at bay

The 2024

InsurSec Report

Ransomware Edition

at-bay.com

An analysis of At-Bay claims and cybercrime data

Table of Contents

Introduction

Ransomware didn't just grow in 2023. It evolved.

In 2023, ransomware frequency increased by 64% overall when compared to 2022, mostly driven by a 415% increase in indirect ransomware (an incident where an organization is indirectly impacted by a cyber event on their vendor or partner). Meanwhile, direct ransomware (a ransomware incident where an organization is directly targeted by a cyberattack) also rose 17%, though below the record levels we saw in 2021.

In addition to the return of ransomware, we've seen more and more threat actors use both encryption and exfiltration tactics in their attacks, in what we refer to as "double leverage." Over half of all ransomware claims we saw in 2023 used this tactic, resulting in the highest average ransoms paid when compared to attacks that were either encryption-only or exfiltration-only.

Double leverage attacks are a serious problem because of their downstream domino effect. Oftentimes, the sensitive data exposed by attackers includes data that belongs to the victim's customers or partners — creating data privacy liabilities to those partners who become collateral damage.

The damage caused by this domino effect is exacerbated when the victim company serves a particular industry, like many vertical Software-as-a-Service (SaaS) companies that tailor their products to specific market segments. This can lead to widespread fallout across entire industries. An outsized example of this occurred in 2023 with the MOVEit breach.

Attackers also evolved with regard to their preferred attack vectors. In 2023, we saw bad actors continue to exploit remote access technologies, making perimeter access tools an increasingly weak link in the chain. Cybercriminals shifted their focus in 2023 from Remote Desktop Protocol (RDP) to targeting self-managed Virtual Private Networks (VPNs) — those implemented on-premises and maintained in-house — which accounted for a whopping 63% of the year's ransomware events where remote access was the initial entry vector.

Businesses deserve more transparency, software companies responsible for the worst outcomes should be held accountable, and the risk associated with threat actors' evolving tactics should be laid out in precise terms. We believe this information can help turn the tide against ransomware and further safeguard businesses of all sizes.

By combining expertise from our Cyber Research team along with technical claims data from our Claims and Incident Response teams, we present the full commercial impact caused by ransomware in 2023. By publishing this report, we aim to show the greater business community what has led us to this point and what can be done to reduce the risk that has resulted from this complexity.

Key Findings

1 **DIRECT RANSOMWARE CLAIMS FREQUENCY INCREASED BY 17% IN 2023.**

In 2023, ransomware claims frequency as a whole jumped 64% year over year, primarily driven by an explosion in indirect ransomware claims frequency that rose 415% over 2022.

2 **REMOTE ACCESS CONTINUES TO BE THE PRIMARY ENTRY VECTOR ACCOUNTING FOR 58% OF CLAIMS.**

Attackers continued to exploit remote access technology, with 58% of direct ransomware events attributable to a remote access vulnerability. In addition, we saw attackers shift their focus from RDP to targeting self-managed VPNs, which accounted for 63% of the remote access ransomware events in 2023.

3 **ORGANIZATIONS USING SELF-MANAGED VPNS BY CISCO AND CITRIX WERE 11X MORE LIKELY TO FALL VICTIM TO A DIRECT ATTACK IN 2023.**

The use of self-managed VPNs was correlated with worse outcomes compared to using a cloud-managed VPN or no VPN at all. Two of the most popular self-managed VPNs, Cisco and Citrix, stood out the most when compared to cloud based VPNs or no VPNs at all.

4 **AVERAGE DIRECT RANSOMWARE SEVERITY IN 2023 WAS $370K.**

Severity was 24% lower than in 2022. Law firms had the highest severity for direct ransomware attacks in 2023, experiencing 32% higher severity than the average.

5 **THE AVERAGE RANSOM PAYMENT IN 2023 WAS $282K.**

The average ransom demand by attackers was $1.26M, though only 46% of incidents actually ended in a ransom being paid. The average amount paid was over 77% lower than the initial demand.

6 **LOCKBIT AND BLACKCAT WERE USED IN 35% OF RANSOMWARE ATTACKS.**

We recorded 41 unique ransomware strains used in attacks in 2023, with LockBit and BlackCat/ALPHV overshadowing all others.

7 **THE COMBINATION OF ENCRYPTION AND EXFILTRATION WAS USED IN 51% OF INCIDENTS.**

A combination of data encryption and exfiltration was the most common direct ransomware tactic. This double leverage tactic was also the most costly for businesses. Encryption and exfiltration events saw the highest median ransom paid ($195K) over encryption-only incidents ($66K) or exfiltration-only incidents ($110K).

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.

All figures in this report derived from 2023 At-Bay claims and cybercrime data as compared to prior year data

CHAPTER 1

The Ransomware Landscape

Ransomware Frequency Increased 64% in 2023

Ransomware is alive and well. After seeing a decline in ransomware in 2022, in 2023 we saw overall ransomware frequency grow by 64%, with increases in both direct and indirect ransomware.

Direct ransomware claims frequency (which we define as a direct attack on an organization resulting in encryption and/or exfiltration of data to hold the organization to ransom) increased in 2023 by 17%, after a brief reprieve in 2022. Despite its increase in 2023, direct ransomware frequency was still well below 2021 levels.

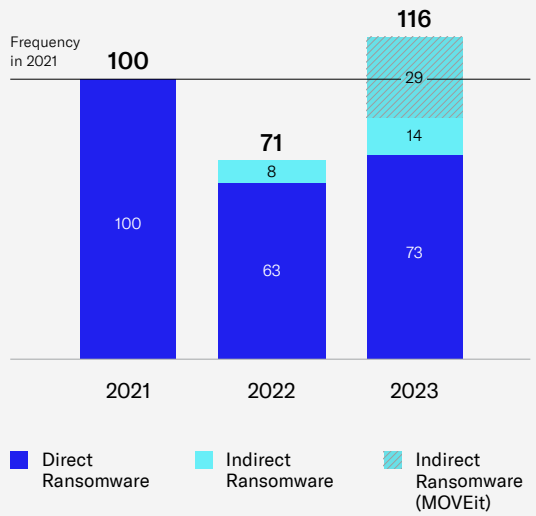
Larger companies saw higher frequencies of direct ransomware, which is no surprise as larger companies tend to have deeper pockets for payouts and more at stake. However, we also saw a 48% increase in direct ransomware for the smallest companies in our portfolio (those with less than $25M in annual revenue). Although smaller companies may be targeted less frequently than larger companies, the threat is growing for this cohort too — making ransomware a risk they cannot afford to ignore.

2023 also revealed a disconcerting trend: a precipitous rise in companies experiencing an indirect ransomware attack (which we define as an incident where an organization is indirectly impacted by a ransomware attack on their vendor or partner, resulting in a data breach or business interruption).

In 2023, indirect ransomware frequency increased by 415% compared to 2022, much of it stemming from the MOVEit vulnerability. Unlike direct ransomware, where the largest companies experienced the highest frequency of attacks, indirect ransomware impacted every revenue band nearly equally.

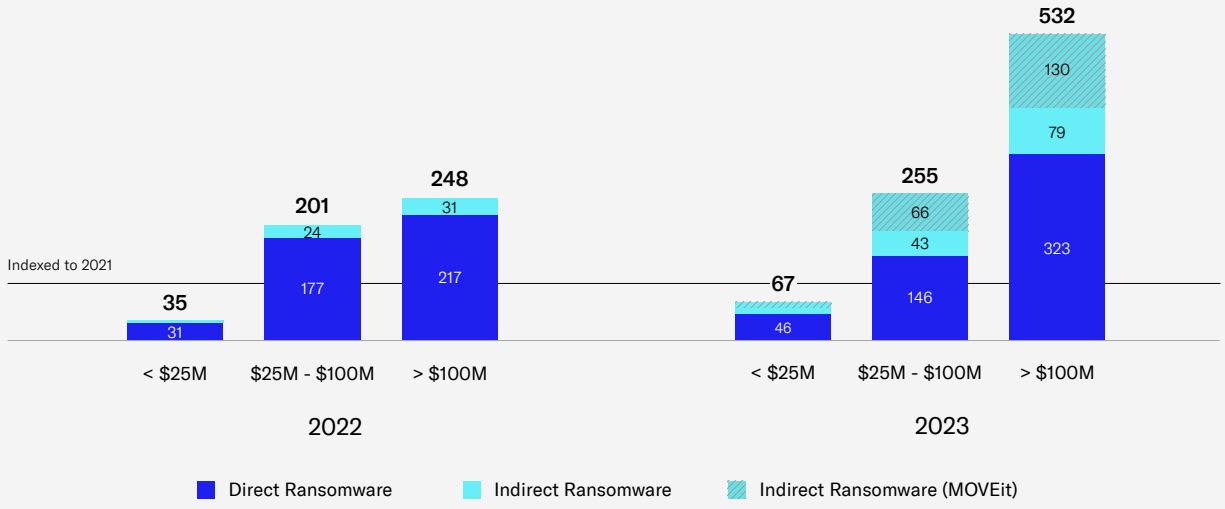
Indirect Ransomware Frequency Increased 415% by 2023

Figure 1: Indexed Ransomware Claim Frequency by Year



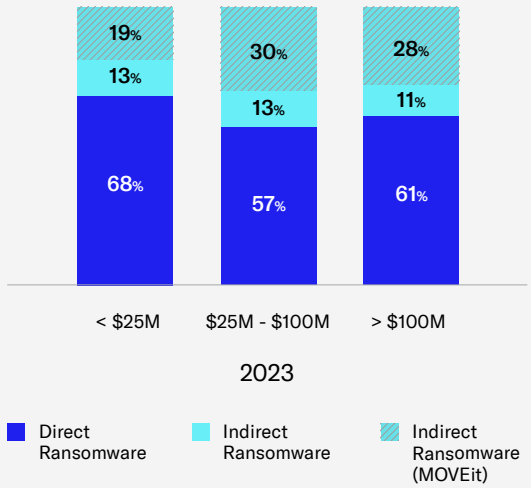
Larger Companies Saw Higher Ransomware Claims Frequencies

Figure 2: Indexed Ransomware Claim Frequency by Revenue Band



Indirect Ransomware Impacted Companies Across All Revenues

Figure 3: Percentage of Ransomware Type by Revenue Band



Anatomy of a Supply Chain Attack: MOVEit

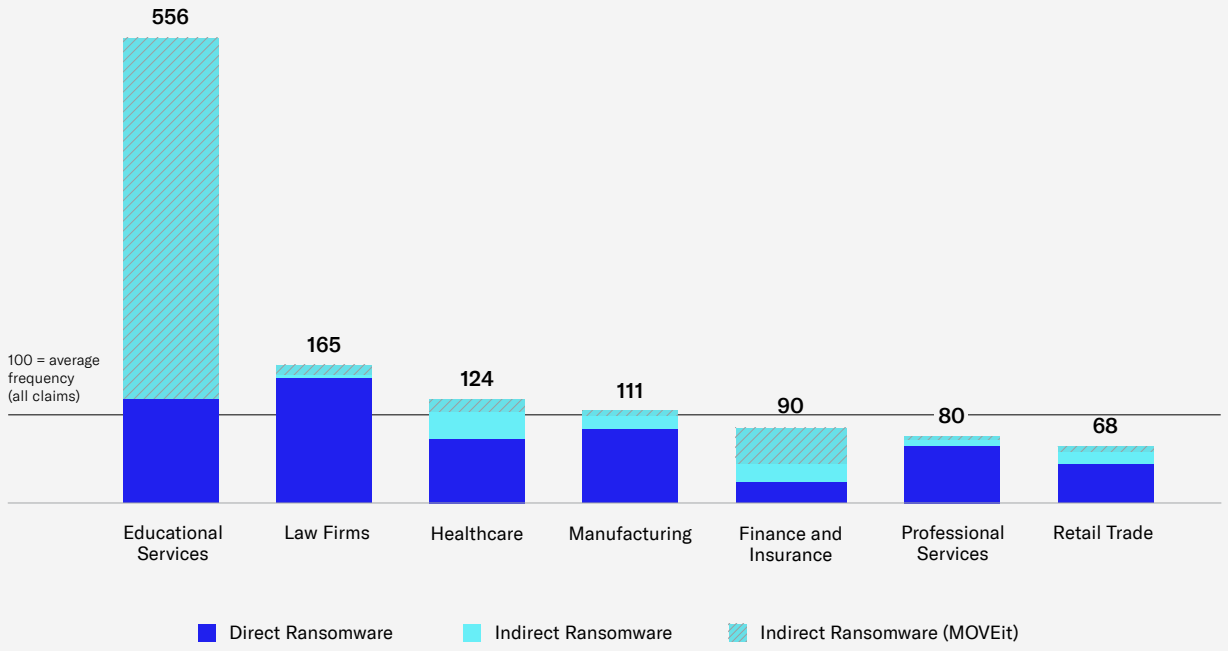
In May 2023, threat actors exploited two zero-day vulnerabilities[1,2] in the well-known file transfer software MOVEit. This event led to thousands of organizations being impacted, either directly or via the software supply chain. The ransomware gang responsible for the attack, CL0P, used the MOVEit vulnerabilities to infiltrate organizations, steal sensitive personal identifiable information (PII), and threaten to publicly release the data if their ransom demands weren't met.

The MOVEit incident had a significant impact on organizations in the educational services sector, along with businesses in finance and insurance, due to a handful of vertical (i.e. industry-specific) software products compromised by the attack.

[1] National Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-34362
[2] National Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-35708

Education Industry Hit Hardest by Indirect Ransomware

Figure 4: Indexed Ransomware Claim Frequency by Industry, 2023



Specifically, threat actors leveraged the MOVEit vulnerabilities to attack the education nonprofit National Student Clearinghouse (NSC). NSC, which produces data and reports on North American high schools, colleges, and universities, partners with 25,000 schools. The attack on the organization led to 890 schools being breached[3], impacting tens of millions of students and alumni.

Across our portfolio, indirect ransomware related to MOVEit alone increased claims frequency in the education sector by 3.4X compared to 2022.

In a similar case, attackers used the MOVEit vulnerability to attack Pension Benefits Information (PBI), a pension records auditor used by many financial institutions[4]. This attack alone drove the financial sector to experience 81% higher indirect claims frequency compared to direct ransomware in 2023.

> MOVEit alone increased claims frequency in the education sector by **3.4X** compared to 2022.

[3] California Office of the Attorney General, https://oag.ca.gov/system/files/Exhibit%20A_6.pdf

[4] The MOVEit Cyberattack – What happened. PBI's response. What's next., https://www.pbinfo.com/the-moveit-cyberattack-what-happened-pbis-response-whats-next/

INDIRECT RANSOMWARE: WHO SHOULD PAY?

The MOVEit attacks underscore a critical issue: An organization's cybersecurity posture, financial and reputational well-being are not solely determined by its own defenses, but also by those of its partners and suppliers. When a threat actor breaches a company, it exposes that company, as well as any data that company stores related to its partners.

We expect this trend of attacks on software supply chain vendors to continue, which could have an outsized impact across a large swath of businesses.

Consequently, these attacks illustrate the growing need for businesses to vet third-party vendors' IT portfolio and security posture, including whether or not they have their own cyber insurance policies. In the event of a claim due to a third-party breach, cyber insurance may cover an impacted organization's loss, underscoring the importance of having robust coverage.

Businesses that experience an indirect ransomware attack are more likely to recoup losses from the organization that was initially attacked if that organization carries cyber insurance.

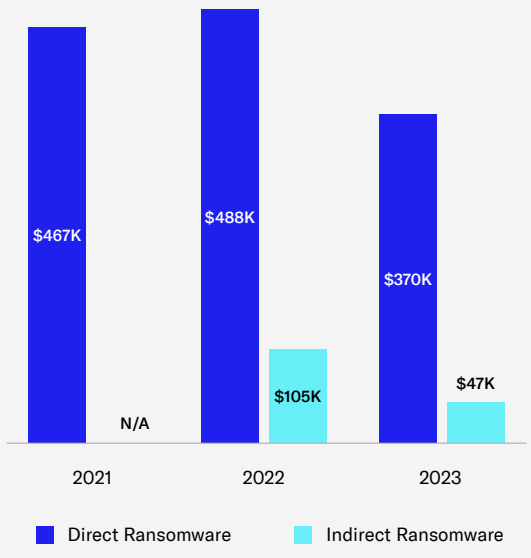
Ransomware Severity Decreased in 2023

In contrast to ransomware frequency, in 2023 both direct and indirect ransomware severity[5] in our portfolio dropped year over year. Average direct ransomware severity was $370K, a 24% decrease from 2022, while average 2023 severity for indirect ransomware events came in 55% lower than 2022 at $47K.

We believe this year-over-year decrease in severity may be attributed to clients' ability to successfully restore from backups more often. When they do, they're less likely to pay a ransom. We discovered this trend in our recent Backups Report (see Figure 6). Companies who failed to restore their data were 3X more likely to pay a ransom than those who were able to successfully restore from backups.

Average Direct Ransomware Severity Was $370K in 2023

Figure 5: Ransomware Claim Severity by Year

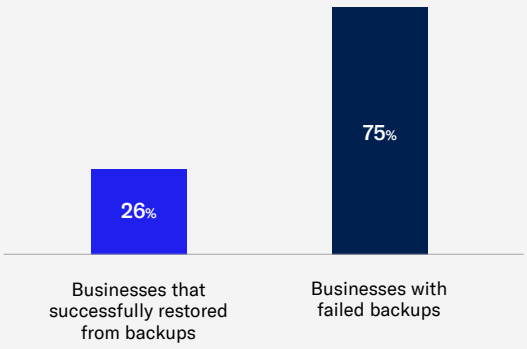


[5] Severity is the financial loss or damages related to a claim

Businesses who successfully restore backups are also more likely to incur a lower business interruption cost and fewer costs to restore systems. Oftentimes restoring from backups can be done by their in-house IT team or MSP, which potentially avoids fees related to hiring third-party vendors to do this work. For more data and actionable advice on what makes a backup successful, read our full report.

Businesses That Successfully Restored from Backups Paid Ransom Less Often

Figure 6: Likelihood of Paying a Ransom for Businesses That Successfully Restore From Backups



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

As expected, our analysis showed indirect ransomware severities were typically only a fraction of direct ransomware incidents. This significant difference in the cost of ransomware events is due to the difference in cost and complexity of recovery: direct ransomware events may include costs related to actual ransom payments, technology replacement (e.g. new servers or computers), recovering or restoring access to networks architecture, business interruption losses, or any cost associated with services, such as digital forensics and incident response professionals or legal counsel.

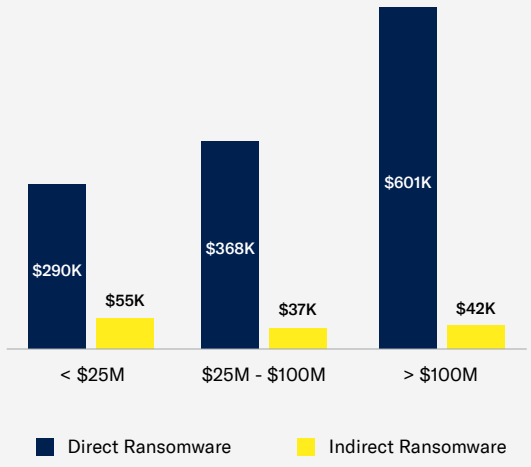
Indirect ransomware severity, by contrast, is more limited as the impacted company's systems are not breached. Costs incurred from an indirect ransomware event are restricted to those related to a partner's data breach, which may include required notifications, legal fees, or contingent business interruption costs.

Despite this welcome decrease in severity, the impact of ransomware is still substantial for companies of every size. For a business with less than $25M in revenue, a $290K incident can be an insurmountable expense, and a $601K claim, even for the largest companies, can still have a sizable financial impact.

Severity of indirect ransomware was similar across different revenue bands. However, it's important to remember that in addition to the cost of the claim or incident, companies subject to indirect ransomware also risk potential reputational harm, which may be equally (or more) damaging than the initial monetary outlay.

Indirect Ransomware Severity Was $55K on Average for Small Businesses in 2023

Figure 7: Ransomware Claim Severity by Revenue Band, 2023



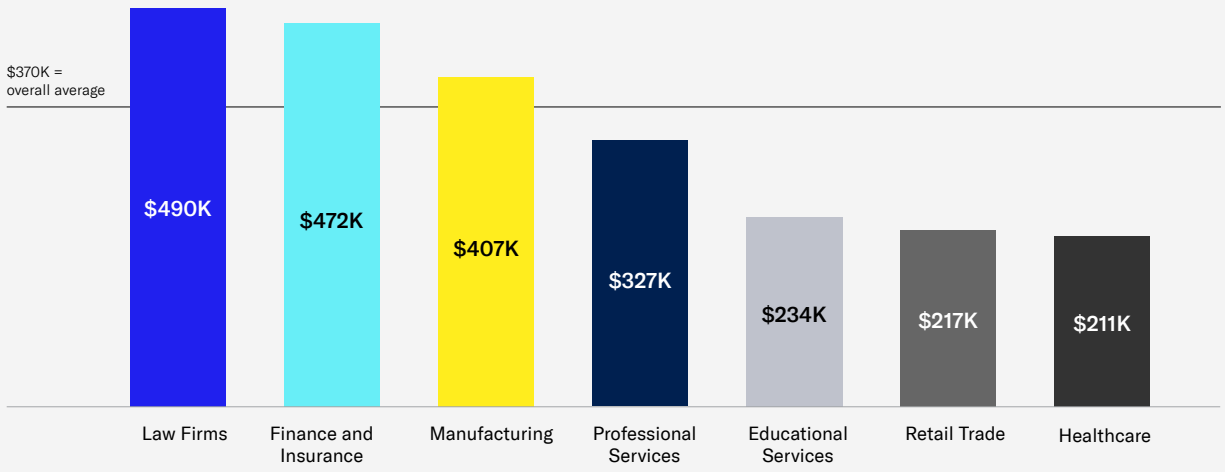
When viewing severity by industry, law firms had the highest severity for direct ransomware attacks in 2023, experiencing 32% higher severity than the average within our portfolio. These firms often fit a perfect profile for threat actors: They typically hold highly sensitive and valuable data like client information, case files, and intellectual property.

Despite holding sensitive data and facing potentially high costs from attacks, healthcare companies in our portfolio experienced an average incident severity of $211K, significantly below the overall average of $370K. The disparity may be a result of our ability to underwrite against these riskier accounts.

Law firms, finance and manufacturing saw the **highest** severities.

Law Firms Experienced 32% Higher Severity Than Average

Figure 8: Direct Ransomware Claim Severity by Industry, 2023



CHAPTER 2

Ransomware Attack Vectors

VPNs Unseat RDP as Leading Entry Vector

Attacks that targeted remote access tools accounted for 58% of ransomware claims in 2023 where an entry vector could be determined. Vulnerabilities in these tools are frequently abused by attackers because these tools are gateways into the network. Moreover, many remote access services lack strong security controls or are misconfigured or poorly run by those managing the tools.

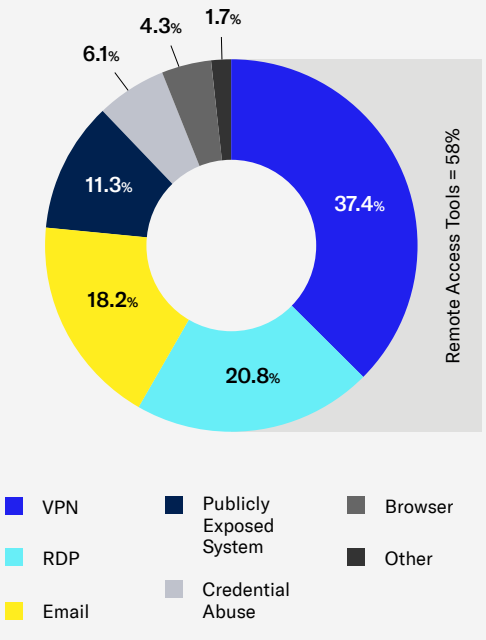
Of the ransomware claims where we identified remote access as the initial entry vector, 63% were tied to self-managed VPNs, a reflection of a shift in attackers' tactics.

For years, RDP has been the most popular ransomware attack vector, leading companies to better secure the service and insurers to better account for its risk. This has, in turn, motivated attackers to focus on other types of remote access technology — namely VPNs. The shift can also be attributed to a number of critical vulnerabilities discovered in popular VPNs in 2023.

We acknowledge that our claims skew away from RDP due to our ability to detect (and underwrite against) risky RDP configurations. It's worth noting that cybersecurity firms[6,7] still report that RDP is a leading issue for companies. However, our statistics show that VPNs are quickly catching up in terms of an initial entry vector, which points to a shift in attacker behavior.

Remote Access Tools Accounted for 58% of Ransomware Claims

Figure 9: Direct Ransomware Claims by Entry Vector, 2023



[6] Combating Ransomware Attacks: Insights from Unit 42 Incident Response, https://www.paloaltonetworks.com/blog/2023/09/combating-ransomware-attacks-insights/

[7] Coveware, Big Game Hunting is back despite decreasing Ransom Payment Amounts, https://www.coveware.com/blog/2023/4/28/big-game-hunting-is-back-despite-decreasing-ransom-payment-amounts

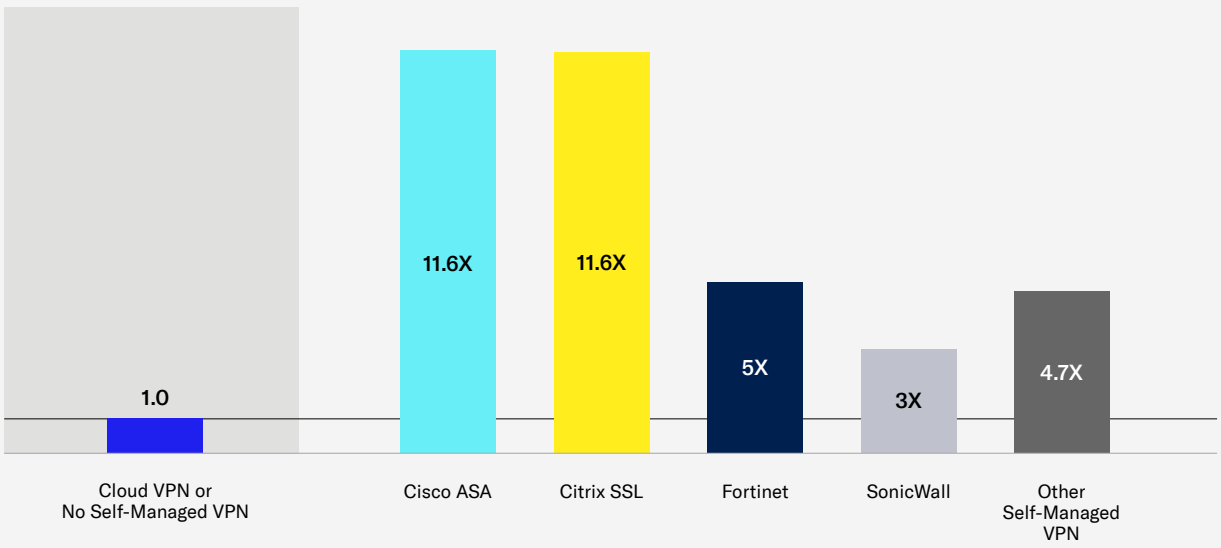
The Problem with Self-Managed VPNs

Our data shows that businesses that use self-managed VPNs, a version of the technology that is implemented on-premises and maintained by in-house IT teams, are associated with a considerably higher risk of a security incident than businesses that don't use self-managed VPNs, use more secure cloud-hosted VPNs, or use other remote access technology.

Organizations using Cisco and Citrix self-managed VPNs were **11X** more likely to fall victim to a direct ransomware attack.

Likelihood of a Business Using One of These VPNs to Fall Victim to an Attack

Figure 10: Indexed Direct Ransomware Claims Frequency by Self-Managed VPN, 2023



Two particular self-managed VPNs stood out in our ransomware claims data. When normalized for their prevalence in our portfolio, organizations using two of the most popular self-managed VPNs, Cisco ASA and Citrix SSL, were 11X more likely to fall victim to an attack than those who use a cloud VPN or no self-managed VPNs.

To be clear, our claims data does not point to these products being directly responsible for every claim. However, this data further supports findings we published in 2023: Self-managed VPNs are routinely exploited by cybercriminals and are associated with major cybersecurity incidents that result in substantial financial losses.

Cisco ASA

A flaw in Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) appliances (CVE-2023-20269) was responsible for over 10% of direct ransomware claims where remote access was the initial entry vector, the highest percentage we recorded.

This vulnerability grants attackers infinite attempts to brute-force usernames and passwords for the vulnerable system. The flaw has become a weapon of choice for threat actors, particularly those using the Akira ransomware strain.

CitrixBleed

Much like Cisco, two vulnerabilities in Citrix's NetScaler products publicly announced in 2023 led to a wave of attacks. Known as "CitrixBleed," exploitation of these vulnerabilities results in threat actors bypassing security measures like multi-factor authentication (MFA), which allows unauthorized access to corporate networks.

The vulnerabilities, tracked as CVE-2023-4966 and CVE-2023-4967, were discovered in August 2023.

Threat actors have shifted their focus from RDP to VPN.

Finding Repeatable Opportunities for Ransomware

Threat actors don't target these products by chance. Because of their widespread adoption, popular self-managed VPNs offer threat actors considerable grounds for exploitation. Successful attacks then give threat actors a repeatable playbook for launching future attacks, as these common weaknesses are well-documented and easily exploitable at scale across multiple target organizations. This repetition allows attackers to refine their strategies and ultimately increase their success rate.

CHAPTER 3

Negotiating Ransom Demands

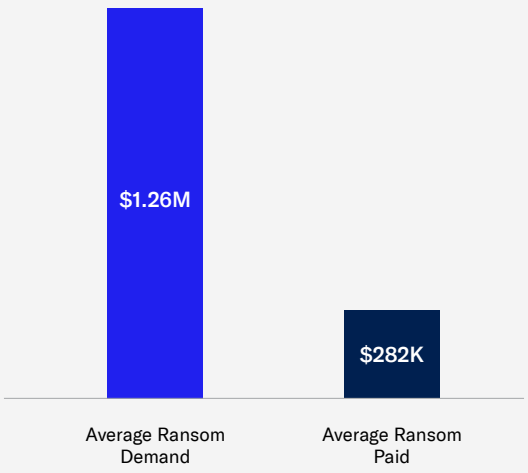
Outcomes Can be Heavily Negotiated

The initial ransom demand in 2023 was $1.26 million on average. However, actual ransom payments were only made less than half of the time — and typically at a dramatically lower price than initially demanded. In 2023, the average amount paid by a victim organization ($282k) was 77% less than what was initially demanded by threat actors on average.

Victim organizations paid **77% less** than what was initially demanded by threat actors.

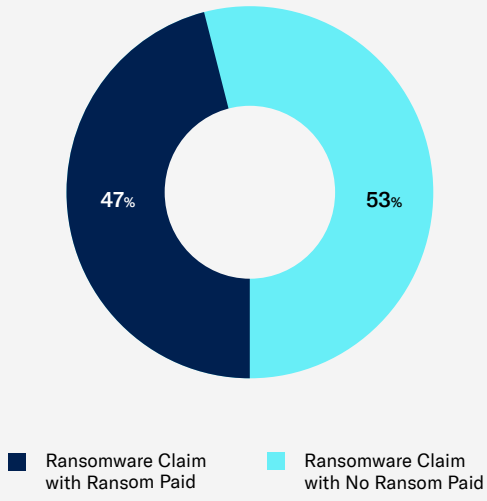
Average Ransom Paid Was $282K in 2023

Figure 11: Average Direct Ransomware Demands and Payments, 2023



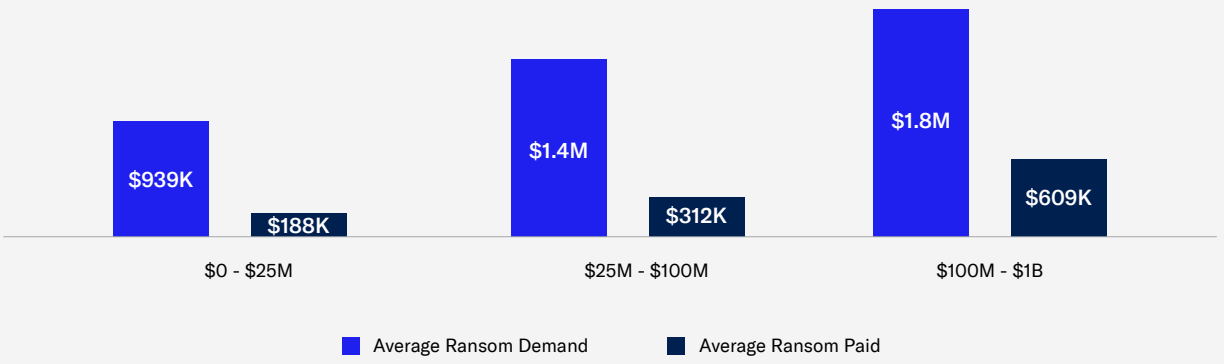
Fewer Than half of Claims Resulted in an Actual Ransom Payment

Figure 12: Direct Ransomware Claims With a Ransom Paid, 2023



Average Ransom Payments Start at Six Figures For Even the Smallest Companies

Figure 13: Average Direct Ransomware Demands and Payments by Revenue Band, 2023

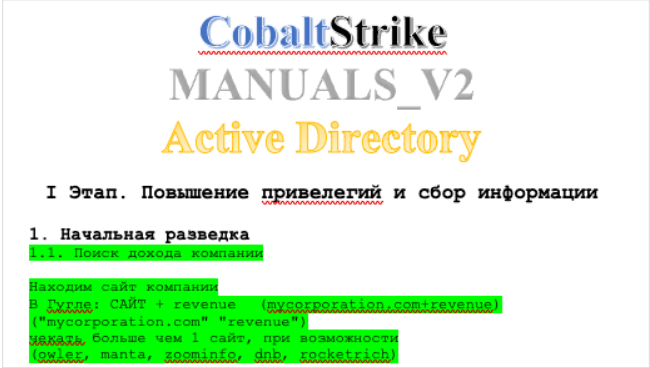


When we broke ransom demands and payments down further by revenue size, we found that larger companies received higher average ransom demands and paid higher amounts on average than their smaller counterparts.

This is no accident. Ransomware groups and their affiliates do their research to take full advantage of their targets. This allows them to customize their demands, striking a balance to ensure the sum is substantial enough to benefit them financially while still appearing payable to the victim.

The ransomware developers create instruction manuals they give to affiliates which include instructions on how to determine the appropriate ransom amount. For example, at right is a portion of a leaked manual from the defunct Conti group[8] instructing affiliates on how to find information from various business intelligence sources like Dun & Bradstreet, Owler, and ZoomInfo.

This tailored approach increases the likelihood of payment, as businesses — especially those unprepared for such threats — may see no other option but to pay in order to regain access to their vital data or business operations and minimize damage to their reputation.

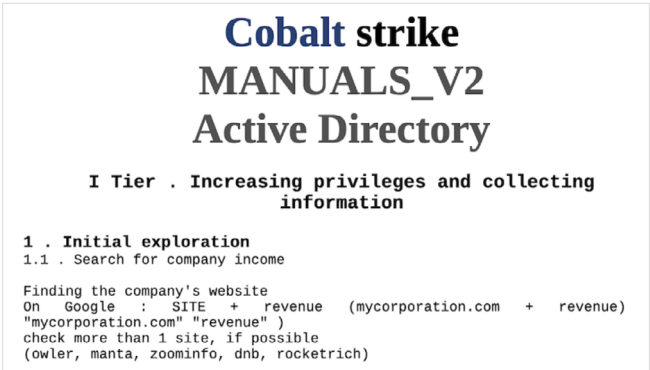

CobaltStrike
MANUALS_V2
Active Directory

I Этап. Повышение привелегий и сбор информации

1. Начальная разведка
1.1. Поиск дохода компании

Находим сайт компании
В Гугле: САЙТ + revenue (mycorporation.com+revenue)
("mycorporation.com" "revenue")
искать больше чем 1 сайт, при возможности
(owler, manta, zoominfo, dnb, rocketrich)

Original Version in Russian


Cobalt strike
MANUALS_V2
Active Directory

I Tier . Increasing privileges and collecting information

1 . Initial exploration
1.1 . Search for company income

Finding the company's website
On Google : SITE + revenue (mycorporation.com + revenue)
"mycorporation.com" "revenue")
check more than 1 site, if possible
(owler, manta, zoominfo, dnb, rocketrich)

Translated to English

[8] Conti manual translation to English, https://talosintelligence.com/resources/269

Two Malware Strains Accounted for the Majority of Direct Ransomware Claims

Among the claims we analyzed in 2023, we found 41 unique strains of ransomware used. Yet even with the breadth of variants, LockBit and BlackCat/ALPHV overshadowed all others, accounting for a combined 35% of all claims tied to direct ransomware attacks.

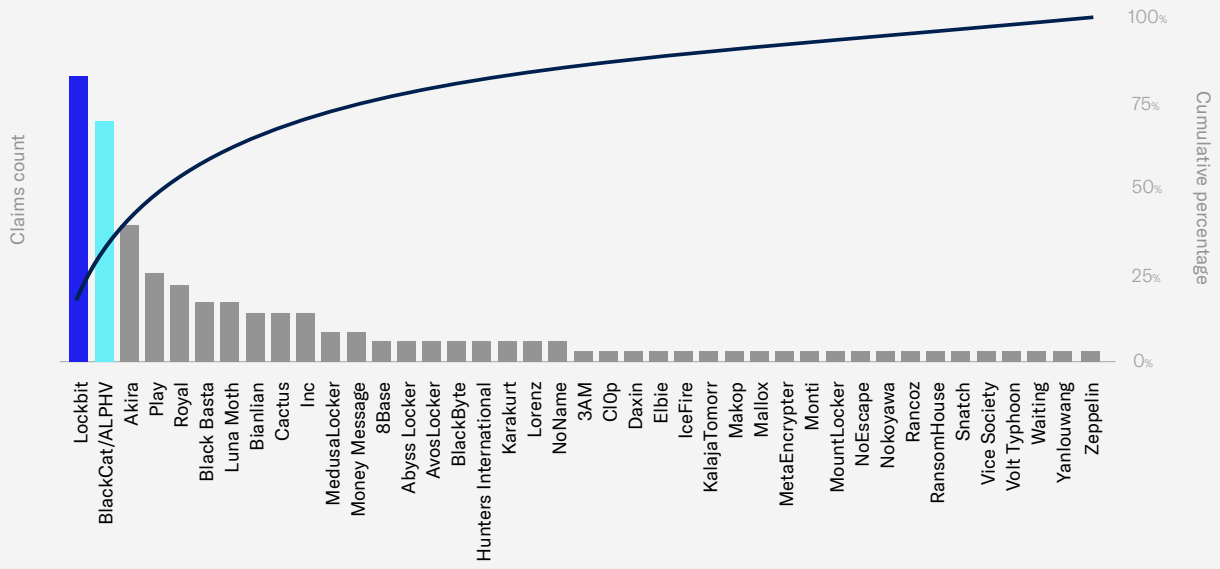
When examining how attacks are spread across different sizes of businesses and industries, it's crucial to understand that these operations function under a Ransomware-as-a-Service (RaaS) model. This means that the core attackers aren't launching individual attacks; instead, they distribute their ransomware code to a wide network of affiliates who then carry out the attacks.

By leveraging this affiliate model, LockBit is able to cause widespread damage as a frequently-used strain. Affiliates made headlines in 2023 by using LockBit in attacks on multinational organizations like aviation giant Boeing, chipmaker TSMC, and the U.S. arm of the Industrial and Commercial Bank of China.

BlackCat/ALPHV follows a similar model and was used in attacks on big companies like global hospitality and entertainment company MGM, data storage manufacturer Western Digital, and medical and dental supply company Henry Schein.

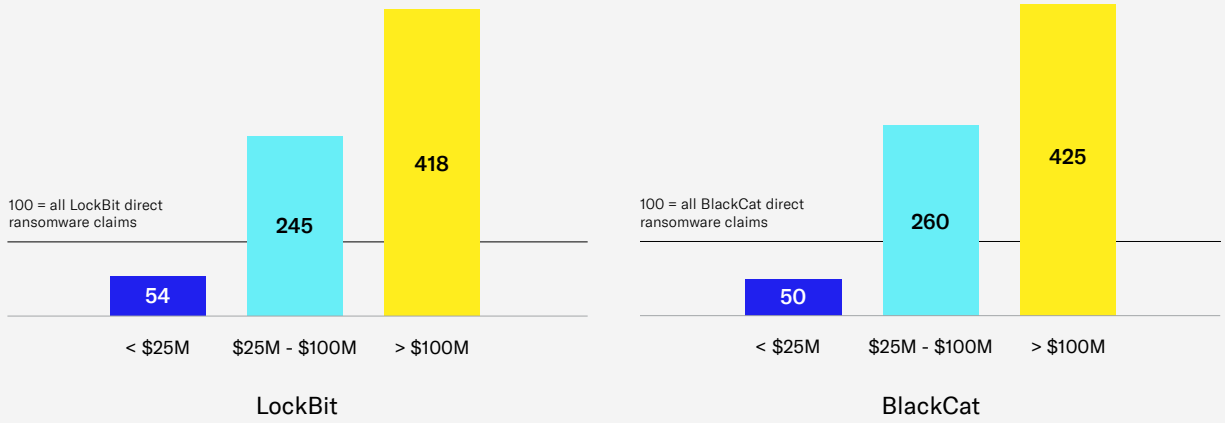
LockBit and BlackCat Were Responsible for 35% of Direct Ransomware Claims in 2023

Figure 14: Prevalence of Direct Ransomware Strains Among Claims, 2023



Both LockBit and BlackCat Were More Likely to Impact Larger Businesses in 2023

Figure 15: Indexed Direct Ransomware Claims Frequency by Revenue Band for LockBit and BlackCat, 2023



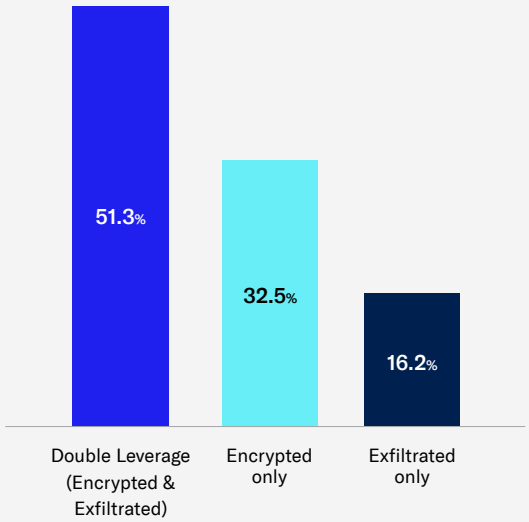
How Threat Actors Use Double Leverage to Demand — and Get Paid — More

Threat actors seek to increase their revenue potential by maximizing leverage over a victim. As such, in addition to encrypting company systems, they have evolved to also exfiltrate data. While some companies may refuse to pay for decryption keys, they may be more inclined to negotiate when it comes to preventing the public release of sensitive data.

More than half of ransomware attacks we saw in 2023 involved both encryption and exfiltration, or what we call double leverage. By both encrypting and stealing data, ransomware attackers maximize the odds of receiving some form of payment, making each attack more profitable and ensuring their criminal enterprise continues to thrive. This method has proven so effective that it's become a standard part of many high-profile ransomware operations.

Nearly 50% of Direct Ransomware Attacks Used Double Leverage in 2023

Figure 16: Percentage of Direct Ransomware Claims by Attacker Tactic, 2023



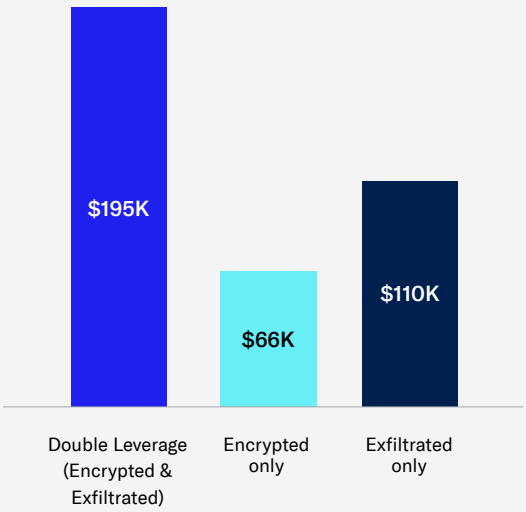
Our data shows claims with both an exfiltration and encryption event had the highest median ransom demand ($600K), as well as highest median payment ($195K). Exfiltration-only events had the second highest ransom paid ($110K).

The common theme in our portfolio is that exfiltration tactics are effective. They not only receive the highest ransom payments compared to encryption-only events ($66K), they also see the highest likelihood that a ransom will be paid at all.

Exfiltration-only events saw ransom payments 39% of the time, with double leverage incidents (which include both encryption and exfiltration) resulting in payment 34% of the time. Encryption-only ransomware resulted in a payment only 24% of the time.

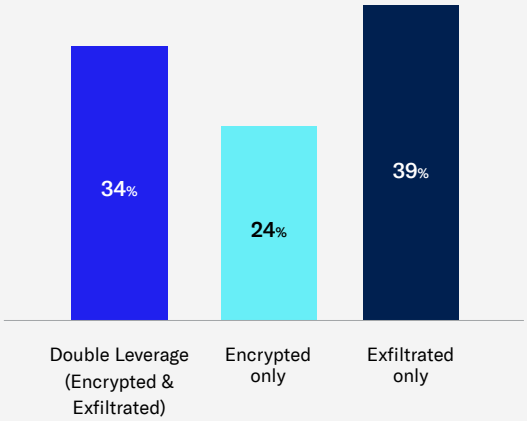
Double Leverage Incidents Led to Highest Ransom Payments

Figure 17: Median Ransom Payment by Attacker Tactic, 2023



Incidents With an Exfiltration Event Saw More Ransoms Paid

Figure 18: Percentage of Ransom Paid by Attacker Tactic



Double Leverage Attacks Heighten Risk for Operational or Reputational Loss

Beyond the immediate ransom payment, which some enterprises might reluctantly consider, double leverage attacks can result in data privacy issues exposing the impacted business to additional regulatory violations or financial risk. When threat actors access, view, or take data, those actions can invite scrutiny from various state or national data protection laws, and they serve as fuel for class action lawsuits from affected parties.

Conclusion

Ransomware continues to be costly for businesses large and small. Most attacks leverage malware strains developed by a handful of attack groups, and attackers continue to target popular remote access technologies as an initial vector of entry. In many ways, our findings confirm that the 2022 reduction in ransomware attacks was temporary and attackers are back to some of their old patterns.

The data also confirms what we've known to be true for several years: managing IT on-premises significantly increases the risk of an attack. While in previous years we've seen attackers target on-premises email servers or remote desktop protocol (RDP), in 2023 the focus was on self-managed VPNs. When compared to businesses with either cloud-based remote access technology or no VPN at all, organizations with self-managed VPNs were associated with a much higher frequency of an attack.

Another noteworthy evolution was the exfiltration of data to achieve double leverage by combining it with encryption tactics. When organizations improve their backup systems they are less likely to pay a ransom when their data is simply encrypted. By exfiltrating data, attackers threaten to leak internal and customer data to incentivize the organization to pay. The rise in double leverage incidents caused a meaningful increase in the "blast radius" of each ransomware attack, when multiple partners of each organization found themselves indirectly hit by having their private data included in the exfiltration.

This requires organizations to reevaluate which vendors or partners should hold their data, what protections are put in place, and whether that partner will be able to reimburse them for damages resulting from such a breach.

Our findings also highlight the fact that attack levels remain high. While targeted IT assets are predictable, organizations continue to struggle to fend off attackers. We believe this calls for higher accountability and scrutiny over the security of perimeter-facing technology, especially remote access technology. This also reinforces the importance of managed security, whether on the cloud or on premises — small organizations highly benefit from experts managing their security on their behalf.

By combining the prevention of security and the protection of insurance, companies can achieve better security and reduce risk. This is the power of the InsurSec model, helping small- and medium-sized businesses close the growing gap they have in security technology and management. And by bringing together security and insurance, we can provide clarity and transparency on drivers of risk, helping defenders, vendors and regulators better address growing cyber risks.

Methodology

At-Bay's analysis is based on claims information from 2021 through the end of 2023. 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 ransomware 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.

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.

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