CLAIMS.**

The majority of ransomware started with an attack on a remote access tool (either VPN, RDP or other remote access tool), up from 63% last year.

5 **SUPPLY CHAIN RISK CONTINUES TO RISE AS INDIRECT RANSOMWARE CLAIM FREQUENCY INCREASED BY 43%.**

For the second year in a row, the majority of indirect ransomware claims were driven by a single large scale event (CDK Global).

DIRECT VS. INDIRECT RANSOMWARE

For the purposes of this report, we distinguish between two types of ransomware incidents. We define them as:

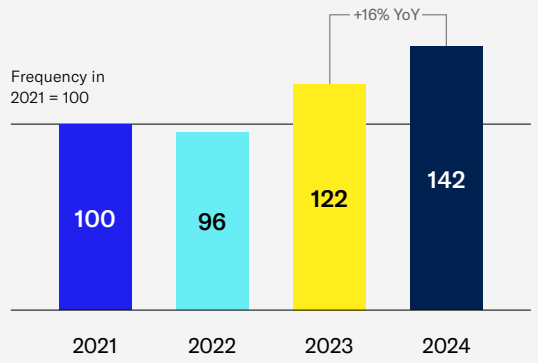
- **Direct Ransomware**: A direct attack on an organization resulting in encryption and/or exfiltration of data to hold the organization to ransom.
- **Indirect Ransomware**: A ransomware attack on a vendor or partner of the organization which results in damages to the organization, typically data privacy breach and/or business interruption.

CHAPTER 1

The Cyberthreat Landscape

Overall Claim Frequency Increased 16%

Figure 1: Indexed Claim Frequency by Year



In 2024, claims increased by 16% year-over-year, driven mainly by three key factors.

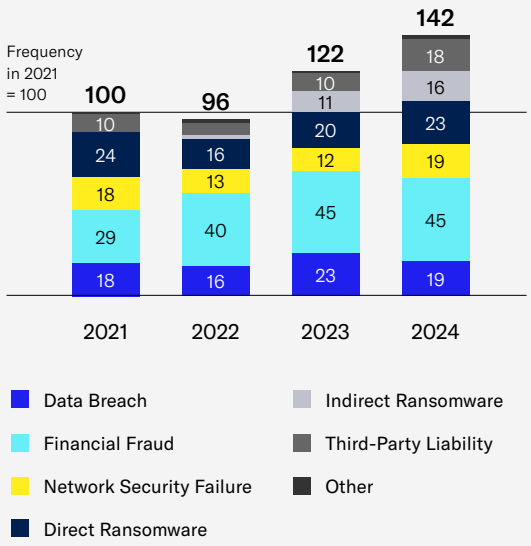
#1 Ransomware Continues to Rise

First, ransomware is on the rise for another year with a larger number of attacks executed by an increasing number of groups. In 2024, ransomware returned to 2021 levels after lower frequency years in 2022 and 2023.

We assessed at the time that the conflict in Ukraine which began in February 2022 was likely responsible for distracting Russia and Ukraine-based cyber criminal groups from their usual activities.[1]

Ransomware, Third Party Incidents Continue to Rise

Figure 2: Indexed Claim Frequency by Incident Type



This effect began reversing in 2023, and claims related to direct ransomware continued their upward climb for a second year in 2024 (up 19%), returning to 2021 levels.

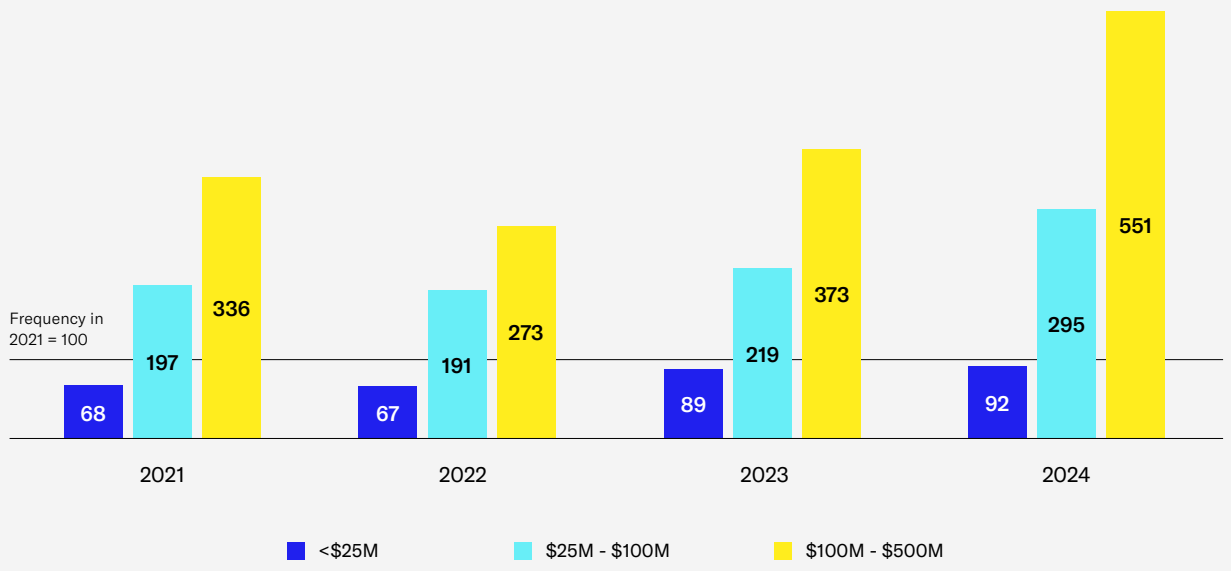
#2 Third Party Incidents Are Here to Stay — with an Increasing Blast Radius

The second factor that had a significant impact on claims for 2024 was the strong increase in usage of

[1] Russian Military Cyber Actors Target US and Global Critical Infrastructure, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

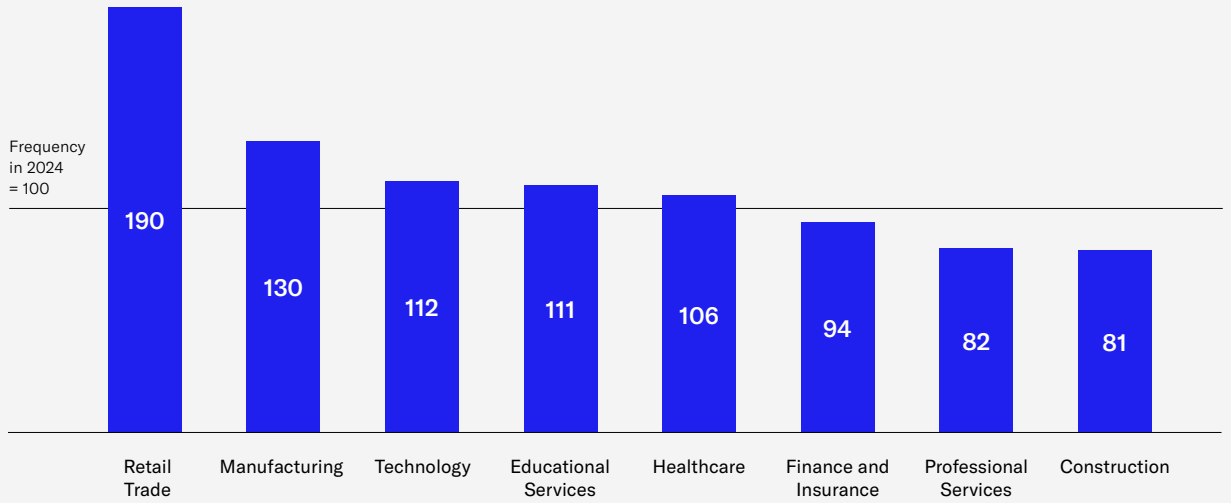
Claim Frequency Increased Across All Revenue Bands

Figure 3: Indexed Claim Frequency by Revenue Band



Retail Trade and Manufacturing Saw the Highest Claim Frequency in 2024

Figure 4: Indexed Claims Frequency by Industry, 2024



insurance to mitigate the effects of cyber attacks experienced by third parties.

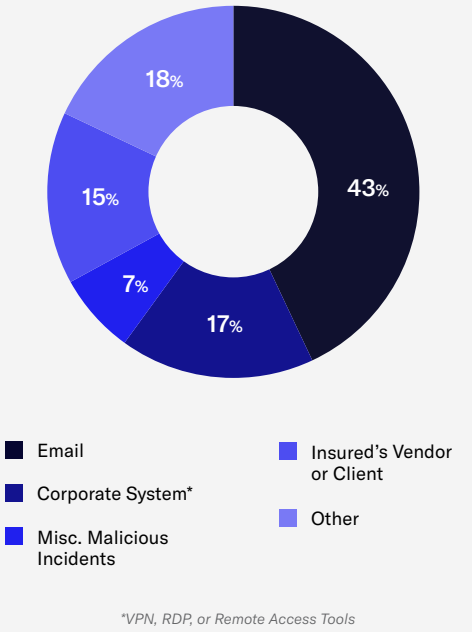
These incidents are counted in our data under multiple categories, including indirect ransomware (an incident where an organization is indirectly impacted by a cyber event on their vendor or partner), which saw a 43% increase in 2024 (see Chapter 4 for more on indirect ransomware).

But, they share one important characteristic: At-Bay's insureds filed these claims after suffering losses that are attributable to the security failures of other companies that they did business with rather than security failures in their own technology environment.

Many of these claims were filed by auto dealerships that experienced a business interruption related to the outage of CDK Global after being hit by ransomware.[2] These incidents are particularly pronounced in our largest revenue segment (Figure 3) and retail trade industry, which is inclusive of auto dealers (Figure 4).

Email Was the Most Common Initial Entry Vector in 2024

Figure 5: 2024 Claims by Initial Entry Vector



#3 Financial Fraud Remains a Common Threat

The third factor was the sustained prevalence of financial fraud incidents experienced by At-Bay insureds. Accounting for roughly a third of claims for the second year in a row, these incidents relied primarily on the abuse of email to slip carefully crafted messages past security controls and entice unwitting recipients into misdirecting funds into the hands of attackers.

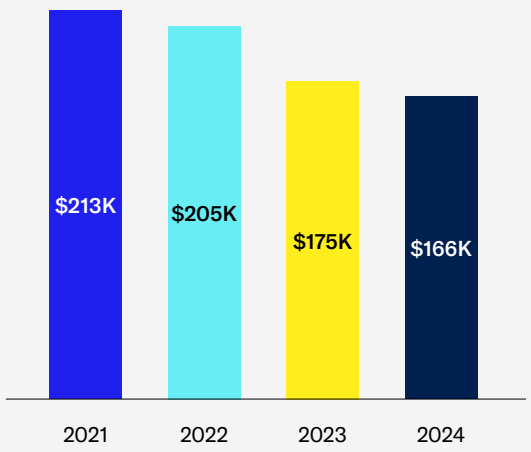
Frustratingly, most email security solutions currently available in the market demonstrate a low level of effectiveness at identifying emails that elicit fraud. And the rise of generative AI has allowed attackers to become more adept at crafting natural-sounding messages, removing many of the traditional tell-tale signs (e.g., poor word usage, misspellings, grammatical mistakes, etc.) that an email shouldn't be trusted. In 2024, email was once again the top entry vector for attackers, accounting for 43% of all claims.

These attacks are relatively less sophisticated and easier to execute compared to malware-based threats like ransomware. This means that attackers can attempt more fraud attacks faster and with lower risk than other tactics. And, when they succeed, victims may not even realize they've been defrauded for weeks or months, removing the possibility that money could be recovered.

[2] Car Dealers Grapple With Dayslong Software Outage After CDK Cyberattack, https://www.wsj.com/business/autos/cdk-cyberattack-outage-car-dealers-a0fd45ec

Average Claim Severity Dropped, a Result of More Frequent but Smaller Claims

Figure 6: Average Claim Severity by Year



While overall severity dropped in 2024 to an average of $166K, this is still a substantial sum for any small and mid-sized business. In addition, this decrease in average severity is deceptive. It is mostly due to more small incidents that are bringing averages down. Crippling incidents like ransomware have increased in both frequency and severity.

Three of the most common incident types grew in severity. Average severity for direct ransomware grew 18%, indirect ransomware rose 72%, and financial fraud increased as well, although marginally by 3% (Figure 8).

In 2024, these incidents cost businesses on average $468K, $241K, and $91K respectively. Retail trade, which includes claims from those auto dealers impacted by the CDK Global outage, led all industries with an average severity of $230K (Figure 9).

THE REAL COST OF RANSOMWARE

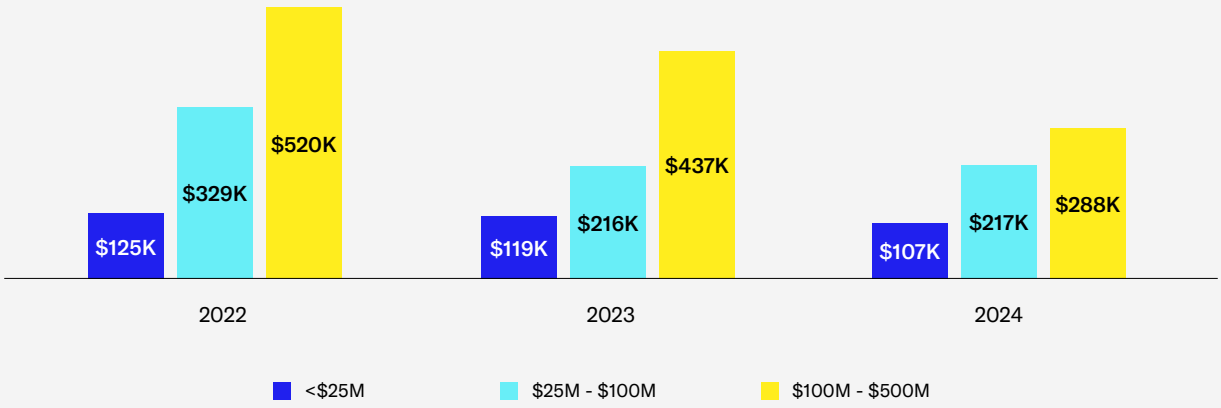
For the fourth year in a row direct ransomware led all incident types in average severity (Figure 8). This may not come as a surprise, considering the average ransom demand in 2024 was nearly $1 million, nearly 4X the average funds stolen in a financial fraud incident.

However, it's not the ransom alone that elevates severity in direct ransomware. In fact, only 31% of ransoms end up being paid (Figure 20). Severity is driven by additional losses that are part of ransomware incidents: business interruption and class action litigation, both of which are on the rise.

When a business is hit with ransomware, it often experiences business interruption due to encrypted systems. Class action lawsuits arising from data compromised in the incident are also increasing in number. These losses are pushing severity up in ransomware claims, both direct and indirect.

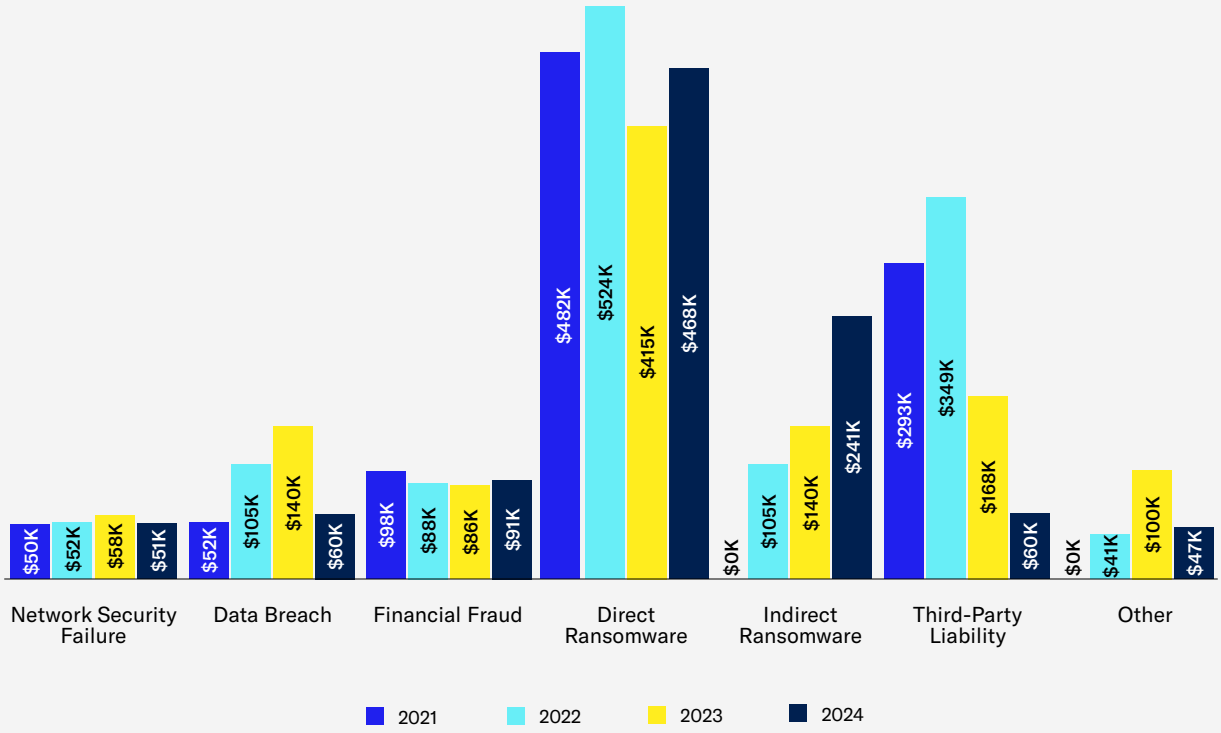
Average Claim Severity Dropped the Most Among $100M-$500M Companies

Figure 7: Average Claim Severity by Revenue Band



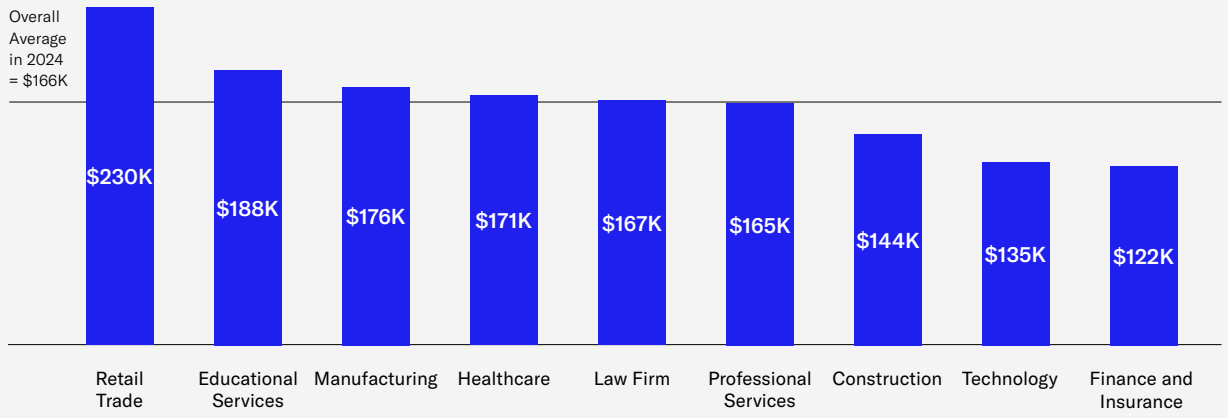
Direct Ransomware Continues to Be the Costliest Incident Type

Figure 8: Average Claim Severity by Incident Type



Retail Trade Experienced 39% Higher Severity Than Average

Figure 9: Average Claim Severity by Industry, 2024



Although email was the most frequently exploited entry vector, corporate systems, which includes VPN, RDP, or remote access tools, were the costliest at 2.4X higher severity than average. These corporate systems are the most common entry vector for ransomware, which is the costliest of all incident types.

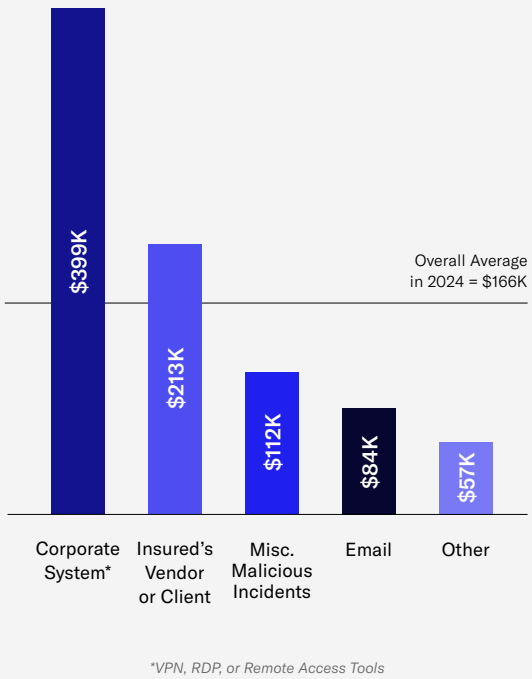
For an incident to have occurred via a corporate system, the implication is that there was an unpatched vulnerability or configuration issue that was exploited.

Companies that have one of these issues that we can see are likely to have many more that we can't (i.e. inside the perimeter). Having unpatched vulnerabilities inside the perimeter means that attackers can move laterally and deploy ransomware that will infect the environment faster while staying undetected longer.

It's less likely to be blocked by an endpoint security tool, and there is a lower probability that the victim will have a robust backup solution to use for recovery, which may contribute to higher severity.

Attacks to Corporate Servers Were 2.4X Costlier than Average

Figure 10: Claims Severity by Initial Entry Vector, 2024



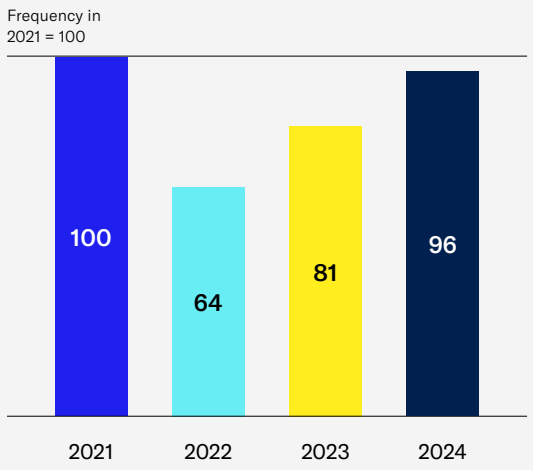
VPN, RDP, or Remote Access Tools

CHAPTER 2

Ransomware Continues to Rise

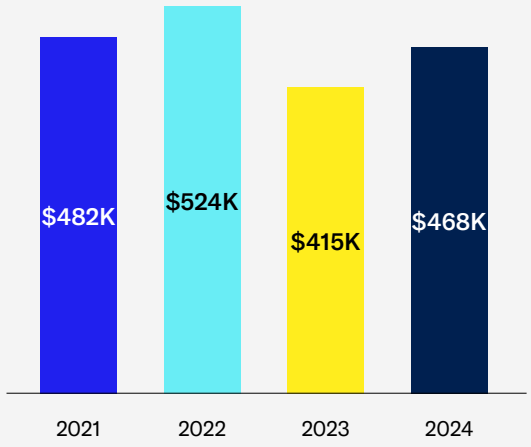
Direct Ransomware Nearly Returned to 2021 Levels

Figure 11: Indexed Direct Ransomware Claim Frequency by Year



Average Direct Ransomware Severity Was $468K in 2024

Figure 12: Direct Ransomware Severity by Year



At-Bay insureds experienced 19% more direct ransomware incidents in 2024 compared to 2023. The average severity of direct ransomware incidents also increased by 13% to $468K.

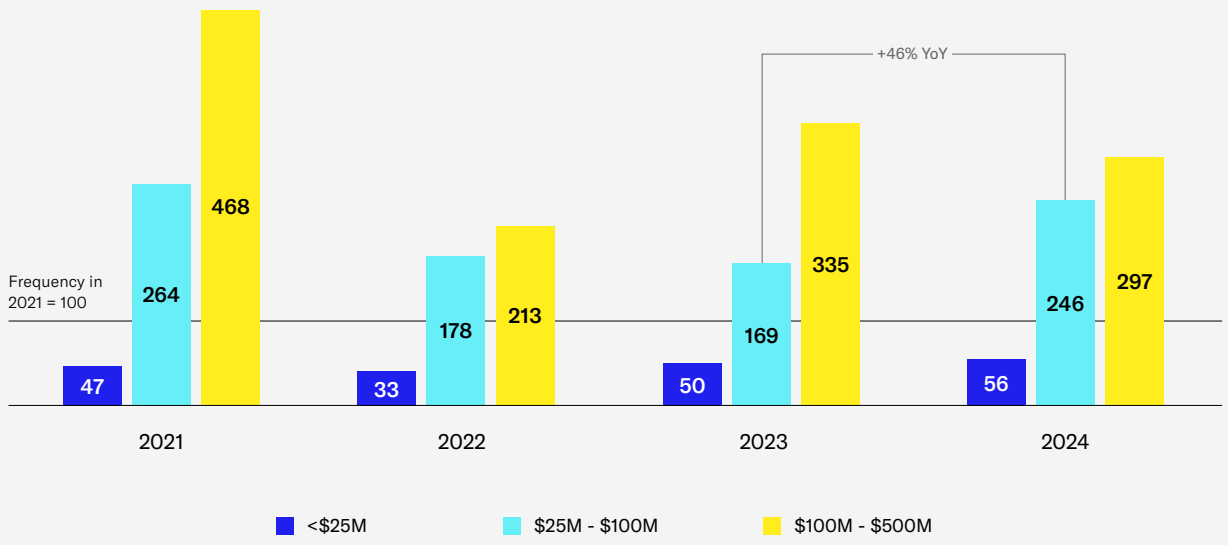
The segment of companies with revenue from $25-$100M saw the largest increase in claims for direct ransomware with approximately 46% more of these ransomware claims for 2024 as compared to 2023 (Figure 13). This same group also saw the largest increase in severity, 47% YoY (Figure 14).

This coincides with an overall increase in attacker activity year over year but also implies that attackers may be intentionally focusing on companies of this size.

The overall picture for direct ransomware tells us that attackers likely feel that they've identified a winning playbook in the tactics that they began adopting in 2022 and 2023 and are doubling down by targeting their attacks at victims who are less resilient to attack and more likely to pay extortion demands.

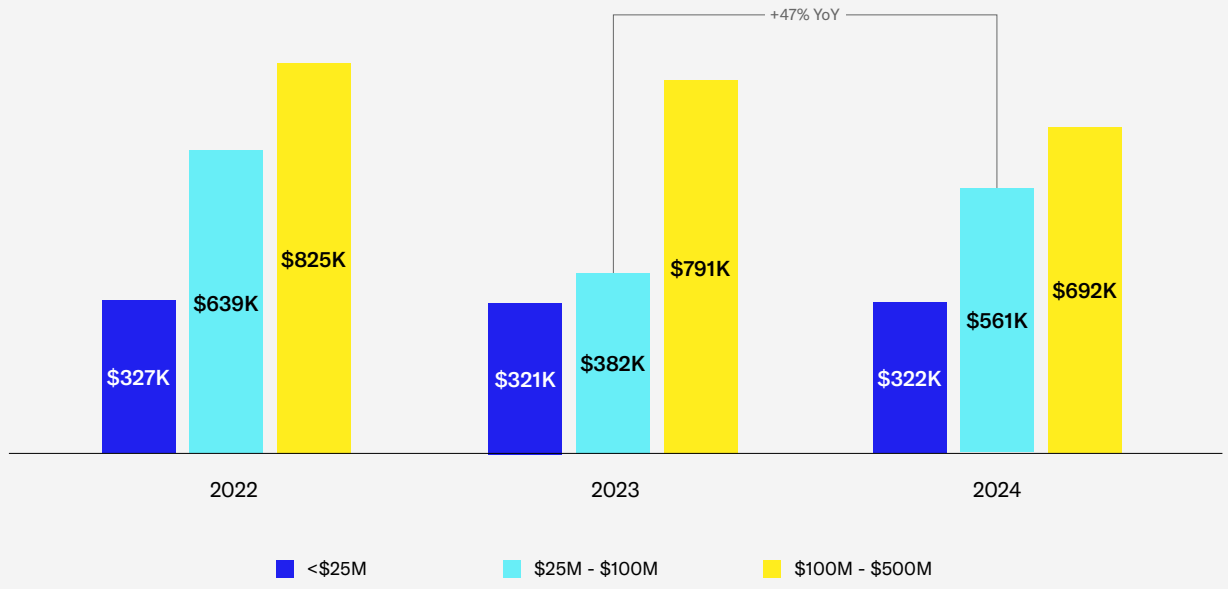
Mid-Sized Companies Saw a 46% Increase in Direct Ransomware Claim Frequency

Figure 13: Indexed Direct Ransomware Claim Frequency by Revenue Band



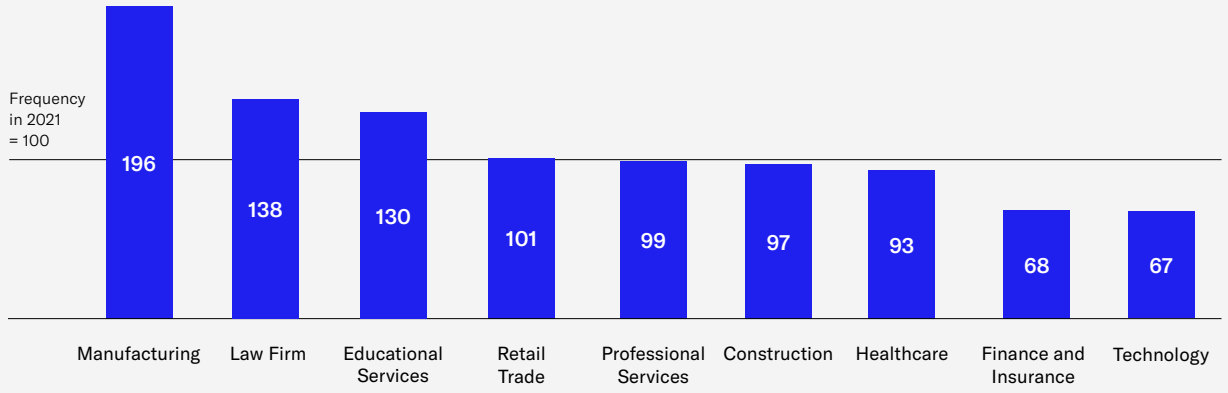
Mid-Sized Companies Saw a 47% Increase in Direct Ransomware Severity

Figure 14: Direct Ransomware Severity by Revenue Band



Manufacturing Industry Hit Most Frequently by Direct Ransomware

Figure 15: Indexed Direct Ransomware Claim Frequency by Industry, 2024



The distribution of ransomware claims in 2024 compared to previous years tells us that attackers are becoming increasingly adept at identifying and attacking victims that they identify as security laggards. We can see that certain segments of At-Bay insureds are clearly suffering disproportionate losses compared to other segments.

Manufacturers, for example, saw the highest claim frequency for any industry by far, experiencing nearly 2X claim frequency compared to the average.

Notably, these elevated averages for the Manufacturing segment were not driven by any single event during 2024 that can explain an increase in claim frequency in the way that the CDK Global incident can be implicated for the significant bump in incidents impacting the Retail Trade segment (Figure 24).

Instead, the disparity can be explained as a combined function of security technology selection and security culture common to each industry segment, a collection of factors that attackers can either see directly or infer.

Healthcare organizations, for example, can be expected to deploy a suite of security controls that correspond with the requirements of HIPAA. Financial services companies also tend to have significant legal and regulatory obligations for safeguarding customer data that necessitate the adoption of relatively sophisticated security controls.

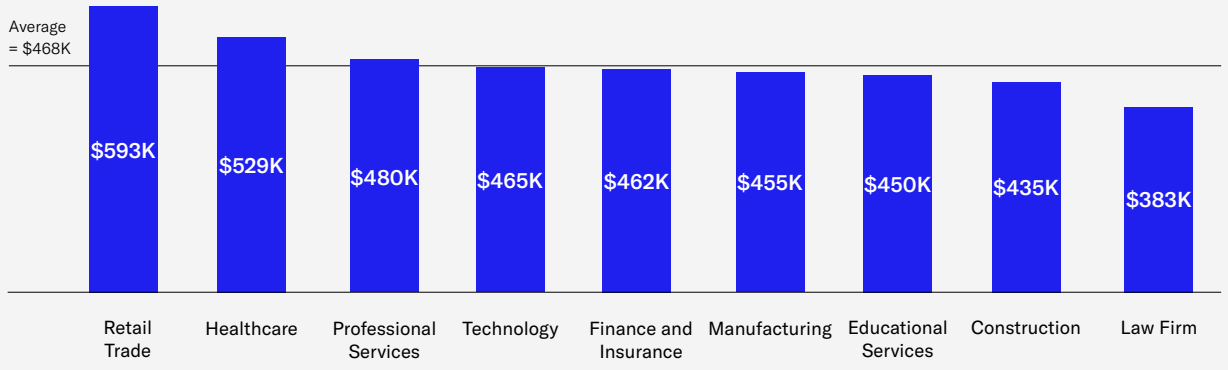
Manufacturers, on the other hand, are not generally subject to any industry-level cybersecurity regulations. They are therefore less likely to adopt any particular security control than other, more regulated industries and also more likely to continue operating older security technologies that may no longer be considered suitable in other segments.

Security culture has a role to play as well. In a phone-based survey of security leaders among our manufacturing customers conducted in the fall of 2024, the most common reason cited for the adoption of individual security controls was, “The control was required to obtain insurance.”[3]

[3] Research conducted by the Stance Advisory Services team

Retail Trade Experienced 22% Higher Severity Than Average

Figure 16: Direct Ransomware Severity by Industry, 2024



Organizations that are adopting controls at the direction of a vendor rather than as part of a holistic risk management effort likely aren't making the investment necessary to sustain the effectiveness of these controls over time.

While attackers can't always get the full picture of a company's vulnerability to attack, they can rely on useful proxies for this. For another year, we see that attackers are continuing to focus on companies that operate specific, high-risk technologies.

At-Bay has previously reported on the correlation between the rate of occurrence and severity of claims and the presence of certain high-risk legacy platforms such as on-premises Microsoft Exchange and VPN appliances from Cisco, Citrix, SonicWall, and Fortinet.

Indeed, VPN, RDP and other remote access tools accounted for the lion's share of entry vectors for direct ransomware at 80%, up from 63% in 2023 (Figure 17).

While many companies have opted to transition away from these and other, similarly risky platforms, the ones that are still operating them are attracting a high level of interest from attackers.

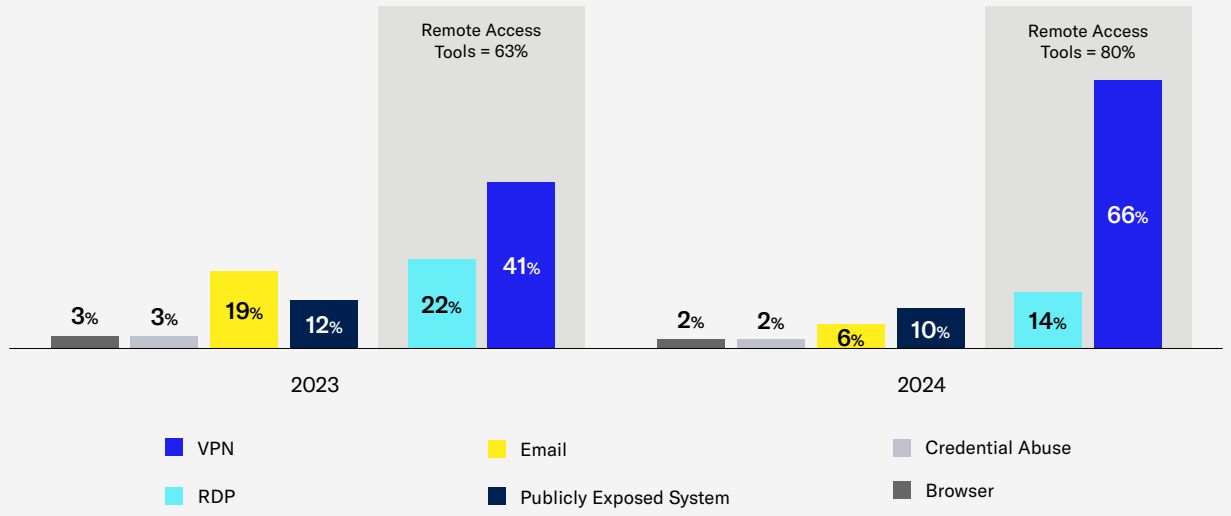
THE BACKUP WAKE-UP CALL

We previously observed the impact that neglect can have on control efficacy with one specific type of control: backup solutions. In 2023, we noted that while more than 90% of insureds reported having offline backups in place, only about 1 in 4 of them were able to use backups to recover successfully from the effects of a cyber incident. In response, At-Bay increased its engagement with customers on the topic of effective backup solution management.[4] This resulted in an increase in insureds' ability to use their backups to successfully recover from incidents as described in the 2024 edition of our InsurSec report.

[4] Data Collected for At-Bay's Backup Breakdown: How Data Recovery Impacts the Outcome of Cyber Attacks; October 2023

Remote Access Was the Entry Vector for 80% of Direct Ransomware Attacks

Figure 17: Direct Ransomware Initial Entry Vector by Year



One ransomware group, Black Basta, has even developed an attack tool that specifically targets some of the technologies considered high risk by At-Bay for the purpose of delivering automated credential stuffing attacks.

Unsurprisingly, we note that our manufacturing customers were 60% more likely than our average insured to be operating a VPN solution that At-Bay considered high risk.

Criminals likely assume that an organization operating a legacy VPN solution probably also has other outdated and vulnerable technologies in their environment, and are therefore using that characteristic as a reliable target identifier.

This explains the increasing severity of claims in cases where attacks successfully progress from a network security failure to a full-blown ransomware attack while the severity across claims of all types has declined slightly.

There is one other factor that is likely to be influencing claim severity for ransomware in particular. It's possible that the steadily fragmenting ransomware ecosystem is driving the severity of ransomware claims of all types by contributing to a breakdown in previously observed norms and customs among ransomware groups.

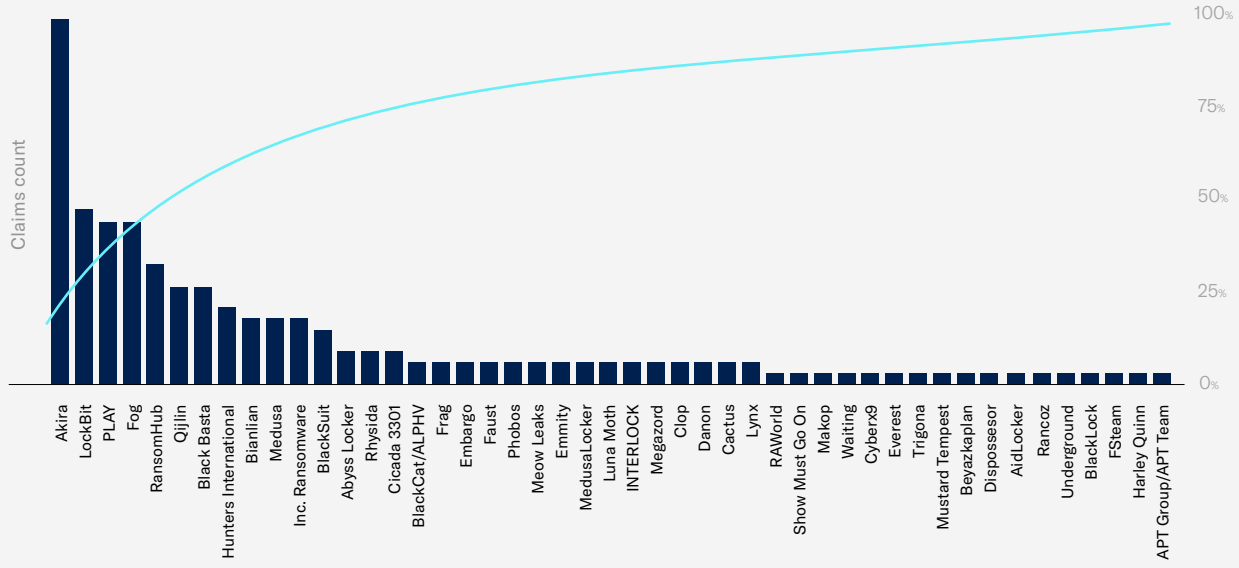
At-Bay previously noted the emergence of tactics such as double leverage attacks that increase the likelihood and amount that victims will pay.[5] These new approaches from attackers coincide with an overall erosion of reliability among criminal groups.

The number of identifiable cyber criminal groups has expanded in recent years. In 2021, ransomware claims were attributed to just 16 distinct groups, growing to 41 in 2023. In 2024, At-Bay saw 47 distinct groups (Figure 18).

[5] The 2024 InsurSec Report, Ransomware Edition, At-Bay

Ransomware Groups Grew to 47, Up 15%

Figure 18: Prevalence of Direct Ransomware Strains Among Claims, 2024



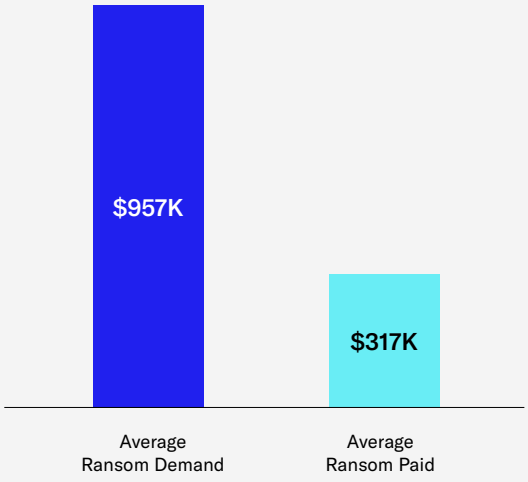
In previous years, the perceived reliability of a criminal group was a significant factor for victims in determining whether to pay extortion demands. Victims were naturally reluctant to pay ransom demands for groups that were observed to not hand over decryptor tools as promised or leak stolen data after saying they wouldn't.

However, with the explosion in the number of ransomware groups and affiliates currently operating, victims can be less sure of who they're actually dealing with, and the threat actors themselves have less incentive to preserve the reputation of their affiliated group, since they can simply reaffiliate or rename themselves tomorrow.

This means that criminal groups in 2024 were, on average, less shy about demanding outsized ransoms and less likely to see good-faith negotiation as a necessary element of the interaction with victims.

Average Ransom Paid Was $317K in 2024

Figure 19: Average Ransom Demand and Payment, 2024



The average ransom paid in 2024 was up ~12% from 2023 to $317K, even though ransoms were paid only 31% of the time.

> In 2024, At-Bay helped customers avoid paying **$146M** in ransoms.

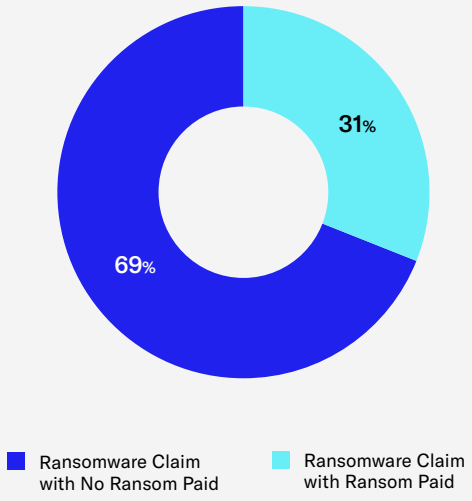
This perceived loss of reliability is supported by the discovery by law enforcement of a trove of victim data among evidence seized during the Lockbit takedown.

While Lockbit had assured many of its victims that stolen data would be deleted after their extortion demands were met, they failed to do so.[6]

This revelation seemingly confirmed the worst fears of blackmail victims everywhere: Stolen data is simply too valuable to destroy after victims prove that they're willing to pay to keep it secret.

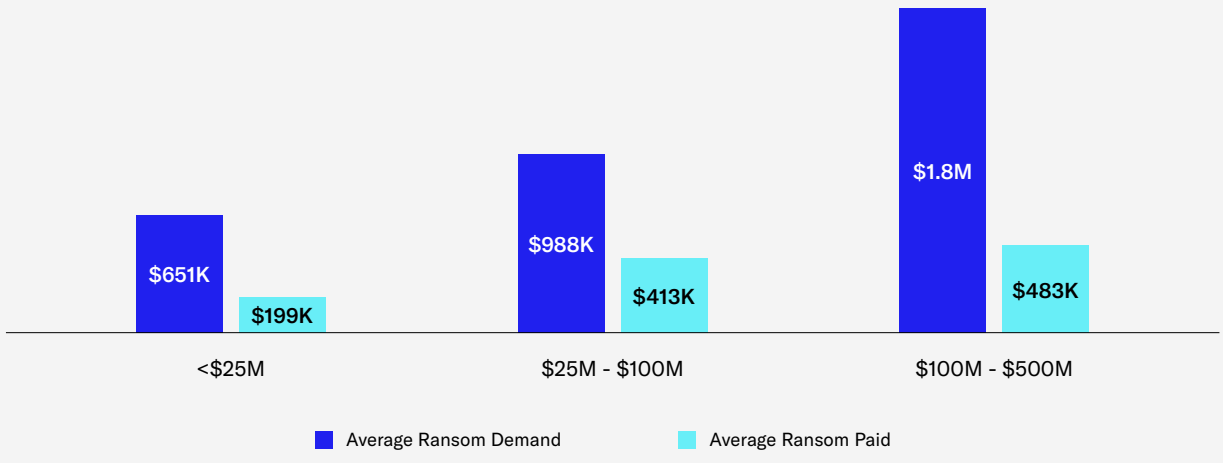
Only 31% of Ransom Demands Resulted in an Actual Ransom Payment

Figure 20: Direct Ransomware Claims With a Ransom Paid, 2024



Even the Smallest Companies Paid Six Figure Ransoms on Average

Figure 21: Average Direct Ransomware Demands and Payments by Revenue Band, 2024



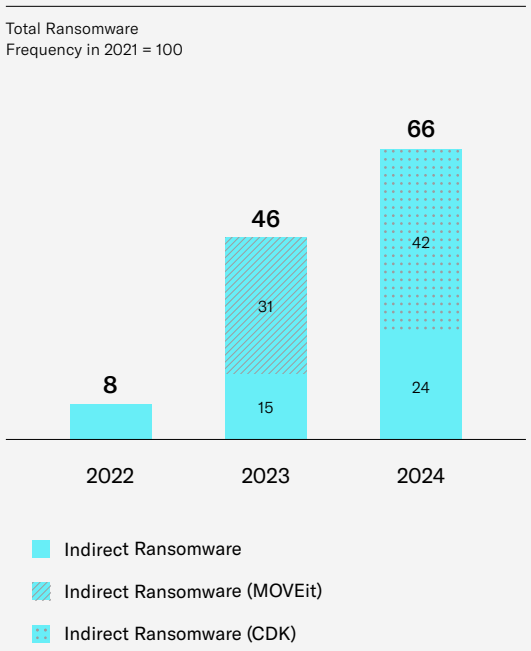
[6] LockBit held victims' data even after receiving ransom payments to delete it, https://therecord.media/lockbit-lied-about-deleting-exfiltrated-data-after-ransom-payments

CHAPTER 3

Third Party Risks Are Here to Stay

Indirect Ransomware Incidents Continue to Rise

Figure 22: Indexed Indirect Ransomware Claim Frequency by Year



While not the biggest loss category for At-Bay in 2024, third party incidents have nevertheless seen massive growth in the previous three years with losses manifesting in difficult-to-predict ways.

We began tracking indirect ransomware (an incident where an organization is indirectly impacted by a cyber event on their vendor or partner) in the last edition of our InsurSec Report, and we have continued to see aggregation events impact industries at large.

In 2023, an attack on the file transfer software MOVEit commonly used among higher education institutions led to widespread data privacy breaches.

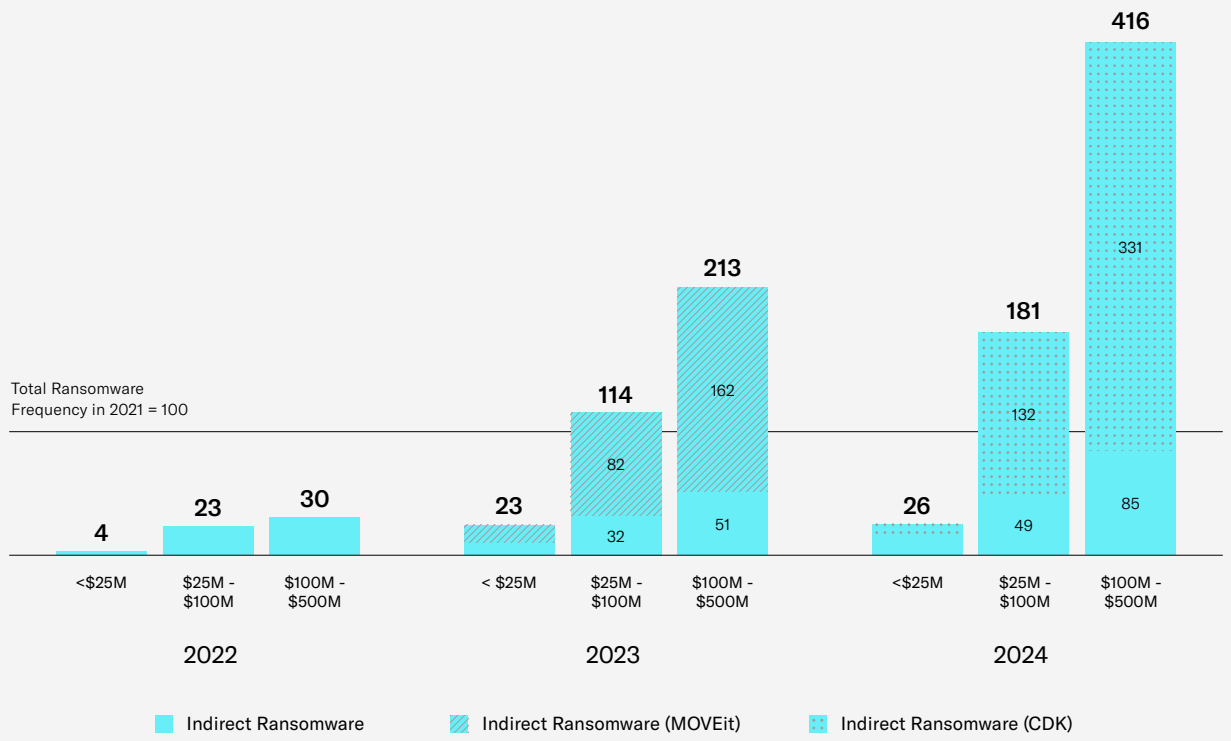
In 2024, a ransomware attack shut down CDK Global, preventing their auto dealership customers from conducting business, resulting in massive operational losses.

Third party losses occur in a variety of ways and can be seen in the average severity discrepancy between 2023 and 2024. The MOVEit event in 2023 mainly resulted in data privacy breaches, which were far less costly than the business interruption losses felt by auto dealerships due to the CDK outage (Figure 25).

Third party risks, historically considered something of an afterthought by cybersecurity teams, are capturing an increasing share of the overall risk related to technology usage for businesses. These losses are on the rise due to the increasing reliance of companies on cloud-based technology solutions.

CDK Outage Hit Auto Dealers $100M-$500M Especially Hard

Figure 23: Indexed Indirect Ransomware Claim Frequency by Revenue Band



And, the blast radius is growing for these incidents. The single biggest driver of the claims increase in the segment of companies with between $100M-$500M in revenue was the CDK Global incident.

The fact that a single event could create such outsized impact in skewing the distribution of claims among At-Bay customers underpins our opinion that the risk of third party security incidents warrants a leading position on the agenda of risk leaders for 2025 and beyond.

The current growth in third party cyber risks has its origin in the pandemic-era scramble among businesses to accommodate new ways of working.

Under significant pressure to continue operations in the midst of social distancing and lock-downs, companies were forced to adopt unfamiliar technologies such as new remote access tools, cloud-based options for existing tools that could accommodate a distributed workforce, and new collaboration tools that supported video conferencing like Zoom or Microsoft Teams.

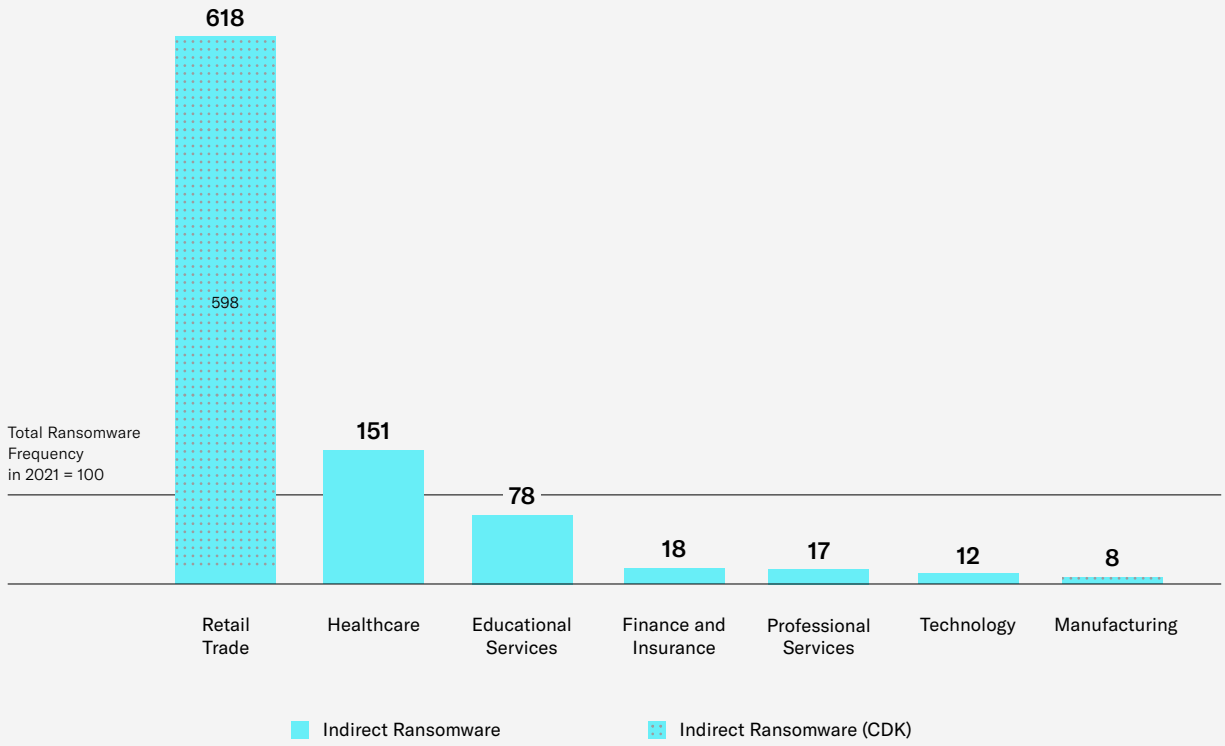
The shift was massive, immediate, and unmanaged.

In April 2020, Microsoft CEO Satya Nadella commented during the company's quarterly earnings call that, "We've seen two years' worth of digital transformation in two months."[7]

[7] 2 years of digital transformation in 2 months, https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/

Retail Trade Claim Frequency Spiked Due to CDK Event

Figure 24: Indexed Indirect Ransomware Claim Frequency by Industry, 2024



This accelerated approach to technology adoption among businesses subverted the typical, risk-conscious approach to acquiring new tools that many businesses may have pursued under other circumstances.

Thus, many technologies were deployed without consideration for the risk that they added to companies' operations (e.g., by adding critical external dependencies) or a plan for future maintenance and upgrades.

The passage of years has created technical debt in the form of missing patches and configuration drift that many companies aren't able to address, leaving them vulnerable.

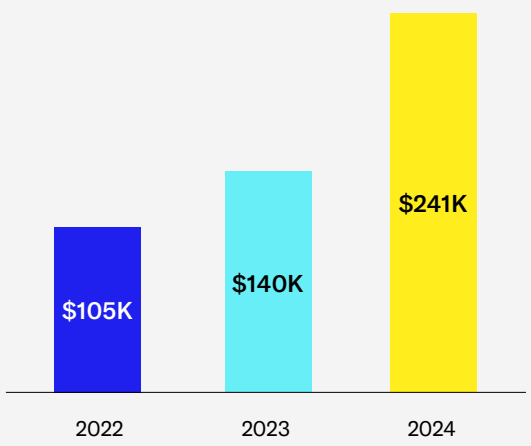
The rise in attacks targeting remote access tools is a result of this trend with many companies operating tools such as VPN solutions that they haven't been able to maintain effectively.

The rise in third party risks is a knock-on effect with companies unwittingly making themselves dependent on outside companies and technology solutions which themselves have become less resilient to attack over time.

Add to this what appears to be a change in tactics among some cyber threat groups. Specifically, we believe that threat groups are increasing their focus on targets that could be described as risk concentration points in the markets that they serve.

Indirect Ransomware Severity Was $241K in 2024

Figure 25: Indirect Ransomware Claim Severity by Year



The reason for this is likely to be an expectation of bigger ransoms paid more quickly due to the significantly increased liability of targeted companies in the event of outage or data breach.

If attackers can identify and successfully attack organizations that have widely distributed obligations to other companies, then their victims are much more likely to pay increased extortion demands commensurate with their liability to their customers.

Attackers also benefit from the additional pressure exerted on the victim by other organizations that feel the second order effects of the attack. Thus, victims in this type of attack are forced to consider not only their own direct costs attributable to an incident but also their potential liability for damage experienced by their trading partners.

This approach has paid well for attackers. As evidence for this, consider the ransomware attack suffered by CDK Global in June 2024.

Within two days of the initial deployment of ransomware into CDK's environment, the company reportedly made a payment of $25 million in bitcoin[8] to BlackSuit, the cyber threat group that was allegedly responsible[9] for the attack. In paying such an outsized ransom so quickly, CDK was doubtless considering the disruption felt by their estimated 15,000 North American auto dealership customers while their products remained unavailable.

In spite of CDK's rapid movement to restore normal operations for their software platform, they still became the defendant in multiple lawsuits alleging a variety of impacts resulting from the incident.

High profile incidents from the last two years impacting Change Healthcare, MOVEit, and Okta followed a similar pattern, reinforcing the idea that this approach is an emerging yet deliberate strategy for attackers.

For At-Bay's insureds affected by the CDK outage, this single incident caused significant damage due to their inability to do business. This resulted in indirect ransomware severity hitting $241K on average, 72% higher than the severity in 2023 when the majority of claims were related to data privacy from the MOVEit breach.

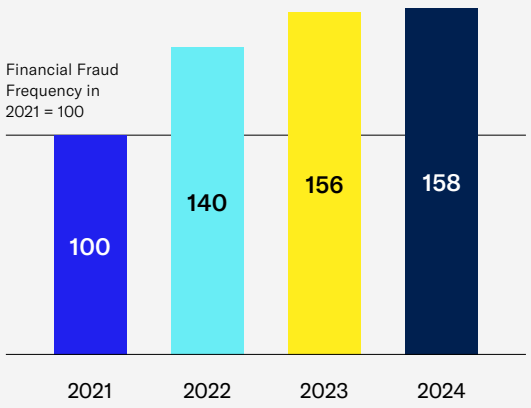
[8] How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom, https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
[9] NewsDealership system hackers seemingly identified as restorations begin, https://www.teslarati.com/dealership-hackers-identified-restorations/

CHAPTER 4

Financial Fraud Still the Most Frequent Incident

Financial Fraud Continued to Damage Businesses

Figure 26: Indexed Financial Fraud Claim Frequency by Year

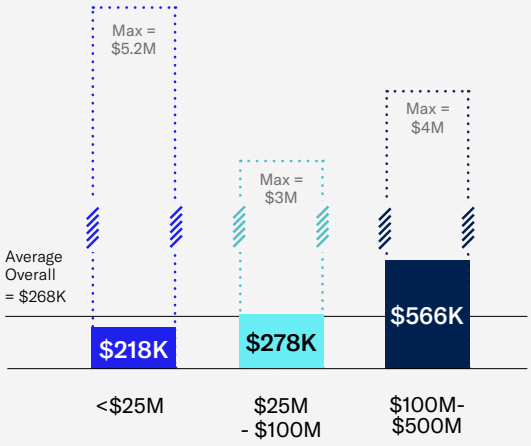


Financial fraud continues to be the most common incident we see among insureds with policies placed by At-Bay. The impact of financial fraud on our policyholders in 2024 was significant but not evenly distributed.

The overall frequency of financial fraud remained essentially static in 2024, but companies with revenue from $25M-$100M saw a 20% increase in fraud incidents (Figure 28).

Companies Lost More Than $5M in the Most Severe Cases of Financial Fraud

Figure 27: Average and Max Amount of Stolen Funds by Revenue Band

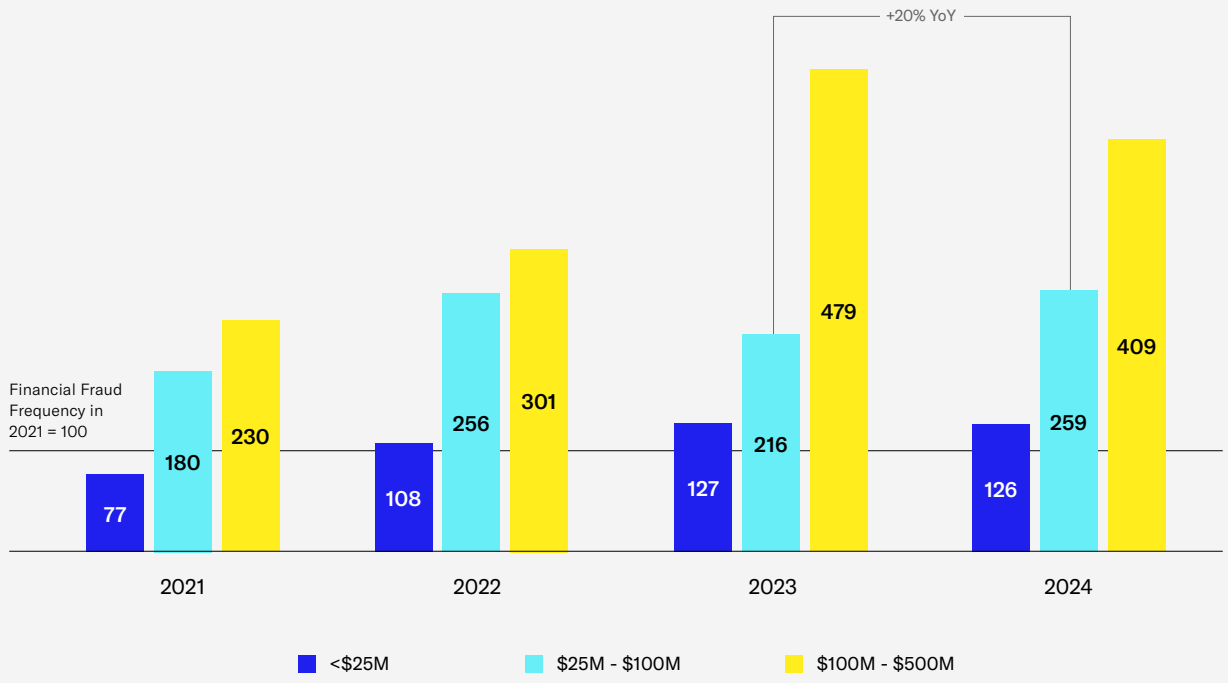


These midsized companies appear to have attracted the attention of fraudsters away from companies with between $100M-$500M in revenue, as that segment saw a 15% decrease in claims related to financial fraud.

The average amount stolen in a financial fraud incident rose to $268K in 2024 from an average of $219K seen in 2023. The most severe case At-Bay saw was an incident where a company with less than $25M in revenue experienced a loss of $5.2M.

Mid-Sized Companies Saw a 20% Increase in Financial Fraud Claim Frequency

Figure 28: Indexed Financial Fraud Claim Frequency by Revenue Group



This demonstrates the existential threat financial fraud represents for many businesses.

And, while a smattering of million-dollar incidents skewed the overall amount of stolen funds for financial fraud incidents upward for all companies, part of the upward trend can be attributed to the relative improvement in success experienced by attackers in refocusing their attention on mid-sized companies.

Mid-sized companies tend to be large enough to have baseline security controls in place (i.e. those controls that are required to obtain cyber insurance at favorable rates) but not large enough to have the administrative and procedural controls necessary to consistently prevent fraud attempts.

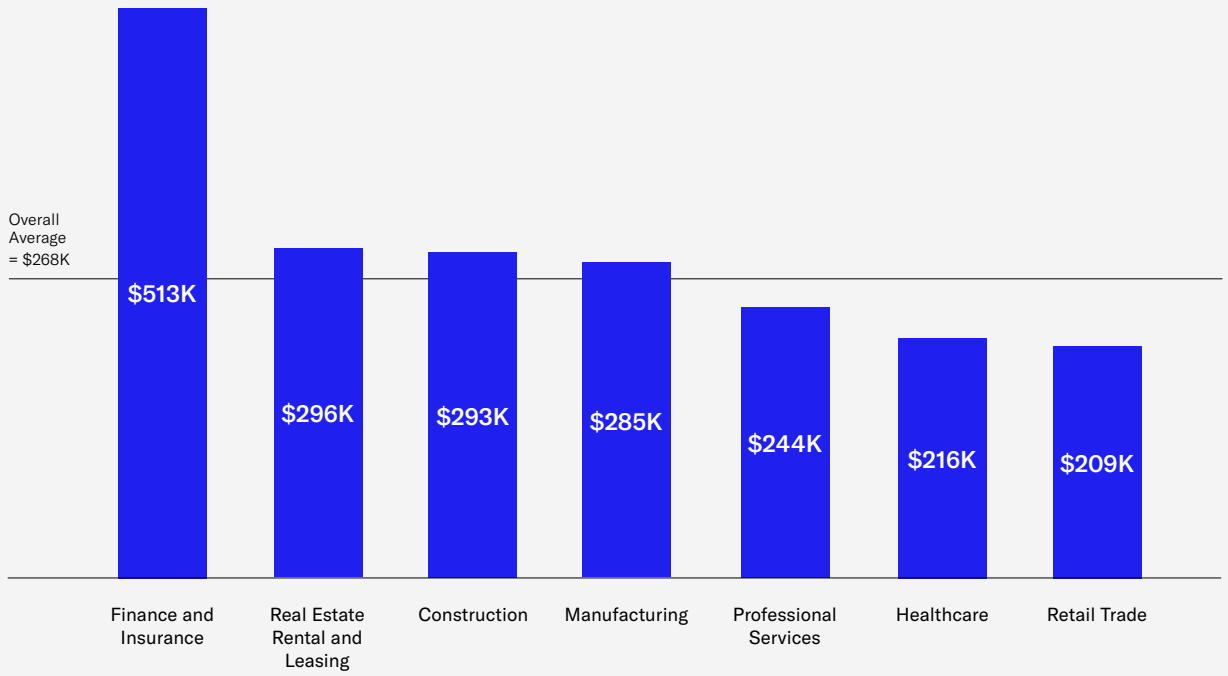
These capabilities would normally be found within robust finance, procurement, and risk management teams more commonly seen in much larger enterprises.

This puts small and mid-sized companies at a significant disadvantage in their resilience to fraud when compared to larger companies.

With more than 80% of fraud incidents originating from a malicious email, attackers need only get past a company's email security solution to get a shot at eliciting fraud — and securing a hefty payday.

Finance and Insurance Industry Hit Hardest by Financial Fraud

Figure 29: Average Amount of Funds Stolen by Industry



Unfortunately, email security solutions aren't keeping pace with changes in attacker behavior.

At-Bay's focus on helping insureds manage their external attack surface over the past several years has forced attackers to shift more of their attention to email as an initial entry vector simply out of necessity.

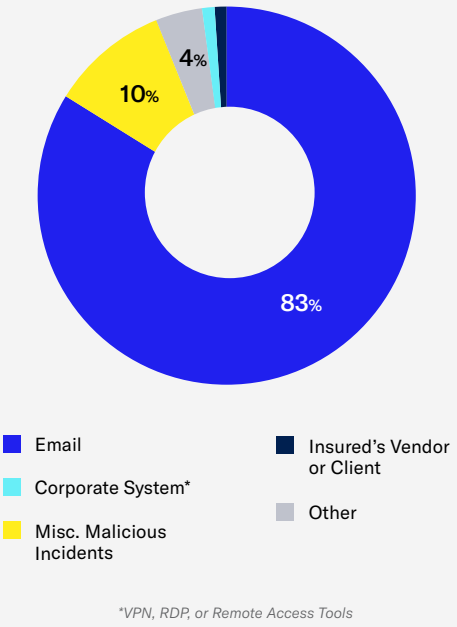
To wit, "corporate system", where a configuration weakness or unpatched vulnerability was exploited, was the initial entry vector for just 17% of overall claims in 2024 (Figure 5). For financial fraud claims in particular, only 2% of incidents began with an attack on a corporate system (Figure 30).

However, the decreased availability of other vectors such as unsecured remote access points and unpatched vulnerabilities doesn't tell the whole story.

In 2024, At-Bay helped policyholders recover **$49M** in stolen funds from financial fraud.

Email Was the Initial Entry Vector for 83% of Financial Fraud Claims

Figure 30: Financial Fraud Claims by Entry Vector, 2024



Email has always been attractive to attackers due to the fact that it provides a common entry point among all types of businesses, making large scale social engineering campaigns easy to execute.

But, the level of effort required for this tactic has been lowered in recent years by the adoption of generative AI tools that are used by attackers to create increasingly credible social engineering emails. This means that, in a threat landscape with an increasing volume of attackers generally, more of them are able to craft effective fraud emails even in the face of limitations like not speaking the language of their intended victims.

Email remains relatively insecure against fraud due to the inability of most email security solutions to spot sophisticated fraud techniques.

While phishing and malware attachments remain a threat, email security tools are increasingly effective at blocking them, especially when backed by a robust security awareness training program.

As evidence of this, we note that while email was cited as the initial entry vector for 43% of all claims (Figure 5), it was the entry vector for only 6% of direct ransomware claims (Figure 17).

Yet a whopping 83% of financial fraud claims began with email as the initial entry vector.

This tells us that while email security tools are effective at blocking threats such as malware attachments, they are proving ineffective at catching emails that elicit fraud – and attackers appear to be shifting their focus away from hacking victims' computers to hacking the victims themselves via deception.

Looking Ahead

We'd like to conclude this edition of At-Bay's InsurSec Report by looking ahead at how events unfolding now might impact the state of cyber risk in the near future. As a cyber insurance provider, there are two factors we use to consider the impact of future events: influence on the number of claims we expect, and influence on the severity of claims. While we've previously discussed technology trends and trends in attacker behavior that are driving claims, there is another category that's worth considering: geopolitical events.

We believe that current events will yield significant increases in both the frequency and severity of cyber incidents afflicting US businesses over the next two to three years.

The main impact will be felt when the war in Ukraine comes to an end. The rate of occurrence of ransomware incidents fell significantly in early 2022. While it's impossible to prove, the consensus explanation among cybersecurity experts is that the conflict in Ukraine was responsible. Technologists on both sides of the conflict who would previously have engaged in criminal activity directed at US companies suddenly found themselves with more urgent business. Many of them were pressed into service by their respective governments, and others saw their pattern of life disrupted in a way that made them unable to continue their previous criminal activities. In the years since, many of these individuals have grown their skills significantly, leveling up from criminal-tier to full nation state grade abilities.

The United States government has prioritized seeking an end to the war as a major element of its foreign policy and is negotiating with both sides (as of this writing) to accelerate them toward a settlement. When the end comes, Ukraine and Russia will likely both demobilize a large number of top-tier cyber professionals who will return to private life. The Ukrainians will have the added challenge of rebuilding the war-damaged parts of their country, a monumental task that will require a massive influx of capital from outside the country.

While most of these technologists will return to software development, IT consulting, and other legitimate uses for their skills, many will not. This latter group will instead look to monetize their abilities by doing what they do best: breaking into computer systems to steal data and plant malware. Thus, the end of the Ukraine war may bring about an unprecedented increase in cyber crime that inverts and magnifies the changes seen in 2022. Worse, the criminals behind the increase will be battle-hardened with more skills, higher levels of motivation, and better organization.

At the same time, US government cyber capabilities are downsizing and refocusing away from Russian-speaking cyber threats. In an effort to improve relations with the Russian Federation, the US government has instructed law enforcement and intelligence agencies to stand down from Russia-focused cyber operations.[10] And, as part of cost-cutting efforts across the US government, the

[10] Hegseth orders suspension of Pentagon's offensive cyberoperations against Russia, https://apnews.com/article/cyber-command-russia-putin-trump-hegseth-c46ef1396e3980071cab-81c27e0c0236; Trump administration retreats in fight against Russian cyber threats, https://www.theguardian.com/us-news/2025/feb/28/trump-russia-hacking-cyber-security

Cybersecurity and Infrastructure Security Agency (CISA) has seen significant reductions to its budget and workforce including key leaders of high-profile programs like CyberSentry, a threat detection service offered to critical infrastructure operators.[11] The CISA employees who remain have reportedly been ordered to cease tracking or reporting on Russia-based cyber threats.[12] Thus, at a critical moment when Russian-speaking cyber criminal groups seem poised for a resurgence, US businesses will be able to count on less cover and less support from government and law enforcement entities.

We are simply unable to imagine a scenario where these developments don't result in a world with more cyber threats arrayed against US businesses.

This makes the support available from private-sector cybersecurity partners such as At-Bay indispensable and invaluable for companies that will feel the heat from those threats. For those companies that are already seeing the impact of InsurSec, we thank you for your support and hope that you will continue to take full advantage of the benefits offered by our cybersecurity solutions. For everyone else, we hope that you find a cybersecurity partner that fits your needs. The road ahead may be uncertain, but no one needs to travel it alone.

[11] 'People Are Scared': Inside CISA as It Reels From Trump's Purge, https://www.wired.com/story/inside-cisa-under-trump/
[12] Trump administration retreats in fight against Russian cyber threats, https://www.theguardian.com/us-news/2025/feb/28/trump-russia-hacking-cyber-security

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 end of 2024. Incidents reviewed included those related to ransomware, either direct or indirect. By analyzing actual claims data, the At-Bay Research Team set out to answer these questions:

- How have cyberattacks and threat actors evolved?
- Which technologies are associated with differing outcomes?
- 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.

Definition of the Various Ransomware Types Mentioned in This Report

For the purposes of this report, this is how we define the different types of ransomware:

- **Direct Ransomware**: A ransomware incident where an organization is directly targeted by a cyberattack.
- **Indirect Ransomware**: An incident where an organization is indirectly impacted by a cyber event on their vendor or partner. The victim of indirect ransomware experiences harm either through the exposure of its sensitive data held on the partner's systems, or because its operations are disrupted when the partner's products or services become unavailable.

A Note About Our Revenue Bands

While At-Bay helps place insurance for business 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

Chin Chang
Senior Manager, Risk Analytics

Elisheva Buchsbaum
Senior Data Scientist

Eva Kwan
VP, Claims

Gal Marko
Director of Tech Strategy & Operations

Liat Klainman
Cyber Data Analyst

Michael Lowe
Head of Marketing

Rebecca Jarrett
Head of Claims Operations

Ronit Suzan
Product Specialist

Samantha Wong
Risk Analyst

ABOUT AT-BAY AND THIS 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 that 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.

at bay