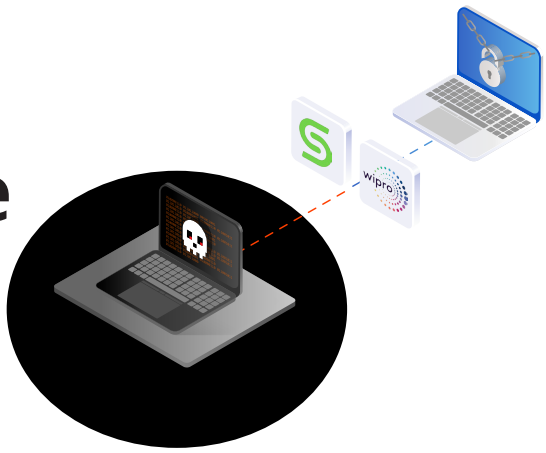
COHESITY | wipro

TIP SHEET

3 Must-Haves for an Intelligent Ransomware Recovery Strategy



Overview

Global ransomware damage costs, including lost revenue and productivity, are predicted to exceed $265 billion by 2031. As ransomware attacks continue to rise, thanks to bad actors taking advantage of unknown vulnerabilities and insufficient security actions, IT teams and businesses are under pressure to mitigate downtime, secure compromised data, and reduce exorbitant recovery fees. Because cyberattacks also decrease operational efficiency, lower employee morale, and negatively affect consumer confidence, developing a robust ransomware recovery strategy is now a top priority.

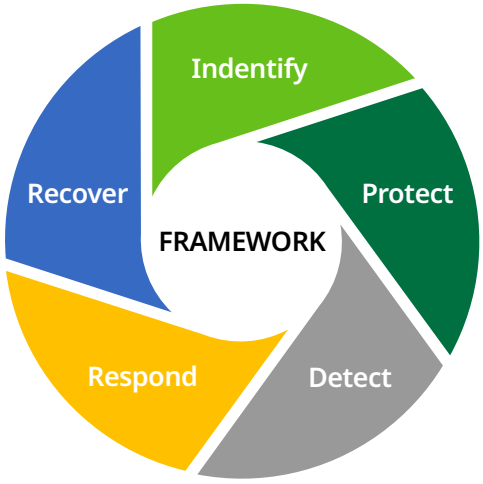
Your organization can build a comprehensive ransomware recovery strategy and become more resilient by recalling these points when you're evaluating your next enterprise cyber recovery investment:

Key Challenges

- Increasing ransomware threats
- Higher costs and complexities
- Lack of ransomware recovery strategy
- Unavailability of skilled resources
- Inability to meet business SLAs

1. Think and fortify beyond NIST cybersecurity recommendations

The NIST Cybersecurity Framework is the respected domain of security practitioners across the globe. The guideline's first step (Identify) centers on planning for threats. Step two (Protect) involves making sure your backup is well suited to allow your organization to recover from a ransomware attack. Step three (Detect) requires an ability to identify any ransomware threats that arise while the fourth and fifth steps (Respond and Recover) focus on overcoming threats and resuming operations, activities supported by data security and data management solutions with backup and recovery that enable organizations to quickly resume operations after a disaster, system failure, or cyberattack.



Historically, NIST guidelines were implemented in legacy environments through static recovery plan documentation and manual procedures. With today's ever-more strict SLAs, that approach is insufficient. Your organization can turn NIST's high-level recommendations into action using a truly automated solution with orchestration that prioritizes two outcomes:

- **Trusted recovery points** – You can't fully recover if you don't have a clean, uncompromised copy of your critical production data. Look for a well separated, air-gapped vault that keeps an immutable copy of your data so you can fully recover from a ransomware attack.
- **Agile, enterprise-class recoverability at scale** – To meet demanding SLAs, you need exceptional recovery performance at scale. Look for a solution with enterprise data protection assurance with performance.

2. Take advantage of end-to-end managed solutions and services

Nearly half of all organizations surveyed by ESG agree they have a problematic shortage of cybersecurity skills. As your team moves workloads to cloud-based environments, you need resources with cloud skills, too. You also have to have seasoned network security specialists, security analysts, and data security specialists. But due to shortage of skilled resources, many organizations remain understaffed and under-skilled in core cybersecurity domains. What's needed to address this skills shortage is to engage with a managed and professional service provider that can help with creating and performing key cybersecurity and enterprise cloud functions, including the following:

- Strategic cybersecurity planning with respect to internal policies and procedures
- Establishing an end-to-end framework for people, operations, roles, responsibilities, communication, and service execution
- Proactive preparation through assessments and mock drills
- Developing a unified dashboard with workflow automation, enabling coordinated action based on predefined procedures orchestrated for mock drills and recovery
- Preparation for cybersecurity assessments and regulatory compliance audits
- Assessing the large number of vendors that offer security solutions

3. Build for cloud and prioritize easy integration

Enterprises like yours are quickly embracing hybrid and multicloud strategies. Yet when your IT professionals go to back up and archive enterprise data in your public clouds of choice, they're finding your legacy backup solution falls short. That's because most installed backup products were introduced before public clouds, so they're not architected with cloud in mind.

In the multicloud era, your organization needs a modern, cloud-native solution that backs up and protects all of your data and applications in the cloud—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud—while taking advantage of cloud scalability and cloud economics. Look for a solution that not only natively supports simple data mobility across the hybrid cloud but also integrates seamlessly with your existing infrastructure. Find an integrated and extensible data security and data management solution that empowers your organization to detect, investigate, and respond to threats faster. The solution you choose should let you take advantage of the leading security tools you already use (for example, Cisco SecureX) and give your developers a rich set of RESTful APIs to continue adding value while countering threats.

Why Wipro Enterprise Recovery Vault – Powered by Cohesity?

Wipro Enterprise Recovery Vault – Powered by Cohesity, pairs innovative, modern Cohesity data security and data management with Wipro's strategic IT consulting services and enterprise resiliency frameworks. Aligned with NIST Cybersecurity Framework 1.1, the comprehensive joint solution holistically addresses all of the aspects involved in ransomware response and recovery. This includes the human effort, the IT recovery and resumption processes, and the intelligent automation required for orchestrating appropriate actions after a cyberattack—all tailored to your organization's unique needs and delivered as a service. The Enterprise Recovery Vault solution is also integrated with the Wipro ServiceTheatre autonomous framework for a seamless customer experience and accelerated time to market.

Download the solution brief to learn more about how Cohesity and Wipro can help you stay ahead of cybersecurity threats.

COHESITY

Cohesity.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

9100066-001-EN 1-2023