at bay

at-bay.com

Backup Breakdown

How Data Recovery Impacts the Outcome of Cyberattacks

AUTHORS:

LIAT KLAINMAN, GREG OTTO

CONTRIBUTORS:

AYELET KUTNER, MATT ACTIPES, LARRY CROCKER, BRIAN WALSH, ADI DROR, SHAY UDELSMAN, ERIC MURPHY

Table of Contents

Executive Summary

In this report, At-Bay's Cyber Research team set out to quantify the importance and success rate of backups. The goal was to look at actual claims data to find out if the accepted wisdom that "backups help" is really true.

The team selected and reviewed claims involving ransomware from our entire claims database — which covers 50,000 policy years — to examine the impact of backups in reducing the total cost of a claim and business downtime after a cyberattack. Our research shows that while successful backups can save organizations a significant amount of money, many companies with backups in place struggle to successfully restore. The type of backup technology used also significantly affects the outcome of an attack, including the decision to pay a ransom, which underscores the importance of choosing the right backup technology and architecture.

This report shows that many businesses have a false sense of security when it comes to their backups, with 92% of our policyholders reporting that they had functioning backups in place but 31% of those failing when they needed to use them. For those that did successfully restore from backups, their claims had a 41% lower severity when compared to those who failed to restore from backups. Additionally, policyholders that successfully restored from backups were 3X less likely to pay a ransom when compared to those that failed to restore.

When examining backup architectures, cloud performed far better than the other options. The recovery rate for cloud backups was 1.5X better than offsite backups. The full data showed recovery rates of 80% for cloud backups, 67% for hybrid solutions, 56% for onsite, and 55% for offsite. Cloud backups, with their high recovery rate, were also most effective at reducing the likelihood of paying ransom and therefore lowering the overall cost of the claim.

Beyond the figures, this report also highlights how a solid backup strategy could lower cyber insurance premiums for businesses. Additionally, our Incident Response team and security partners share important lessons gleaned from working with At-Bay customers and actionable advice on what makes a backup successful.

Introduction

This should have been a boring report. For the longest time, backups were such a simple part of an IT inventory that they were almost an afterthought. Then ransomware emerged. Now, what was once a mundane technology has become, in many cases, the last line of defense safeguarding your company against the growing threat of cybercrime.

In recent years, ransomware groups all over the world have been increasingly active. These attacks can be devastating: attackers use malware to block a victim's access to their own files or systems, holding that data hostage and leveraging the threat of ruinous reputational or legal damages unless the victim pays a ransom to regain access to their data.

It's no surprise then that most cyber insurance companies consider backups to be a critical security control when offering coverage. The technology has proven to be crucial to organizations looking to protect sensitive data, avoid ransom payments, and quickly resume operations in the wake of an attack.

But what we find is that backups don't always work, and not all backup configurations are the same. Some configurations have a significantly higher chance for fast and successful recovery. That's why we decided to look more closely at our claims data to help quantify the real-world impact of these different architectures.

However, complexities involved in setting up and maintaining backups often pose challenges for organizations, which can lead to negative outcomes and increased costs. Many organizations fail to properly configure and operate backup solutions, resulting in failure to restore.

Our research found that backups can help reduce the severity of claims — both in terms of the cost of a claim and any downtime the business suffers.

We trust this report helps guide businesses toward making the best decisions for their organizations and incorporate it into their multi-layered cybersecurity and data protection strategy.

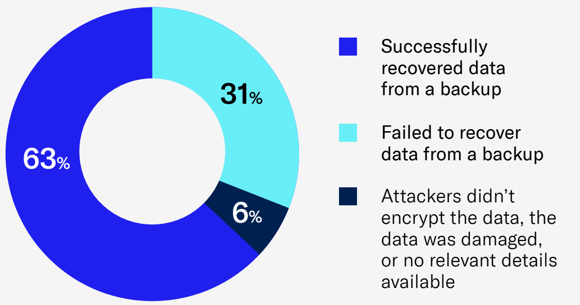
Data Findings & Analysis

31% of Businesses Were Unable to Restore From Backups After an Attack

Many organizations believe that having backups will protect them from the downtime and financial impacts of system failure. However, when businesses experience an attack, these backup systems are tested — and are often found wanting.

While 92% of At-Bay policyholders report having backups in place, our analysis of claims data – which examined 186 ransomware claims — found that only 63% of policyholders were able to successfully recover data from their backups, while 31% failed to restore data from their backups. (An additional 6% of the businesses in our analysis couldn't be categorized because attackers didn't encrypt the data, the data was damaged, or no relevant details were available.)

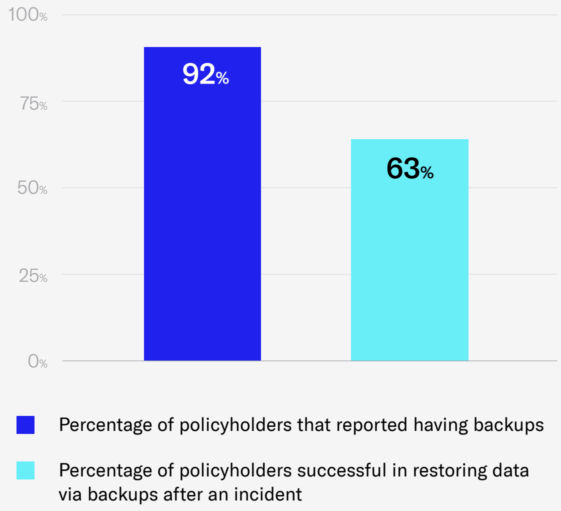
More than 1 in 4 Backups Failed to Restore



Source: At-Bay claims data where backups were involved

Many businesses may have a false sense of security around how much resilience their backups provide, when in reality more than 1 in 4 fail to recover their data from a backup when they need it most.

Having a Backup Does Not Guarantee Recovery



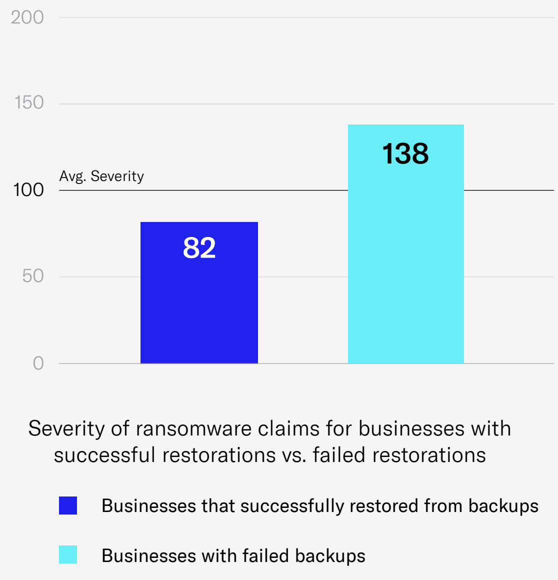
Source: At-Bay claims data where backups were involved

Effective Backups Decreased the Severity of a Ransomware Claim by 41%

Our research found that successful restoration from backups significantly reduced the severity of an incident and the likelihood of paying a ransom, underscoring the importance of having properly configured and tested backups.

For those 63% that were able to successfully restore from backups, the impact on severity was significant and quantifiable. The total cost of a ransomware claim for these businesses was 41% lower than that of businesses that failed to restore from backups.

A Successful Backup Reduced Losses by 41%



Severity of ransomware claims for businesses with successful restorations vs. failed restorations

Source: At-Bay claims data where backups were involved

Source: At-Bay claims data capped at $1 million in loss per claim. Severity Index calculated for all ransomware claims analyzed and adjusted for differences in company revenue, where the average claim severity = 100.

Depending on the size and scale of the business, that difference in attack severity could mean hundreds of thousands of dollars in losses.

Let's further examine that difference in severity. Of the 186 claims that were part of this data set, the average company revenue was approximately $55 million. The average cost for a ransomware claim (see total cost definition in the Methodology section) for a company in this data set amounted to approximately $343,000.

When further averaged out by a company's use of backups, the severity difference becomes clear. Companies in the data set **that successfully restored from backups** paid approximately $281,000 per claim, approximately $62,000 less than average. Companies in the data set **that did not successfully restore from backups** paid approximately $474,000 per claim, approximately $130,000 more than the average.

When examined together, the difference in the average claim cost between those who did and did not successfully restore from backups amounts to approximately $192,000.

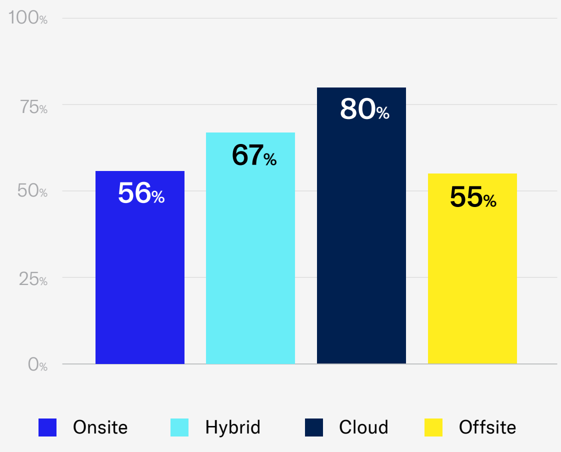
Different Backup Types, Different Outcomes

While backups are a crucial IT risk management solution, they are not all the same. Even as they help organizations protect against data loss, mitigate risk, facilitate business continuity, and aid in disaster recovery, our data shows that different backup architectures (see backup type definitions in the Methodology section) and the way an organization sets up its IT systems have a deep impact on data restoration and the associated costs of a ransomware attack.

Cloud backup architecture provides the best likelihood of a successful data restoration

Our research found that cloud backup solutions led to a successful recovery rate of 80%, which is approximately 1.5X better than offsite (55%). Onsite backups showed a 56% recovery rate and hybrid solutions were at 67%.

Recovery Rate for Cloud Backups Was 1.5X Better Than Offsite Backups



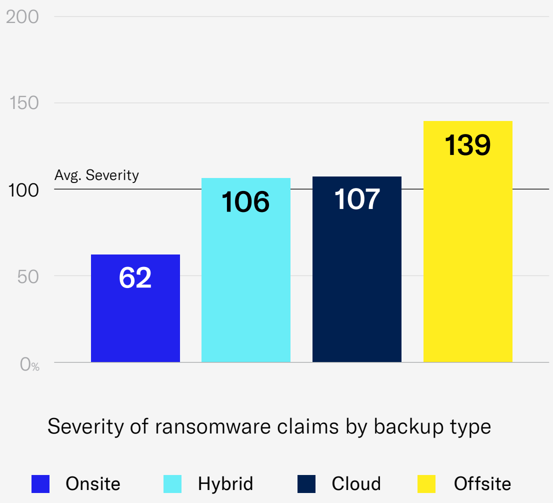
Source: At-Bay claims data where backups were involved

Severity of ransomware claims by backup type

However, when we index by severity of the attack (i.e., the total cost of the claim), the rankings change. Backups stored onsite had the lowest claim severity, followed by hybrid and cloud (nearly identical), and strictly offsite architecture with significantly higher severity. Overall, offsite backups saw 2.25X higher severity than onsite backups.

Hybrid backups in which offsite backups were part of the configuration drove the highest severity index of 163.

Backup Architecture Meaningfully Impacts Overall Cost of a Ransomware Claim



Source: At-Bay claims data where backups were involved

Source: At-Bay Claims data for report capped at $1 million in loss per claim. Severity Index calculated for all ransomware claims analyzed and adjusted for differences in company revenue, where the average claim severity = 100.

Why backup rankings by type stack up differently when considering recovery rate vs. severity/cost

In the experience of our Incident Response team, there are a few things that can explain this: in some cases, while the restoration of data was successful, there may have been other associated costs related to that effort. For instance, if an organization has many terabytes of data stored offsite, there may be an added cost to download all that data, on top of the cost of storing that huge volume of data once downloaded.

Other factors that can impact the total cost are the organization's lack of understanding about how to structure data to interact with vital applications or the disk space needed to store restorations if they originate from a cloud or hybrid backup, which can delay time to restore, leading to a more significant overall interruption to the business.

> **"With cloud backups, you are going to be at the mercy of your bandwidth. If your organization has on-premise backups, you can restore everything much faster through your local-area network, and this can result in a lower restoration cost overall."**
>
> Larry Crocker, Head of Incident Response, At-Bay

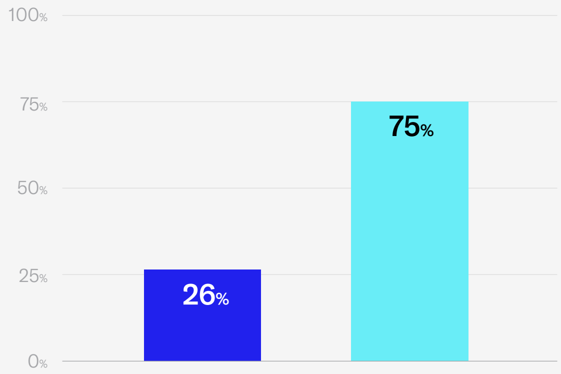
However, if an organization's onsite backup is connected to its network, the backup is also at risk of being damaged in a cyberattack. This offers one example of the many ways that data recovery can go wrong even for businesses that think they're prepared.

Ransomware Demands — To Pay or Not to Pay

Backups can serve as a critical factor in decision-making when dealing with ransomware attacks. Organizations that can successfully restore their data from backup are less likely to pay a ransom to recover encrypted data.

Our research shows that effective backups led to organizations avoiding substantial ransom payments. Businesses that were successful at restoring from backups paid ransom in only 26% of cases, compared to 75% of cases for those that couldn't successfully restore their data. **So in effect, policyholders unable to successfully restore from backups were 3X as likely to pay a ransom than those who were able to successfully restore their data.**

Businesses That Successfully Restore From Backups Are 3x Less Likely to Pay a Ransom



Likelihood of paying ransom for businesses with successful vs. failed backup restorations

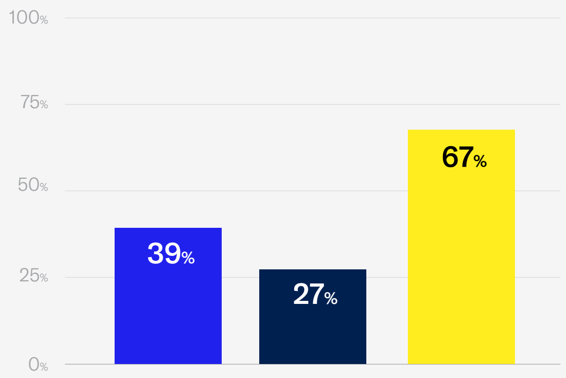
■ Businesses that successfully restored from backups

□ Businesses with failed backups

Source: At-Bay claims data where backups were involved

Additionally, when it comes to the frequency of ransom payments based on backup architecture, our data shows that organizations with offsite backups paid ransom 67% of the time, onsite 39% of the time, and those with cloud backups paid the least often at 27%.

Businesses With Offsite Backups Paid Ransom 2.5X More Often Than Those With Cloud Backups



Likelihood of paying ransom based on backup architecture

- 🟦 Businesses with onsite backups
- ■ Businesses with cloud backups
- 🟨 Businesses with offsite backups

Source: At-Bay claims data where backups were involved

In recent years, ransomware groups have evolved their tactics to target and compromise backup solutions, and in some cases exfiltrate the data to increase leverage over the victim.

We've reached a point where you may be asking: why would any company pay a ransom if they have successfully restored from a backup? Companies may still pay in order to avoid further data leaks, better respond to data privacy regulatory requirements, or protect their reputation for practical operational difficulties with the restoration process.

HIPAA, for example, has stringent notification laws. Healthcare companies impacted by ransomware may pay a ransom in an attempt to figure out exactly what the threat actor took (by purchasing that data back). It can be a lot less time-consuming than running digital forensics on systems in the company's environment to identify exactly what data has been breached. There is an obvious caveat: criminals are far from guaranteed to act in an organization's best interest. There is no guarantee attackers will comply with this type of request.

In other cases, companies pay a ransom to protect their reputation by buying the threat actor's silence to prevent them from leaking stolen, sensitive customer data. While paying a ransom may not always prevent cybercriminals from trying to sell or expose that data in the future, attempting to stop further sharing of that data is an option some victims may pursue in an attempt to settle any worries about a future incident.

The Insurance Perspective

Given that good backups materially decrease the cost of a ransomware incident (and the likelihood of paying a ransom), it will come as no surprise that the price an organization pays for cyber insurance can also vary by a company's use of backups.

When translated into cyber insurance premiums, the cost savings generated from an effective backup solution could reduce the company's cyber insurance premium by 25% on average.*

But it doesn't stop there — we know that the architecture of your backup can also help reduce your cyber risk. Backup strategies that result in smaller or less frequent losses help reduce risk, and can in turn impact your cyber insurance costs.

The table below illustrates hypothetical examples of the potential insurance pricing differences based on a company's size and backup architecture. These illustrated differences are based on the effectiveness of each architecture type to reduce risk of loss.

Based on this portfolio cost analysis, a typical company with an offsite backup solution could save up to 39% on their insurance costs by switching to an onsite backup, due purely to their lower expected claims costs.

As noted earlier, cloud backups perform best at reducing the likelihood of paying a ransom, whereas onsite backups produced the lowest claim costs overall. The example premiums calculated consider the full cost of potential claims, but the best backup for your business will vary based on a number of different factors.

Insurance Pricing Examples* for Businesses Using Low- to High-Risk Backup Architecture Based on At-Bay Claims Analysis

Backup Architecture	$25M Revenue	$50M Revenue	$100M Revenue
Onsite	$9,174	$13,622	$22,765
Hybrid	$12,497	$18,557	$31,013
Cloud	$12,567	$18,660	$31,185
Offsite	$14,937	$22,179	$37,066

**Pricing based on average policy within At-Bay Insurance Services LLC's portfolio with given revenue. Premiums represent potential rate differences due to differences in average claim cost associated with each backup solution. Actual premiums offered are based on a variety of factors. The values in this table are not indicative of future pricing, nor do they guarantee future coverage offerings. At-Bay Insurance Services LLC is a licensed property and casualty insurance agency and surplus lines broker in all fifty states and the District of Columbia.*

Ensuring Your Backups Work

Our Incident Response Team Weighs In

Similar to an insurance policy, a robust backup strategy serves as a lifeline, enabling business continuity in the wake of a cyberattack. Having such a strategy ultimately translates to enhanced resilience and less downtime in case of a catastrophic event, preserving both the valuable trust of clients and the stability of the organization.

But as this report highlights, restoring your data and systems from backups is not as simple as clicking a few buttons. Like other aspects of cybersecurity, a backup strategy should follow best practices that can maximize resiliency, enabling effective incident response and minimizing the impact of data loss or system disruptions.

Pulling from decades of experience in restoring systems, At-Bay's Incident Response team has some advice for organizations looking to enhance their backup strategy:

1. **Understand how your IT system works together.** It's not good enough to haphazardly copy data or other assets and back them up in one or two repositories. Cataloging and categorizing how your entire system works together is essential for successful restoration. Small businesses in particular struggle with determining what they have, where it sits in the network, and how those assets should be backed up.

   Indiscriminately dumping data into a backup often leads to trouble in the restoration process. Without knowing what data is being backed up and what applications interact with that data, organizations set themselves up for extra work during the restoration process, which means a longer path back to normal business operations.

> **"One of the hardest things about backups is understanding what you own and where it resides in your network, including endpoints, assets, data, admin accounts, and more. This is difficult, so it's really important to establish a strategic plan to ensure backup success."**
>
> Brian Walsh, Senior Engagement Manager - Incident Response, At-Bay

2. **Implement a strong password protection policy.** Service accounts are often used for backups, which can be a target for cyberattackers. An organization should go above and beyond to protect these passwords. Having a specific account for backups is highly recommended. Our Incident Response team team suggests setting up a separate account in Active Directory, with a more stringent password to protect from credential theft.

3. **Invest in the internet bandwidth you need.** If an organization has terabytes of data stored in a cloud-based backup but has a slow or unreliable internet connection, it will severely impede the speed at which it can restore data and resume normal operations.

   One thing to remember: you can only move data at a certain speed. For example, moving terabytes of data over ethernet could take days or even weeks.

4. **Test regularly to verify backup integrity.** It is vital to regularly verify the integrity of backups

by performing restoration tests. This ensures that the backup files are complete and can be successfully recovered, providing confidence in the process and your ability to restore data when needed.

> **“No matter what type of technology an organization uses, the biggest challenge is testing your backups on a regular basis to ensure that what you are backing up will actually work.”**
>
> Larry Crocker, Head of Incident Response, At-Bay

Regularly testing backups is akin to routinely rehearsing emergency evacuation drills. If a physical disaster strikes, organizations should have an escape plan that is methodical and organized in the face of a major threat. Restorations in the wake of a cyber attack should follow the same logic: testing backups can provide organizations with the confidence that their critical data can be accurately and completely restored in functionally usable form, ensuring their recovery process will be as swift and smooth as possible.

Expert Speak

3 Key Steps to Streamline Your Backup Strategy

Andy Fernandez
Director of Product Management
HYCU

No matter how technologically savvy an organization may be, managing backups can be a complex task, especially without the right tools and expertise.

As a company that specializes in data protection, HYCU has helped organizations formulate ways to protect their valuable data. However, I've seen companies of all sizes — not just small businesses — struggle with the optimal way to back up and successfully restore their data in the event of an attack. Here are some ways organizations can avoid failures with their backup strategy as they learn to maximize their use of modern technologies.

Backup is Easy, Recovery is Hard

One of the biggest pain points I've seen is that organizations fail to properly test their backups once they've determined how they plan to store business-critical data.

I've spoken to so many folks who didn't test their ability to recover data from backups until after an incident occurred. When they tried to recover their data, they realized that they didn't have the ability to back it up, their backups were corrupted, or there was another issue with the way they structured their backups that led to a failed restoration.

Besides continually testing, small businesses should also understand how data interacts with your applications — and how that will factor into your backup strategy. We refer to this as "purpose-built backups."

You simply cannot rely on bulk exports when you are restoring from backups. You want to make sure that you are protecting the workload that you have as it's meant to be protected. An organization should be able to make sure that it has visibility into the way the data and applications work together, and have a way to consolidate and orchestrate the protection of IT without having to allocate a lot of resources to this.

Avoid the "Spaghetti Monster"

When it comes to backups, there is no one-size-fits-all option. There are different technological architectures— cloud, onsite, offsite, hybrid — that, when coupled with an organization's unique backup processes and policies, can unintentionally add complexity to its security strategy.

It is imperative that both the architecture and strategy fit your business as seamlessly as possible to ensure a successful restoration. Many organizations don't fully understand how their backup architecture fits into their strategy, making things unnecessarily complicated in the process.

I like to call it the 'Spaghetti Monster.' Every single IT manager has to protect several different workloads that come from different places in the system. This can easily become a monster of scripts and configurations that are all a Rube Goldberg machine. The more complexity you have, the more difficult you'll find not only backing up, but actually restoring data.

A Holistic Plan for Protection

Procuring technology and obtaining coverage can be exceptionally helpful, but if an organization doesn't know how to use them in conjunction with one another, it may struggle to survive an attack.

Partnering with an InsurSec provider can be the catalyst small businesses need to craft a holistic security strategy. InsurSec is an integrated approach to protecting business from cyberthreats by bringing insurance and security together. It combines the best prevention and detection technology, the expertise of cyber professionals, and the backing of an insurance company, to protect a business in a way that neither of these solutions could do alone.

This holistic effort is an extremely important part of any organization's security plan. I liken it to using a parking garage: The garage is responsible for allowing you to have access to your spot. But if anybody touches your car or steals it, it's on you, right? Data is the same thing. If something happens to it, you are still responsible for protecting it.

To learn more about how At-Bay and HYCU can help strengthen your security posture, visit our Security Partner Network page.

Bringing Backups To The Forefront

The data in this report is clear: cloud-based backups are the best option for limiting risk and providing resilience. However, many organizations are not paying enough attention to the associated factors that impact the ability to successfully restore their organization's IT stack from backups, leading to additional downtime and money lost.

Organizations should understand how other factors — such as network bandwidth, data integrity, and system inventory — can impede restorations if not properly managed. Struggling with these factors will have an impact on how quickly an organization can resume normal operations in the wake of an attack. Cloud-based backups, when properly configured, better support these factors and can cut down on errors that occur in the restoration process.

While certainly better than having no backups at all, offsite backups led to poorer outcomes across the board. Claim costs are higher, more ransoms are paid, and losses are greater among organizations that depend on offsite backups. Given those statistics, we do not recommend making offsite backups part of an organization's restoration plan.

It's important to remember that backups are just one part of a holistic cybersecurity plan that includes strong security measures, regular patching/updating of systems, regular employee training, and a robust business continuity plan. Businesses of any size should partner with an InsurSec provider like At-Bay to ensure a strong backup strategy is in place.

Methodology

1. ***Data Sources & Methodology:***

   The data set used for the analysis in this report is from small to mid-sized businesses that held an At-Bay policy. We analyzed 186 ransomware claims in which backups were involved. Our goal was to understand the data restoration process and identify useful data points for predicting successful recovery from backups.

   By analyzing actual claims data, the At-Bay Cyber Research team set out to answer these questions:

   - *Do backups lead to successful restorations?*
   - *Which backup solutions are more effective?*
   - *How much do backups reduce the overall severity/cost of a ransomware attack?*
   - *How much can an organization save on cyber insurance premiums by having a backup in place?*

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

   Severity calculations include the total cost of a ransomware claim, which can include but is 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; and legal expenses, particularly if personally identifiable information was compromised.

2. ***Definition of a Successful Backup***

   For the purposes of this report, we are defining a "successful backup" as one that's up to date, includes all relevant systems, and partial or complete data was able to be restored by the company in a timely manner.

3. ***Definition of the Various Backup Types Mentioned in This Report***

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

   - ***Onsite Backups**: Onsite backups are stored on local storage devices within an organization's premises. This could be on dedicated servers, external hard drives, or even tapes. Onsite backups provide fast, convenient access to data, making restoration quick in the event of data loss. They do, however, possess additional risks: They are susceptible to physical damage from disasters (like a fire or flood) and theft. In the event of physical damage or theft affecting the company, their backups could also be compromised. They can also be affected by onsite cyber attacks if connected to an organization's network.*
   - ***Offsite Backups**: Offsite backups involve storing copies of data at a location separate from the primary business site. This could be a secondary office location, a dedicated offsite data center, or storage provided by a third-party vendor. The main advantage of offsite backups is that they provide protection against data loss in the event of a disaster at the primary location.*

- ***Cloud Backups***: *Cloud backups (also known as Backups-as-a-Service or BaaS) involve storing data with a third-party provider via the internet. With data stored in the cloud and/or data centers across various locations, you get the advantage of geo-redundancy — meaning your data is duplicated in multiple physical locations — further reducing the risk of data loss. Companies usually pay based on the amount of data they need to back up, allowing for scalability. Data can also be accessed and restored from anywhere with a good internet connection. The potential downsides of cloud backups include their reliance on a fast, stable internet connection for data downloads and ongoing cloud storage costs over time.*

- ***Hybrid Backups***: *A hybrid backup combines multiple methods or technologies and can be any combination of the above configurations. Typically, it involves a combination of onsite (local) and offsite (remote or cloud-based) backup solutions. This aims to provide a balance between the advantages of quick access and control offered by local backups and the security and redundancy provided by offsite backups. Even if one backup is compromised, a copy remains safe in the other options, ready to be used for restoration. Hybrid backups are designed to offer a robust and flexible data protection strategy, minimizing the risk of data loss and downtime while providing a level of redundancy and security that local or cloud backups may not achieve on their own.*

Contributors

Liat Klainman

Cyber Data Analyst

Liat Klainman is a Cyber Data Analyst at At-Bay, specializing in the cybersecurity sector and focusing on product improvements based on insights. She specializes in creating reports, building dashboards and visualizing data.

Ayelet Kutner

Chief Technology Officer

Ayelet Kutner is the CTO and GM of At-Bay's Tel Aviv office, leading the R&D, Product, Data Science, and Cyber Research teams. She was previously VP of Engineering at Forescout and Head of Platforms, SMB, and Industrial Control Systems Products at Check Point.

Brian Walsh

Senior Engagement Manager of Incident Response

Brian Walsh is the Senior Engagement Manager of Incident Response at At-Bay, where he is responsible for post-breach client engagement, post-breach response and investigation, digital forensics investigations, and reverse engineering malware.

Adi Dror

Cyber Researcher

Adi Dror is a Cyber Researcher in At-Bay's Tel Aviv office. Prior to joining the company, she spent three years at Unit 8200 and JCDI in the Israeli Defense Forces.

Eric Murphy

Senior Actuarial Manager

Eric Murphy is the Senior Actuarial Manager of Pricing at At-Bay, where he oversees the maintenance of the company's pricing model and overall program profitability. He previously worked at Esurance, where he led a team of actuaries to develop pricing strategies.

Greg Otto

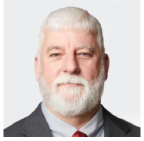
Senior Security Writer

Greg Otto is a Sr. Security Writer for At-Bay. He is an award-winning cybersecurity journalist, most notably during his stint as Editor-in-Chief of CyberScoop from 2016-2020. He has also led content initiatives at Intel 471 and Trail of Bits.

Matt Actipes

Actuary

Matt Actipes is an Actuary at At-Bay specializing in cyber products. He has over 7 years of pricing and predictive modeling experience in property and casualty insurance, with a focus on personal and commercial lines.



Larry Crocker

Head of Digital Forensics and Incident Response

Larry Crocker is the Head of Incident Response at At-Bay, responsible for post-breach remediation, digital forensics investigations, and threat hunting services. Larry has decades of experience in cybersecurity, having led teams at Kivu Consulting and Dell SecureWorks.

Shay Udelsman

Cyber Researcher

Shay is a Cyber Researcher in At-Bay's Tel Aviv office. Prior to joining the company, she spent four years as an intelligence analyst at Unit 8200 in the Israeli Defense Forces.

This document is intended for information purposes only and does not modify or invalidate any of the provisions, exclusions, terms or conditions of the policy and endorsements. For specific terms and conditions, please refer to the coverage form. At-Bay Insurance Services LLC is a licensed insurance agency and surplus lines broker in all fifty states and the District of Columbia.