A HACKER'S GUIDE

Ransomware Mitigation and Recovery

By Hector Xavier Monsegur
and Andy Stone

PURESTORAGE®

Table of Contents

Introduction

The battle against ransomware attacks has intensified with a staggering 37.75% uptick[1] between April 2022 and April 2023.

Recent, headline-making cybersecurity incidents on universities, healthcare systems, utility companies, and even the world's largest casino chains have only highlighted the stark reality that no organization is immune—and the stakes are only getting higher. As the threat landscape continues to evolve, cybercriminals are becoming increasingly bold and sophisticated with ransom amounts surging. Simply put, there's no time like the present to prioritize your ransomware threats, detection, and response efforts.

A Hacker's Guide to Ransomware Mitigation and Recovery was created to provide a detailed look at today's ransomware threat landscape, as well as expert guidance to help you prepare for attacks and safeguard your organization's data.

What You'll Learn

1. Why ransomware attacks are on the rise
2. Attackers' modus operandi before and after an attack happens
3. What you can do to mitigate your risk of an attack and minimize data loss should one occur
4. What to do if you detect an attack in progress
5. How to quickly recover and restore after an attack

Today's Threat Landscape

From the mid-2000s through the early 2010s, it was common for "hacktivists" to launch cyberattacks to further social or political causes, but these loosely organized, international groups have cut back their activities significantly in recent years. Improved security postures within organizations have greatly reduced the effectiveness of neophyte hackers who focus on low-hanging fruit. Arrests and prosecutions against members of hacktivist groups like Anonymous and LulzSec helped to temporarily thwart attacks.

Yet despite the decline in hacktivist activity, the threat of cyberattacks continue. In 2022, organizations around the world detected nearly half a billion ransomware attacks, with a ransomware or phishing attack occurring every 11 seconds.

Today, the primary source of ransomware attacks is state-sponsored, ransomware extortion groups that often work together, reflecting global collaboration and an increased sophistication of attacks.

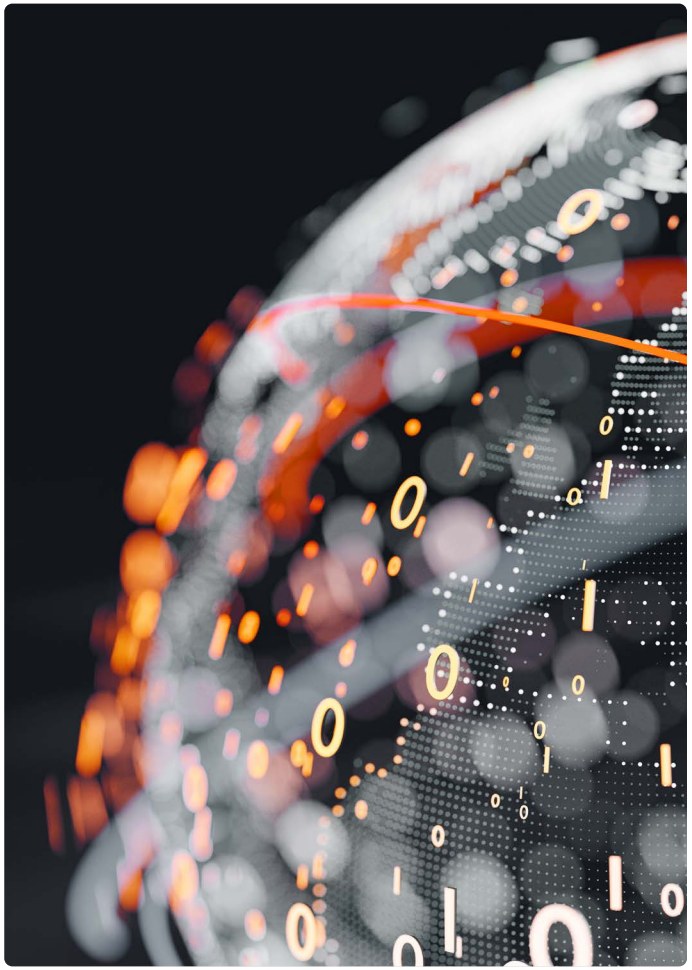
These groups help distribute ransomware as service “kits” that can be purchased on the “dark web,” enabling skilled (and more increasingly, unskilled) private sector, offensive actors to rent out their capabilities, like mercenaries. Nation states find this a cost effective way to fund ransomware operations with the intention of causing disruptions.

Another recent development, which is particularly challenging for victims and security professionals alike, is encryption-less ransom attacks. In this scenario, attackers bypass encryption to directly target and compromise essential systems and data, propelling the need to understand the techniques leading up to attacks to develop effective mitigation strategies.

Artificial intelligence (AI) has also taken center stage when it comes to cybersecurity. Ransomware groups are upping their game, using AI-developed malware code, chatbots, and more to develop complex ways to get past traditional cybersecurity measures.

In response to these escalating cyber threats, the U.S. government has raised ransomware to the top of its national security agenda, releasing new policies surrounding ransomware payments and holding countries accountable for harboring cybercriminals. They have even outlined steps that businesses can take to bolster their defenses in response to current ransomware threats.

Resiliency Is Top Priority in 2023 White House Cybersecurity Strategy



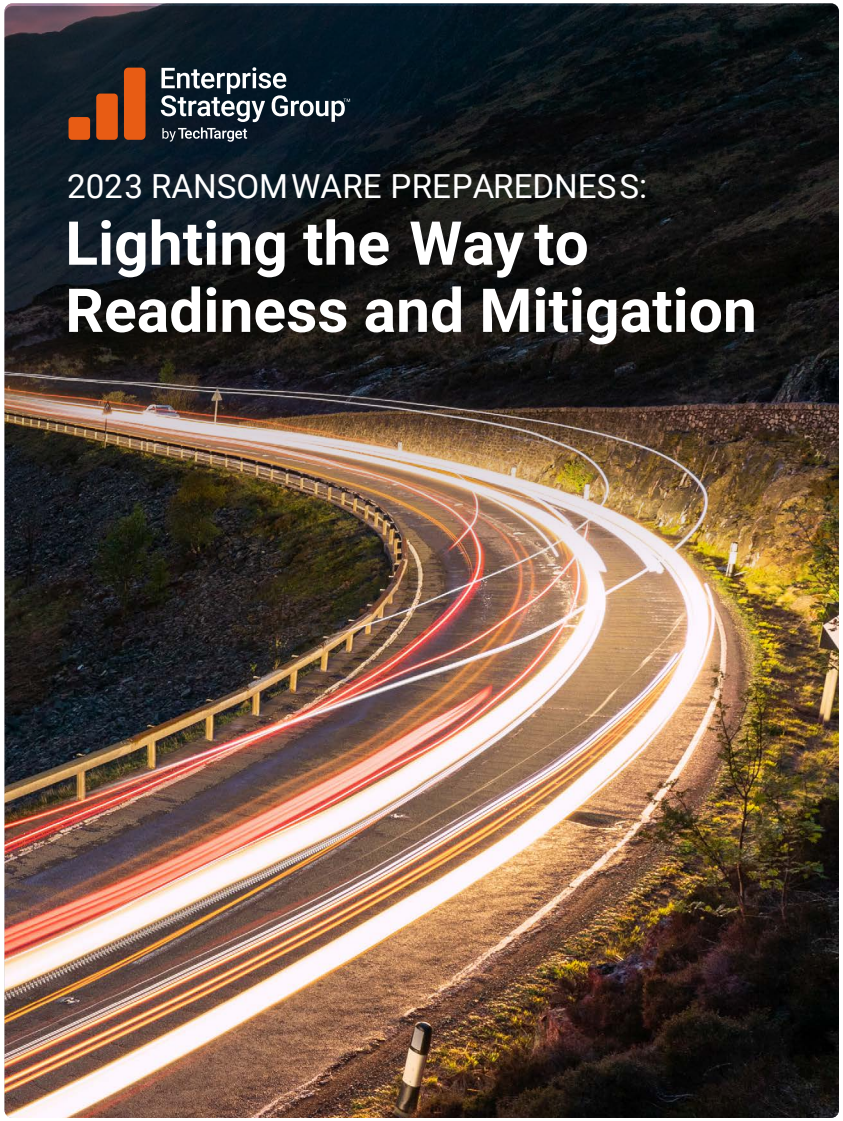
Financial Motivations

With the shift in actors has come changing motivations for attacks. Years back, “hacktivists” were motivated by political views, cultural or religious beliefs, national pride, or terrorist ideology. Today, the key motivation for ransomware attacks is financial, with ransoms becoming increasingly costly, topping an average $740,000 in 2023.[2]

One factor that has contributed to skyrocketing ransom amounts is the role of cyber insurance. Cyber insurance providers have historically had a tendency to quickly give in to attackers’ demands for ransom. This has emboldened hackers to increase their efforts and has resulted in sharp increases in cyber insurance premiums with tighter terms and conditions, and greater scrutiny from underwriters.

With cyber insurance becoming increasingly difficult to secure and price prohibitive, enterprises with larger budgets for cyber risk management infrastructure are far more likely to have cyber insurance than small businesses, and in turn, are more lucrative targets for bad actors. Attackers have even been known to research how much insurance a target company has and then ask their victim to pay that amount. When the victim says they don’t have the money, the attackers point to the victim’s insurance policy.

However, it’s important to stress that organizations of all sizes are targets of cybercriminals. And as long as ransoms are being paid, bad actors will continue to attack and find new ways to exploit their victims.



Read the Ebook

Paying the Ransom Is Just the Beginning

Of course, cyber insurance only goes so far when it comes to the total cost of a ransomware attack.

Even organizations that have the means to pay ransom often discover much bigger, more costly problems as they move forward. According to the FBI[3], total losses due to cybercrime in 2022 reached a staggering $10.2 billion, reflecting an increase of nearly 48%. IBM's latest data breach report indicates that the average cost of a ransomware attack, not including the ransom, now tops $4.5 million[4]. This is a combined cost that often includes operational disruption, reputational damage, investment in new security implementations, legal action, and more.

Low Risk for Attackers

From the attackers' perspectives, crypto currencies have made ransom demands relatively low risk.

For example JBS allegedly paid $11 million (using Bitcoin) as ransom to get back online after its recent ransomware attack. Analysts say that Bitcoin and other cryptocurrencies, such as Monero and Zcash, make it possible to extort huge ransoms from large companies. Because these transactions are anonymous, there's little chance of getting caught.

The Ransomware Task Force, an international coalition of government officials, private sector technologists, and law enforcement, have reported that crypto currencies add to the challenge of tracking down ransomware criminals because of the borderless nature of these types of digital currency.

Inadequate Cybersecurity Measures

Another key contributor to the proliferation of ransomware attacks is the fact that most organizations do not have sufficient defenses.

Because of this, it's not surprising that one in three IT leaders express serious concerns about the security of their backup and recovery infrastructure. Many are failing to address obvious security gaps. IT teams are often focused on sexy new security technology but don't practice good security hygiene, such as password authentication, identity management, backup policies, and incident management. These hygiene lapses make life easy for attackers who typically focus on finding the easiest, most cost-effective way to get into an organization's systems.

Threat Patterns and Analysis[6]

83%

Of breaches involved external actors with the majority being financially motivated.

74%

Of breaches involved the human element, which includes social engineering attacks, errors, or misuse.

Don’t Overlook the Human Factor

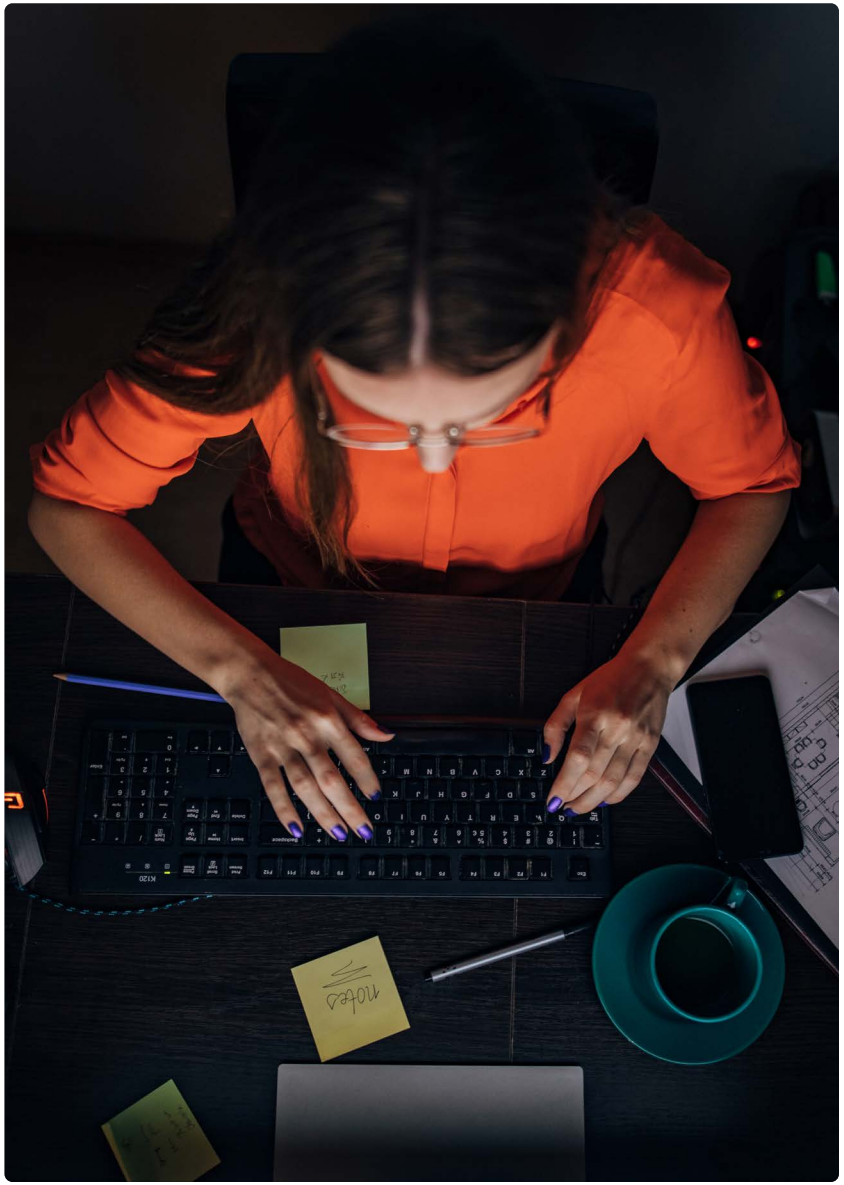
Cybersecurity measures also often fail to account for human psychology. Of all the attacks we’ve seen, only a small percentage were technical ones that used exploits, zero-day attacks, or direct compromise of services.

Most attacks start with a human. Such attacks use phishing emails, vishing, or some other interaction between the attacker, their automated systems or tools, and the victim that enable the attacker to steal a user’s login credentials. Attackers then use these credentials to log into the network just like any other user.

Humans fall prey to these attacks for many psychological reasons. They may not be adequately trained. They may want to help people. They may be afraid of looking incompetent. They may fear losing their job. For all these reasons, if they see a link from their CEO, they click on it. If launching a social engineering campaign can get attackers inside a billion dollar company after just a few days of setup and $100 or less in setup costs, it can be a huge, very profitable win.

Another issue comes from the inside. We’ve seen nation states and other attackers bribe employees and pay them to set up ransomware inside the organization.

Thus, the combination of security measures, bribery, and human psychology, where employees surrender their access credentials to phishing attacks, results in successful compromises that enable attackers to move laterally across the internal network and ultimately to ransomware attacks.



The Three Pillars of Ransomware Protection

With most enterprises encountering a ransomware attack in the last 12 months, preparation isn't just a good idea; it's a necessity for doing business today. This means becoming educated on how hackers operate and developing a plan that spells out what you should do before, during, and after a ransomware attack. The following are specific recommendations based on my experiences both as an attacker and as a consultant working with organizations to defend against attacks.

The Three Pillars

1. Before an Attack
2. During the Attack
3. Restoring Your Data after an Attack

PILLAR 1

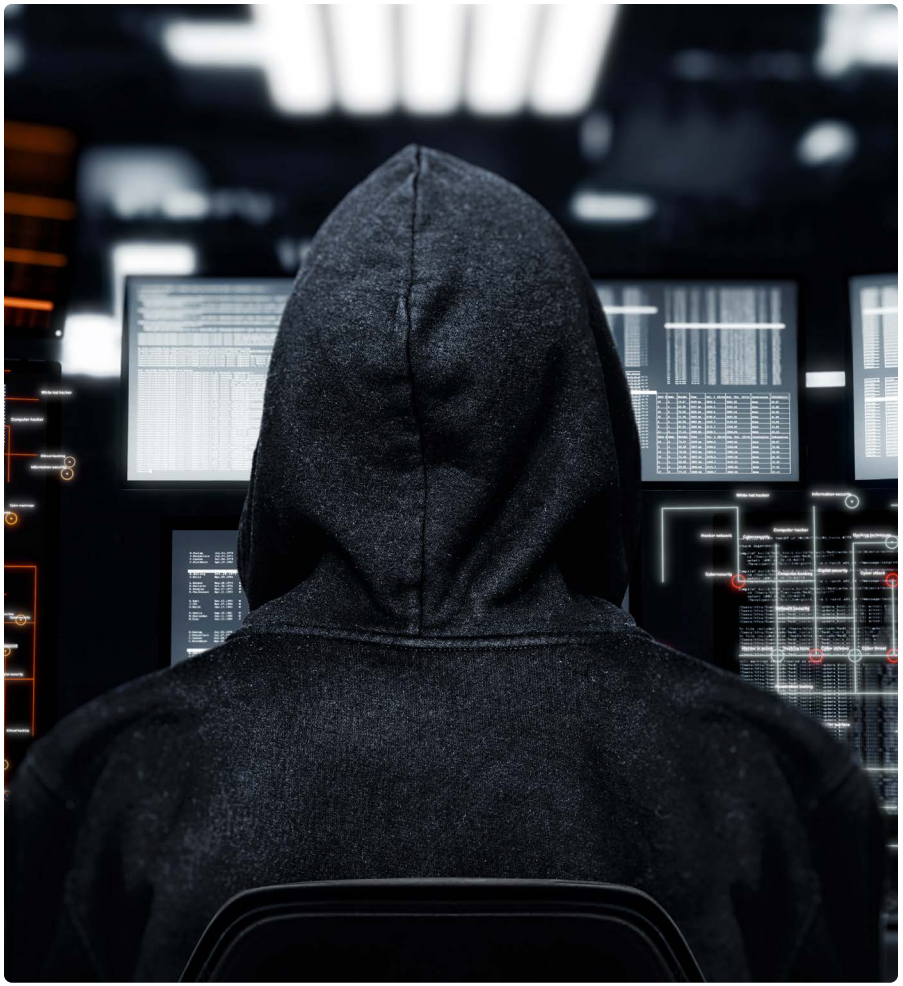
Before an Attack

Before cybercriminals attack, they perform reconnaissance to identify targets. They may begin by looking for companies with cyber insurance that are more likely to pay a ransom. And they'll have a defined methodology for sizing up a target's attack surface, looking for weakness in that attack surface and creating an appropriate attack path.

For example, an attacker might hone in on a target like a small ISP that works with multi-billion dollar corporations. The attacker will uncover potential entry ways to that ISP by identifying:

- Support staff they can social engineer
- Services, tools, or software the ISP uses and the breadth of the attack surface
- Internal host names from published SSL certificates
- DNS names or host names pointing to hijackable resources

Once an attacker gains entry to an ISP, they can access the larger corporation.



What You Can Do Before an Attack Occurs

To thwart these reconnaissance efforts and prevent a potential attack, it's critical to be both proactive and preemptive. In other words, you'll want to put in place a robust cybersecurity plan before anything happens.

To create your plan, take the following steps:

1 Gain Visibility

Start by obtaining technical, operational, and organizational visibility.

- **Technical visibility** requires a full understanding of the connected devices you have on your network, where they are vulnerable, and the threats to them. This entails putting the right tools in place to get visibility into your system, so you can identify anomalies. For example, a fast analytics platform can help spot suspicious behavior, anomalies, and more before an attacker breaks in, enabling you to identify threats and eradicate them before your data is widely compromised.
- **Operational visibility** will prevent phishing attacks which make up the majority of cybersecurity incidents. This means gaining a full understanding of how and why people are accessing data, as well as what cybersecurity training you're providing.
- **Organizational visibility** will help mitigate lost business due to reputation damage—the largest contributing factor to data breach costs. This requires the ability to assess the extent to which an attack could damage your company's brand, reputation, or intellectual property.

2 Get Control

Once you know what you have on your network, eliminate obvious holes in your attack surface by performing all necessary security hygiene. For example, make sure routers and firewalls are properly configured, keep your IT systems patched, upgrade to the latest versions, keep whitelists and blacklists updated, enforce strong password rules and multi-factor authentication (MFA).

3 Reduce the Surface Area of Your Environment

Safeguarding your network is easier with a smaller attack surface. Reducing your surface area is about eliminating duplication. For example, having fewer versions of Windows or Linux makes it easier to manage and maintain them in a consistent manner.

4 Increase the Cost of an Attack

Attackers seek out the easiest avenues for access. When I was an adversary, I placed an emphasis on targeting services and vectors that I was intimately familiar with. So, to thwart attackers, you simply need to make it incrementally harder for an attacker to get into your environment than into that of the guy next door. You can make life more difficult for attackers by:

- Putting in place the right tools, such as centralized logging and events.
- Partnering with your solution vendors to understand the features offered and to implement them properly.
- Maintaining good system hygiene.

5 Build a Tiered Resiliency Architecture

A tiered resiliency architecture built by Pure Storage® can offer several layers of defense.

- For Tier 1 data and applications (i.e. core databases and application services, along with their defined dependencies), house three to seven days of SafeMode™ Snapshots on FlashArray//X™, FlashArray//XL™, or FlashArray//C™.
- Build a snapshot archive for Tier 2 on FlashArray//C, FlashBlade//S™, or FlashBlade//E™ for long-term storage (3+ months) or compliance needs.
- For extreme scenarios, use FlashArray//C or FlashBlade//S with ISVs and enterprise application native solutions to allow backup data to be written directly to the array, protected with immutable snapshots and SafeMode. You could also use FlashBlade//E to replace traditional spinning disk backups.
- An optional fourth layer of defense would comprise a one-way-in data bunker built on FlashArray//C or FlashBlade//S that's used for large-scale disasters.

6 Create a Response Policy

Invest the time to compile a response playbook that spells out policies for how your organization should respond to an attack before one occurs. Such policies will be unique for each company but may include:

- Analyzing SIEM logs for events to identify potential compromised systems and users
- Contacting the incident response team and incident response vendors
- Shutting down connections to the internet
- Turning off machines
- Communicating with law enforcement
- Preparing an incident report for the C-suite and the board

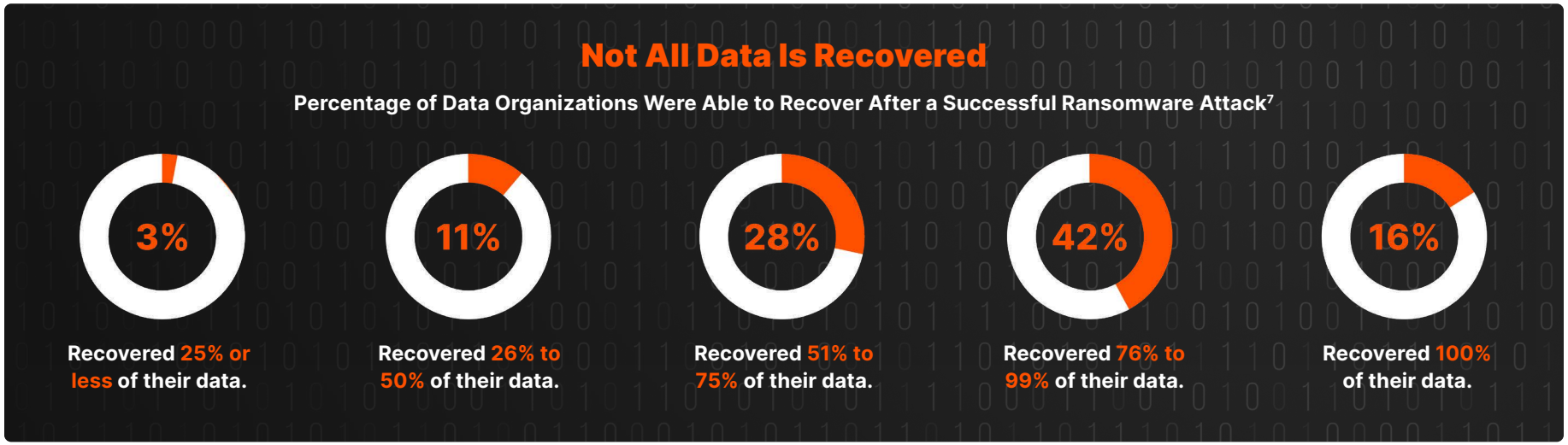
7 Provide Proper Training

Make sure the IT staff who monitor your security tools understand what the logs mean and how to react when anomalies are detected.

8 Build a Comprehensive Business Continuity and Disaster Recovery Plan

Despite proactive planning, an attack can still shut you down. You need to be prepared to recover as quickly as possible by creating a comprehensive business continuity and disaster recovery (BCDR) plan.

- Define what applications and systems you have in your environment and which ones are most critical.
- Work with your line of business teams to understand how quickly they need and expect to have data back online, so you can put in place the right systems and controls to meet SLAs.
- Implement the right architecture for backing up your data and building tiers of recoverability.
- Sit down with your backup vendors to understand what your products do and how to properly implement them. Because hackers are more likely than ever to target backup data and metadata, you'll want to choose a storage vendor that offers immutable, read-only snapshots of backup data and associated metadata catalogs.
- Test everything to ensure you can recover quickly should unplanned downtime occurs, regardless of the cause.
- Beware that attackers will target your critical infrastructure. If they do, you won't be able to access your core systems or use remote access tools or even email. You'll need to plan for how to get the right people to the right places. You'll need to specify who to call, in what order, where they should go, and what they need to do there.



PILLAR 2

During the Attack

During an attack, cybercriminals begin exploiting weaknesses in your company's attack surface.

For example, say that during surveillance, an attacker found a DNS hostname that points to a vulnerable WordPress blog. The attacker might now compromise that instance to get access to the server hosting it. They might then start a phishing campaign that uses that URL with the host name included to convince employees to click on a link to a false webpage where they request the user's credentials for the company's internal network or VPN.

Once the attacker uses these stolen credentials to get on the network, the attacker can then move laterally, accessing servers to exfiltrate data, steal intellectual property, or launch a ransomware campaign. These attacks can work very quickly, potentially spreading across your enterprise in 30-40 minutes, while going into your backups and deleting them and/or changing your credentials, so you can't get in. Alternatively, after the initial entry, the attacker may sit there for weeks or months, monitoring the network to see how you'll respond and then creating an attack plan or strategy and deploying the ransomware. Thus, just because the network is quiet doesn't mean an attacker isn't lurking on it.

What to Do During an Attack

Assuming that you have all the proper network monitoring tools in place, such as SIEM logs, a well-trained staff looking for anomalies and events will be able to identify an attack in action. When it does, it's time to leap into action.

1 Identify the Attack

You can identify an attack by finding anomalies in events, network traffic types, or protocols being used. Anomalies are simply events that don't make sense. For example, you might see an employee logging into the domain controller, or a secretary logging into the backup server. These activities indicate a lateral move where the attacker has compromised the user's credentials and is using them to log into systems they shouldn't be logging into.

Another tipoff to an attack is the kind of traffic on the network. For example, IPv6 traffic on the internal network is often used to bypass security products implemented to monitor IPv4 traffic, so seeing this type of traffic on a network with zero IPv6 use may be an indicator of compromise. It should be noted that Windows systems may send out DHCPv6 requests looking for connectivity and DNS details that can be supplied by an adversary without much privilege beyond listening and responding to broadcast requests.

Further indications of attack can come from broadcast communications like LLMNR and NBT-NS. These protocols broadcast name translation requests. If a server responds back to such broadcast requests with arbitrary hosts, it's a dead giveaway for defenders that an attacker is in the network. Attackers also commonly use low-hanging fruit attacks on internal Windows networks.

2 Execute Your Plan

Once you've confirmed that you're under attack, it's time to execute the response plan you've mapped out previously. Following your incident response plan and recovery procedures is extremely important. Otherwise, network and systems administrators are left using their own judgment to neutralize the threat, which in my experience is usually ineffective or even potentially disastrous.

3 Prepare for Investigations

Contact those in charge of incident response, communicate with your leadership and legal teams, and prepare your environment for investigations down the line with your vendors and/or law enforcement. If you've brought in a company to do an investigation, make sure there's a successful handoff between them and law enforcement.

4 Should You Pay the Ransom?

As a general rule, I don't think organizations should pay a ransom as it only encourages attacks. For example, a report by Cybereason found that 80% of organizations that paid the ransom were hit again.

But there are many variables involved. For example, if you are an intensive care hospital, and physicians won't be able to treat patients without these systems, you might need to pay the ransom immediately. In other words, you'll want to evaluate the need to make a ransom payment based on your specific circumstances.

And whatever you do, beware that attackers may double or triple dip. Not only do they encrypt the data and get you to pay, they may also extort you to pay even more, or they'll post your data online. Finally, they will threaten to tell the media to make sure your customers know about the attack. This disclosure can lead to additional legal costs, the need for regulatory compliance filings, and significant reputation damage.

5 What Happens If You Don't Have a Security Plan?

Unfortunately, many organizations don't have a security and recoverability plan in place due to constraints that include lack of budget or manpower. If the organization has a security team, individual roles may not be properly defined.

If you don't have a response plan, things can get very dicey because your security team won't know what to do. If a security engineer, analyst, or incident responder identifies the attack without having a policy to give them a structure to work with, you could end up in total confusion. You may not understand the full scope of the compromise. They might take systems offline that don't need to be offline. Or, you may simply be unable to provide your incident response vendor or internal team with enough information to pass on to help address the scenario.

More Victims Are Paying Ransom[8]

2022	2023	
46%	46%	Paid Ransom to Get Data Back
73%	70%	Used Backups to Get Data Back
8%	2%	Used Other Means to Get Data Back
61%	97%	Total Using Encryption That Got Data Back

PILLAR 3

Restoring Your Data after an Attack

Every minute your business is offline costs you money.

According to the Information Technology Intelligence Consulting (ITIC), a single hour of downtime costs approximately $300,000 for the majority of enterprises. And for large companies like Costco or Target or Walmart, the costs can easily rise to millions of dollars per minute. The average downtime for businesses as a result of a ransomware attack now stands at 24 days.[9] And fully recovering from an attack takes even longer—from several weeks to multiple months.

With these high costs in mind, the shorter the duration of any breach the better. After the attack, you'll want to clean up and restore your systems as soon as possible.

Steps to Take after an Attack

1 Clean Up Your Systems

During the attack, your defense team should have isolated and disconnected compromised network systems. Once the attack is over, it's time to fully audit all the systems on your network to make sure no artifacts or malware remains. Otherwise, you might find yourself in a situation where you shut down multiple systems, do migrations, restore your data, and get the network back online only to have the automated ransomware reactivate. So, make sure you sanitize your environment before you restore data from your backups and go live.

2 Rapid Restore

Before you were attacked, you should have established proactive and preemptive recovery measures including implementing a BCDR plan. These plans should include having backups that you can restore from that were not deleted. You should also make sure you can recover quickly because every minute you're down costs you money. However, in order to effectively and rapidly restore, you must have a current or very recent point of recoverability. Without that, your recovery process will be slowed or even impossible. Ensuring your storage and backup solutions offer a degree of recoverability is absolutely critical. A good solution is to leverage modern storage technologies that prevent attackers from fully deleting your organization's data.

Don't overlook the fact that after an event, your existing arrays will be off-limits. That means that any affected array flagged for forensic investigation by insurance or law enforcement cannot be used. Pure Storage's Ransomware Recovery SLA guarantees clean arrays and a recovery plan to get systems back up and running fast.

Pure partners with leading data protection companies like Cohesity, Commvault, Rubrik, Veeam, and Veritas. Our systems are tested to ensure they will work seamlessly with your software and ensure you won't need to go through a forklift upgrade.

It's also important to have the appropriate sandbox environment available for forensic analysis of your snapshots and backup data. You can't just restore directly without performing a forensic review and cleansing to remove identified indicators of compromise left behind by the attacker. Having a solid logging environment in place that delivers the proper visibility will be critical through your restoration process as you seek to find "patient zero" in the attack.

3 Adapt, Recover, and Respond

After you're back up and running, it's important to review what happened, learn from that, and modify your systems and policies accordingly so you can move on in an educated manner. This postmortem evaluation should look not only at technology, but also at people and processes. For example, you may find that you need to educate users more comprehensively to recognize phishing attacks. By evaluating lessons learned and incorporating them into your plans and policies, you can continuously improve your readiness and response.

Conclusion

By understanding why and how ransomware attacks occur as well as what you should be doing before, during and after an attack occurs, you should be better prepared to prevent an attack or recover quickly. These actions should include putting in place the right tools, from the right vendor, with the proper implementation, and providing education for both your technical team and end users. You should also ensure that strong passwords are set and managed properly, as well as inventory your software and assets so you can protect them and minimize your attack surface.

Pure Storage solutions can help with these efforts by ensuring your data is safe from encryption, that it's stored in a protected manner, and that it leverages an out-of-band, multi-factor authentication approach to ensure that even people or processes with administrative access cannot fully delete data without manual interaction and intervention from Pure support. Pure Storage products and solutions ensure you have a starting point for recoverability and provide the fastest recovery solution available to get your business back up and running quickly.

Learn More about Pure Storage Ransomware Solutions

Endnotes:

1 - Zscaler ThreatLabz 2023 Ransomware Report | Zscaler, 2023

2 - Average amount of cyber ransom payments | Statista, 2023

3 - FBI Internet Crime Report | Federal Bureau of Investigation Internet Crime Complaint Center, 2022

4 - Cost of a Data Breach Report 2023 | IBM, 2023

5 - Lighting the Way to Ransomware Readiness and Mitigation | ESG, 2023

6 - 2023 Data Breach Investigation Report | Verizon, 2023

7 - Lighting the Way to Ransomware Readiness and Mitigation | ESG, 2023

8 - The State of Ransomware 2023 | Sophos, 2023

9 - Average Duration of Downtime After a Ransomware Attack | Statista, 2023

Author Bios

Hector Xavier Monsegur

Hector Monsegur is an internationally recognized expert on global cyber security issues and a leading voice on cyber-attacks and cyber warfare. Formerly known by his online alias "Sabu," Monsegur was once the technical expert behind the Anonymous/LulzSec hacker collectives. As a "black hat hacker", he highlighted critical vulnerabilities in numerous organizations, including governments, military organizations, and cyber security firms. Later, in working with the US Government, Monsegur identified key vulnerabilities—and potential attacks—against major federal infrastructure, including the US military and NASA. Since working with US government and commercial security executives around the world, he has helped prevent upwards of 350 cyber-attacks against US government computer systems. Today, Monsegur works to identify vulnerabilities and secure client systems across many industries including technology, healthcare, finance, and government. In his leadership role, his unmatched technical experience is shared to both educate other operators and guide technical research.

Andy Stone

Andy Stone joined Pure Storage in April 2019 as CTO – Americas where he supports go-to-market and internal, product development activities. Prior to joining Pure, Andy worked at PwC as US and Global Chief Technology Officer and Global Head of Security Technology and Engineering supporting the Firm's 160 global territories and nearly 300,000 users. At PwC, Andy implemented a number of global technology solutions to improve overall usability, scalability and security posture while enhancing overall IT services' performance. He also led efforts to virtualize PwC desktops to improve end-user usability and protect from outside attacks and internal data leakage. Prior to PwC, Andy was the Farmers CISO and Global Head of Security Engineering, Architecture, Technology and Strategy for Zurich Insurance where he led a global security transformation across 140+ countries. Andy has also worked for Accenture, leading the creation of multiple security offerings including Identity and Access Management and Application Security as well as the Power of 3 security alliance between Accenture, Avanade, and Microsoft. He also worked with numerous, Global Fortune 500 companies, where he provided thought leadership and helped design, implement and support a broad set of custom and commercial technology solutions. Andy holds a BS in Business – Information Systems from Indiana University, Bloomington and an MBA from the University of Southern California. Andy has been presented at numerous conferences and been published on several topics in security and other technologies. Lastly, Andy holds patents in the security space for various identity and access management technologies.

PS2534-01-en 01/24