AUGUST 2024

Build Cyber Resilience Using the NIST CSF With Cohesity and HCLTech

Todd Thiemann, Senior Analyst

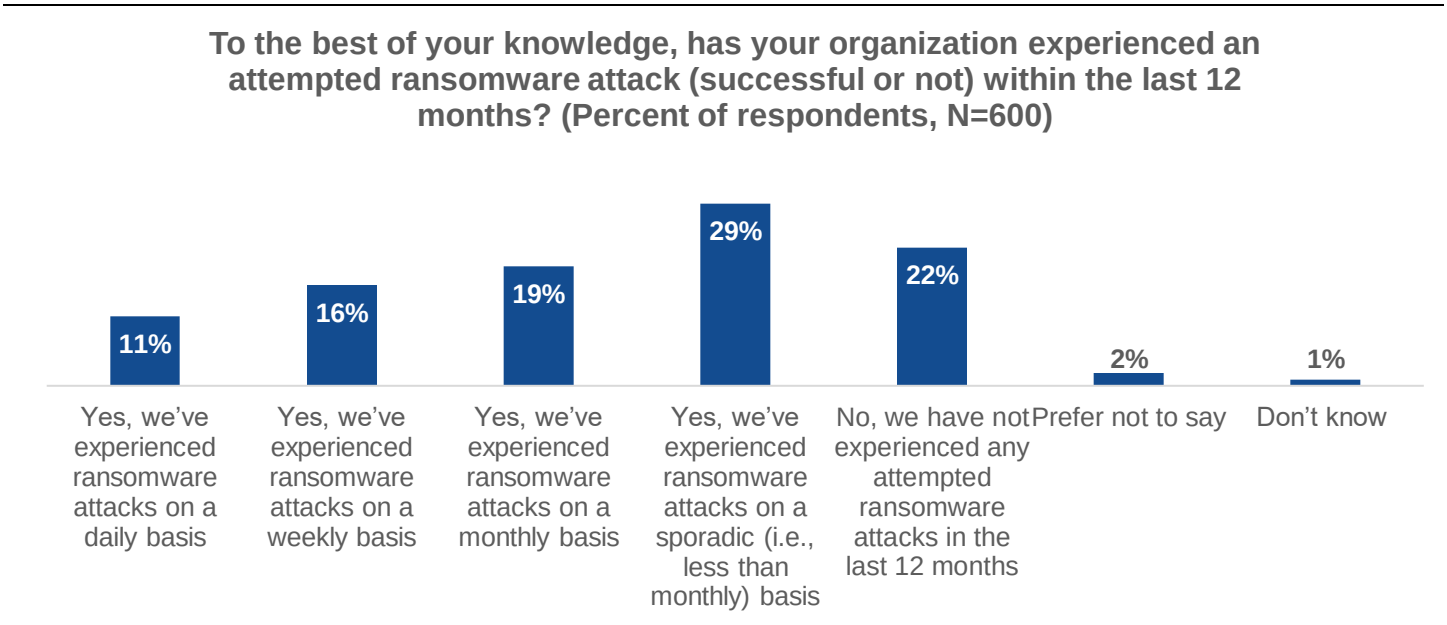
Abstract: Enterprises face a daunting threat landscape with increasingly sophisticated cyberattacks that can have catastrophic business consequences. Establishing and maintaining cyber resilience is guided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which provides a pragmatic path to mitigating cyber risk and improving an organization's security posture. The combination of Cohesity and HCLTech enables enterprises to prepare for, protect against, and recover from cyberattacks in alignment with the NIST CSF.

Introduction

Data is more critical to businesses than ever before. Nearly half (49%) of organizations surveyed plan on increasing their spending on data protection.[1] This increased spending underscores that bad actors continue to launch attacks on both primary and backup data sources, potentially costing organizations millions of dollars in lost revenue, reputational damage, fines, and legal damages.

Ransomware is a large component of the current threats organizations face. In fact, 75% of companies report that they have experienced an attempted ransomware attack in the past 12 months, with 11% experiencing them daily.[2]

Figure 1. Organizations Have to Prepare for Ransomware Attacks

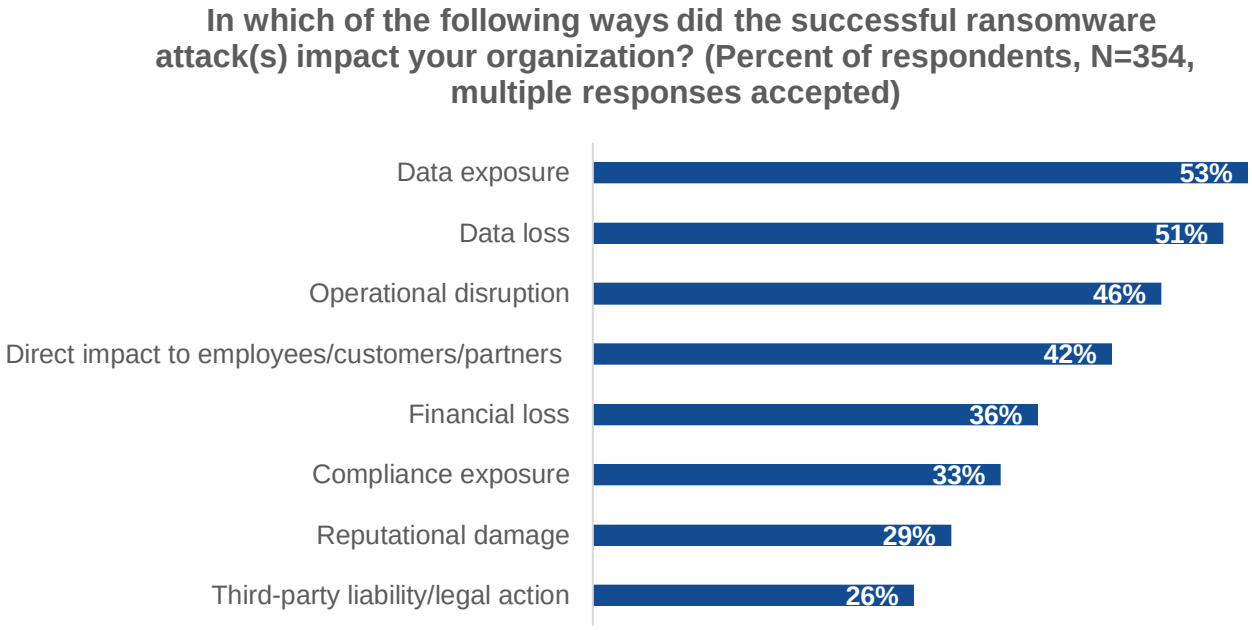


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Research Report, *2024 Technology Spending Intentions Survey*, February 2024.
[2] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.

Successful ransomware attacks cause ripple effects throughout an organization. Organizations cited many impacts, including data loss, operational and financial issues, and personal ramifications to employees, customers, and partners (see Figure 2).[3]

Figure 2. Impacts of a Successful Ransomware Attack



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations looking to protect their assets should move toward a cyber resilience strategy, focusing not only on protection but also on how to recover if a successful attack occurs. Cyber resilience programs enable organizations to get ahead of threats and help mitigate damages when an attack occurs.

The Focus Shifts to Cyber Resilience

Given the prevalence of ransomware and the increasing sophistication of cyberattacks, it's becoming more important than ever to have backup and recovery plans in the event of a successful attack. Organizations have begun thinking in terms of cyber resilience, making sure that mitigation and recovery are given equal attention to prevention and detection.

Research from TechTarget's Enterprise Strategy Group showed that backup and recovery strategies are becoming critical pieces of a cyber resilience program. Seventy-four percent of survey respondents reported being either very concerned or somewhat concerned that their data backups are becoming a ransomware target. Seventy-seven percent indicated that they do a detailed scan of backup data to find anomalies and anomalous user activity. Fifty-eight percent indicated that they have deployed an air-gapped solution to protect their data from ransomware.[4]

Enterprise Strategy Group research found that only 11% of survey respondents were able to restore 100% of their cloud data when they had to. Twenty percent could only recover 25-50% of their cloud data.[5] Losing such data permanently can be devastating to smaller companies and expensive to recover from for any organization.

[3] Ibid.
[4] Ibid.
[5] Source: Enterprise Strategy Group Research Report, *Cloud Data Protection Strategies at a Crossroads*, August 2023.

Organizations should look for solutions that align closely with the NIST CSF. Organizations can use the revised NIST CSF 2.0 and its pillars (Identification, Protection, Detection, Response, and Recovery) to create sound cyber resilience strategies. It provides an enterprise guide to better managing cyber risk; documenting critical security outcomes through which organizations can govern their cybersecurity programs; and planning for preventing, detecting, and recovering from cyberattacks. The CSF isn't prescriptive, however, so outside assistance is typically required to achieve the framework's outlined resilience goals.

Achieving Cyber Resilience With Cohesity and HCLTech

Cohesity and HCLTech have partnered to provide a solution that helps organizations increase cyber resilience, mapping to the NIST CSF to provide full coverage of the framework. HCLTech provides comprehensive cybersecurity services in concert with Cohesity, building a comprehensive suite of capabilities providing end-to-end cybersecurity solutions.

Identification

The initial step in the NIST CSF framework is identifying the assets to secure. HCLTech VaultNXT, supported by in-house cybersecurity and GRC teams, helps assess the likelihood of a breach and helps enterprises identify their crown jewels so they understand the key assets to be protected. Cohesity complements these services with data discovery and classification for sensitive information within the protected data. Cohesity Data Cloud applies a machine learning algorithm to classify sensitive data and applies threat intelligence in the form of curated and managed threat feeds to identify malware.

Protection

Protecting sensitive data enables organizations to avoid threats and recover quickly. HCLTech and Cohesity deliver comprehensive and robust data protection based on Zero Trust principles. By safeguarding data against cyber threats and unplanned business disruption with unlimited, immutable snapshots, combined with role-based access controls, encryption, and multifactor authentication (MFA), Cohesity Data Cloud can isolate backups in an immutable cloud vault to better protect against ransomware.

Cohesity's FortKnox delivers a SaaS-based cyber vaulting and recovery solution that provides a modern 3-2-1 strategy of having three copies of the data stored on two different types of media, with one copy kept offsite. This approach helps enterprises improve cyber-resilience with an immutable copy of the data in a Cohesity-managed vault available via a virtual air gap.

Detection and Response

Together with HCLTech's ongoing security monitoring, threat intelligence, and incident response retainer services, the Cohesity Security Center provides an integrated dashboard to monitor security alerts, threats, sensitive data exposure, data isolation status, and the security posture of the Cohesity Data Cloud. Cohesity uses AI to perform anomaly analysis on files and data to identify malware like ransomware and threats from malicious insiders. With threat-hunting capabilities and curated indicators of compromise (IOCs) threat feed, organizations can identify the early stages of an attack and mitigate it before there's an impact. Cohesity offers data classification that helps organizations determine if sensitive information has been exposed and guides incident response and regulatory actions that might be required. The solution also uses automated SOC integrations to leverage existing security controls and processes for incident response and remediation to help organizations determine whether attacks exposed sensitive data and help ensure the data is clean—then recover with confidence. By including user behavior monitoring, audit logging, and reporting, this combination also speeds the response to ransomware attacks and other security.

Recovery

Robust preparation leads to robust recovery when an attack occurs. Cohesity Data Cloud includes cleanroom features that enable practitioners to quickly create a minimum viable response capability to support the response and recovery process. It provides the intelligence that incident responders need using native AI/ML threat-hunting tools and third-party products in a safe, isolated environment. In addition, with services from HCLTech such as sandbox/cleanroom, recovery validation, and recovery response, combined with Cohesity instant mass restore (IMR) capabilities, enterprises can instantly recover hundreds of objects/VMs, NAS data, and databases to any backup point in time, leveraging "fully hydrated" snapshots that contain a complete and immediately usable version of the data at a specific point in time.

Conclusion

It is not a matter of "if" but "when" an organization will be hit with a cyberattack. Aligning with the NIST CSF can be an effective path for organizations to reduce cyber risk. Having skilled consultants facilitate cyber resilience and the data management process leads to a more positive outcome when a cyber incident eventually occurs.

The combination of the HCLTech VaultNXT offering and cybersecurity services with Cohesity Data Cloud maps to the NIST CSF and enables organizations to better manage risk and achieve desired security outcomes. With HCLTech's expertise and Cohesity's modern platform, the HCLTech VaultNXT cyber-recovery service fosters a foundation and approach for creating, building, and operating a cyber resilient architecture featuring robust data management and SaaS data isolation. The foundation is supported by trained and certified HCLTech experts who continually work toward achieving enterprise objectives and cyber resilience maturity with operational simplicity and efficiency.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com