tierpoint

Strengthening Cyber Resilience Against Ransomware

A Guide to Ransomware Protection

As long as ransomware attacks continue to work, cybercriminals will use the technique to extort money from businesses. Building cyber resilience against ransomware means that businesses will need to adopt a holistic and continuous protection strategy, integrating proactive defense measures alongside robust resilience strategies, to keep attackers at bay.

Threat actors use ransomware as part of cyberattacks to lock up important data and demand money in the form of cryptocurrency to return and unlock the data. This type of attack can come from inside or outside of the organization. If the ransom isn't paid, the data remains encrypted, gets deleted, or can be publicly exposed. Sometimes, even when organizations pay the ransom, the data is not returned.

Ransomware attacks cause significant disruptions to business operations and can lead to revenue loss, steep decreases in productivity, and tarnished reputations.

Focus on a balanced approach with both defense and resilience capabilities. Balanced investments in defensive security tools and modern data resilience and recovery can reduce the risk and impact of impending business disruption brought about by ransomware. Improving cyber resilience against ransomware with balanced prevention, detection, protection, and recovery can enhance business value, reduce the business impact and cost of a breach, prepare an organization for cyber insurance, and increase trust and confidence both inside and outside of the business.

Ransomware Threat Landscape

Ransomware is still part of an evolving threat landscape. As companies build safeguards against ransomware attacks, cybercriminals find new ways to infiltrate IT infrastructure.

In 2023, 75% of organizations have had at least one ransomware attack in the past twelve months. These are not small events and can be quite expensive, with the average global cost of a data breach coming in at $4.45 million.

It's not uncommon for organizations to miss data breaches entirely. Two-thirds of all data breaches were not spotted by an internal team and were instead identified by a partner or supply chain. Without the right tools or an understanding of their complexity, it's easy for incidents to fly under the radar. While tools are important, there is a substantial human element to cyberattacks as well. Phishing and stolen or compromised credentials are two main attack vectors. 82% of data breaches involve human error of some kind.

Fortunately, the tide is turning, and many organizations are starting to take cyber resilience measures more seriously. Recent surveys show that 57% of organizations expect to modernize their data protection systems. For those who are still on the road to modernization, it's vital to understand the potential risks a ransomware attack can bring and what you can do to build resilience.

Evolving Threat Landscape

75% of organizations had at least one ransomware attack in 2023

75% of backup repositories were affected

200 days on average to identify and contain a data breach

Data Breaches Are Expensive

$4.45M is the global average total cost of a breach

Security Tool Complexity

66% of breaches were missed internally and identified by a partner or supply chain

Human Element

82% of data breaches involved human error

Top factors are **phishing** and **stolen/compromised credentials**

Data Availability, Protection, and Recovery

45% of production data is commonly affected

IT Modernization, Complexity, & Compliance

57% expect to modernize data protection

71% plan to recover to DRaaS or cloud-hosted infrastructure

Building Cyber Reslience

Businesses that build cyber resilience can reduce their risk of business disruption and damage from breaches. As previously mentioned, the cost of a data breach averages $4.45 million - reducing this risk is key to maximizing productivity, maintaining trust, and preventing a loss in revenue. The best way to achieve this is through continuous data protection and real-time detection.

To stay resilient, the goal is to engineer and practice resilience as an organization. It's important to maintain a balanced approach with defense and resilience by modeling the key traits of highly reliable and cyber-resilient organizations (CROs).

Businesses looking to focus on cyber resilience can do so by leveraging frameworks such as NIST CSF or other cyber resiliency frameworks. When it comes to tools and services, organizations should align modern data protection and recovery capabilities with "as a service" benefits for functionalities they lack internally.

Understanding a Ransomware Attack

When it comes to a ransomware attack, it is a matter of when, not if, you will experience a cyber breach. Generally, each attack has six distinct phases.

Initial Access

In the first phase, the attacker gains access to your system. This is commonly done through a phishing attack, where a threat actor sends a message, phone call, or other form of communication pretending to be someone the target is likely to know. Through a phishing attack, a cybercriminal might ask for access to certain credentials, either directly or through a fake application or website that will capture the information a target puts in.

Initial access can also happen by exploiting vulnerabilities in your software or hardware. Oftentimes, this includes zero-day vulnerabilities - weaknesses that have been disclosed by the vendor but not yet patched by the organization.

Supply chains are another area of weakness. While supply chain vendors may be the ones to identify a breach, they can also be a source of attacks. When a company in your supply chain is compromised, it can open the door for the attacker to gain access to your system as well.

Command and Control

Next, they take control of your compromised server. A command and control (C2) channel gives the attacker the ability to communicate with the malware they've installed on your system and send it commands to exfiltrate data, launch more attacks, or install more malicious software.

Lateral Movement

From there, the attackers will start to move from system to system. This can involve network scanning and environment mapping - lateral movement that allows them to continue to spread malicious code and gain access to more and more sensitive data.

Disable Security & Backup Agents

Before they are discovered, most cybercriminals will make it difficult for businesses to detect and respond to their attacks by disabling security and backup agents. They will locate these agents and disable as much as they can. To make it harder to recover from the breach, they will also delete any files and copies they find.

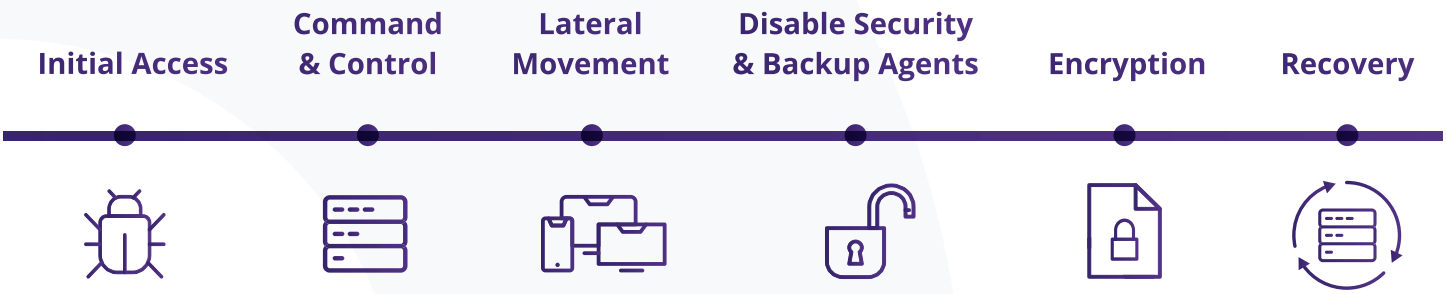
Encryption

Ultimately, an attacker's goal is to encrypt the data, locking down files and folders so they can force you to pay the ransom to get them back. Encryption is the most common form of ransomware. With this method, bad actors limit or completely prevent access by encrypting data, files, and information for one or more targets. If the user misses the deadline to pay in cryptocurrency, criminals threaten to delete all the data or expose it to the public.

Recovery

Once an organization has experienced a ransomware attack, the recovery plan needs to kick in as soon as possible. There are a few common scenarios. Businesses may choose to pay the ransom, but that's not always a guarantee that everything will be returned. They can try to rebuild systems from scratch, but that can take a lot of time and money that most organizations can't afford. However, companies that have backups in place can start to restore their systems from a previous backup point.

If you don't have a ransomware plan in place before a cybercriminal starts infiltrating your systems, it's likely already too late. Most attackers spend 5-9 days in your systems getting everything in place before they reveal themselves. Because of this, building cyber resilience is a must.



Industry-Leading Governance to Promote Cyber Resilience

The National Institute of Standards and Technology (NIST) developed Ransomware Risk Management: A Cybersecurity Framework Profile to combat ransomware. That profile includes five key functions: Identify, protect, detect, respond, and recover.

Identify

Start by developing an internal comprehensive plan that addresses the people, assets, data, and capabilities that need to be protected. Before anything else happens, your organization needs to have assessment and strategy discussions with all key stakeholders.

Protect

Implement safeguards to limit the impact of an attack and ensure the delivery of critical services to end users. Decide which services you can't live without and find ways to protect them. Businesses may employ the following measures to protect data and services:

- ✓ Employee training
- ✓ Data security tools
- ✓ Antivirus software with automatic scans
- ✓ Regular patching of operating systems with all security updates
- ✓ Secure, isolated backups that contain all critical data
- ✓ Immutable backups that can't be changed or deleted

Detect

Even with robust protection measures in place, attacks can happen. The faster activities are discovered, the more effectively they can be remedied. Businesses can leverage tools, including AI, to continually monitor for anomalies and events.

Respond

There should be no question about what your business will do next after discovering an attack. Develop a plan of action, including immediate containment, to respond to an attack. After containment, the plan should also include steps for communications, analysis, and mitigation. Who needs to be informed about an attack? What needs to be audited? How can the negative impacts of the attack cause the least amount of fallout possible?

Recover

The end goal of any incident is to return to normal operations as quickly as possible. Determine your strategy to restore capabilities and services that were impacted by the attack. To ensure everything will work as planned, test frequently and modify as you go, making improvements based on lessons learned.

Govern

A new function is coming to the NIST 2.0 framework which will emphasize the importance of cybersecurity governance and will serve as a foundational piece that encompasses all other functions. By forming a plan, businesses will accomplish much of what is expected in the Govern function.

Zero Trust

According to NIST, zero-trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero-trust architecture (ZTA) uses zero-trust principles to plan industrial and enterprise infrastructure and workflows.

- ✓ The Zero Trust model enhances cybersecurity defenses to detect and prevent cyberattacks. Complementing the previously discussed measures, key principles include:

  Enhance. Modern identity-based controls, incorporating robust measures such as Multi-factor Authentication (MFA) and session-based controls, establish a solid foundation for ensuring security in various digital environments.

- ✓ Continuous Monitoring of user and system activity to detect real-time patterns and anomalies.
- ✓ Least Privilege Access, combined with Just In Time (JIT) and Just Enough Access (JEA), confines users and systems to the precise access levels essential for their tasks, mitigating security risks.
- ✓ Application and content inspection can identify attacks and prevent the execution of malicious files.
- ✓ Network micro-segmentation compartmentalizes the network, preventing a widespread attack.
- ✓ Implementing data ingestion and classification facilitates the enforcement of policies that govern behaviors related to specific content types

Many other cyber resilience frameworks also build on the basics laid out by the NIST CSF functions, including the MITRE Cyber Resilience Engineering Framework (CREF), the Cybersecurity Assessment Framework (CAF), and the Center for Internet Security (CIS) best practices. While each framework has its benefits and drawbacks, what's most important for businesses is that they select a framework and create a plan instead of oscillating between frameworks and never creating a plan.

How TierPoint Can Help

Some organizations may be well-suited to tackle ransomware attacks head-on. However, no business should face this challenge alone. TierPoint offers a comprehensive suite of services encompassing hybrid and multi-cloud environments, following a vendor-agnostic approach to deliver a secure solution. Our goal is to empower organizations with the technology and services needed to enhance their Zero Trust posture. Here are some of the ways we help:

Preparation

- Modernize your infrastructure to enable **Zero Trust**
- **Cybersecurity assessment** Identify threats, risks, and weaknesses
- **Ransomware incident responses** Establish a team that can quickly respond to an attack
- **Business continuit**y Create a fully documented business continuity plan, including a comprehensive disaster recovery runbook that contains all testing and response procedures
- **Network isolation** Establish a plan for prompt containment of servers, data, and users after an attack is detected
- **Compliance** Meet compliance and governance requirements through our professional services engagement

Prevention

- Continuous security audit and policy improvement
- **Vulnerability management** Eliminate known vulnerabilities by staying current with the latest OS and installing updated patches
- **Employee training** Teach employees how to avoid phishing and other malware attacks across all endpoints
- **Firewalls** Restrict port access on the network using CleanIP, next-generation firewall (NGFW), and extended detection and response (XDR)
- **Multifactor authentication** Restrict unauthorized access attempts
- **Rehearsal drills and penetration testing** Set up frequent, non-disruptive isolated drills that can produce new insights without impacting production

Detection

- **Scanning** Malware scanning to detect infected files
- **XDR** Detect and respond to cyber threats
- **Email security and managed detection response** Perform user and entity behavior analysis (UEBA) on normal user and system behaviors to produce alerts based on anomalies

Response & Recovery

- **Restoration** Instant file and virtual machine (VM) restore, validation of clean restore points, rollback to different checkpoints
- **Disaster Recovery as a Service (DRaaS)** Service that scales as your business grows, offering continuous data replication, encryption detection tools, full site failover of all data and servers, and immutable data copies that are encryption-resistant. Achieve a recovery point objective (RPO) of seconds and a recovery time objective (RTO) of minutes. Recover data to the point before the attack within mere minutes of the attack without losing portability.
- **Backup and Recovery** Pull clean backups before infections. Threat actors will be unable to modify or delete backup copies with immutable and air-gapped configurations.

TierPoint can aid in transforming your hybrid and multi-cloud environments through assessments and the implementation of security operations, fostering the establishment of a robust zero-trust infrastructure.

Businesses that can for a comprehensive cyber resiliency plan can enjoy a competitive advantage, confidence in leadership, and stronger compliance with regulatory standards, all while ensuring unparalleled business availability.

About TierPoint

TierPoint (tierpoint.com) is a leading provider of secure, connected IT platform solutions that power the digital transformation of thousands of clients, from the public to private sectors, from small businesses to Fortune 500 enterprises. Taking an agnostic approach to helping clients achieve their most pressing business objectives, TierPoint is a champion for untangling the complexity of hybrid, multi-platform approaches to IT infrastructure, drawing on a comprehensive portfolio of services, from public to multitenant and private cloud, from colocation to disaster recovery, security, and more. TierPoint also has one of the largest and most geographically diversified U.S. footprints, with dozens of world-class, cloud-ready data centers in 20 markets, connected by a coast-to-coast network.

Learn More

Call **844.267.3687** or email **sales@tierpoint.com** to connect with one of our advisors. Or visit us at **tierpoint.com** to learn more.