Ransomware Preparedness Assessment Report

Brought to you by

COHESITY Enterprise Strategy Group by TechTarget

Introduction

Ransomware attacks are prevalent, but few organizations are prepared for them. Despite decades of investment in preventative strategies, attackers are still finding ways to evade security controls. Only one in seven organizations that have been the victims of a successful ransomware attack could fully restore their data. And while more than half of organizations cite data exposure and data loss as a result of ransomware attacks, successful attacks are further impairing operational processes and causing both supply chain and service availability issues.

That's why we designed this survey—to help you assess your preparedness and strengthen your resilience plan so you aren't caught waiting around for days or weeks to recover from an attack. The results below summarize your preparedness in the areas of readiness, prevention, response, recovery and business resilience when compared to others in the industry, based on research conducted by TechTarget's Enterprise Strategy Group.

TechTarget's Enterprise Strategy Group surveyed 600 IT and cybersecurity professionals responsible for the technology and processes associated with protecting against ransomware at midmarket (100 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (U.S. and Canada) and Western Europe (U.K., France, and Germany). Respondents were also evaluated against the 5 key strategic dimensions of readiness, prevention, response, recovery, and business continuity/resilience and placed in 4 groups denoting their maturity level in ransomware preparedness.

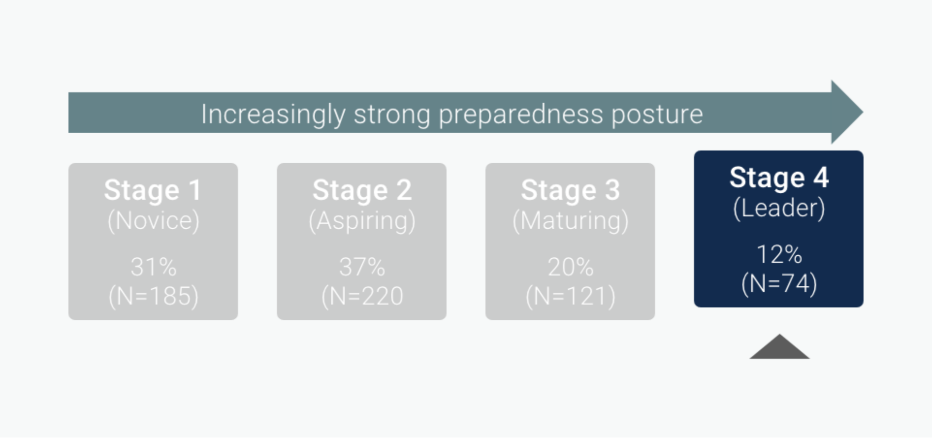
Based on your responses, the report below compares your performance to market Leaders.

Your Detailed Results

Summary

Thank you for taking the Enterprise Strategy Group/Cohesity cyber resilience self-assessment. Your answers were evaluated against 5 key dimensions, loosely coupled with the NIST framework, to establish your level of ransomware preparedness and provide you with a gauge of how you rate against market leaders based on Enterprise Strategy Group's market maturity research: readiness, prevention, response, recovery, and business continuity/resilience. Enterprise Strategy Group employed a points-based scoring system, with increasing point values awarded for behaviors and attributes consistent with a robust, multifaceted ransomware preparedness strategy.

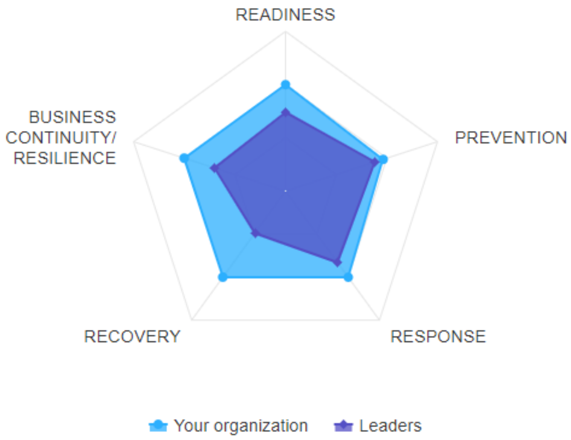
Figure 1. Ransomware Preparedness Market Maturity Stages: Overall Preparedness Results


Increasingly strong preparedness posture
Stage 1 (Novice) 31% (N=185)
Stage 2 (Aspiring) 37% (N=220)
Stage 3 (Maturing) 20% (N=121)
Stage 4 (Leader) 12% (N=74)

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

Congratulations—you are in the Leaders' group! Leaders are organizations that have scored the highest and typically receive the best score in each dimension. Compared to the overall market, you are among only 12% of peers who are Leaders. This is an achievement you should be proud of. Typically, Leaders get high readiness, prevention, and response scores and tend to do well in Business Continuity/Resilience. Among some notable characteristics, Leaders report having more mature vulnerability management programs currently in place than their peers in other stages: 85% report having a mature vulnerability management program in place versus 41% for the overall market.

Figure 2. Your cyber resilience ransomware preparedness results



Regarding adopting Zero Trust strategies (a key best practice), 70% of Leaders see it as foundational, versus 32% overall. Also, 84% of Leaders take extra measures to protect all of their backup copies, which is a key best practice, compared to 40% overall. This, in turn, may be why the time to fully recover from a ransomware event and resume operations in less than one day is a reality for 28% of Leaders versus only 12% of organizations overall. However, there is a significant word of caution for these Leading organizations in the area of recovery: On average, Leaders do not achieve a great score overall, barely hitting the 50% mark. This concern must be addressed to ensure business viability in the face of the constant onslaught of cyberattacks. Let's take a look at your detailed results by key dimension.

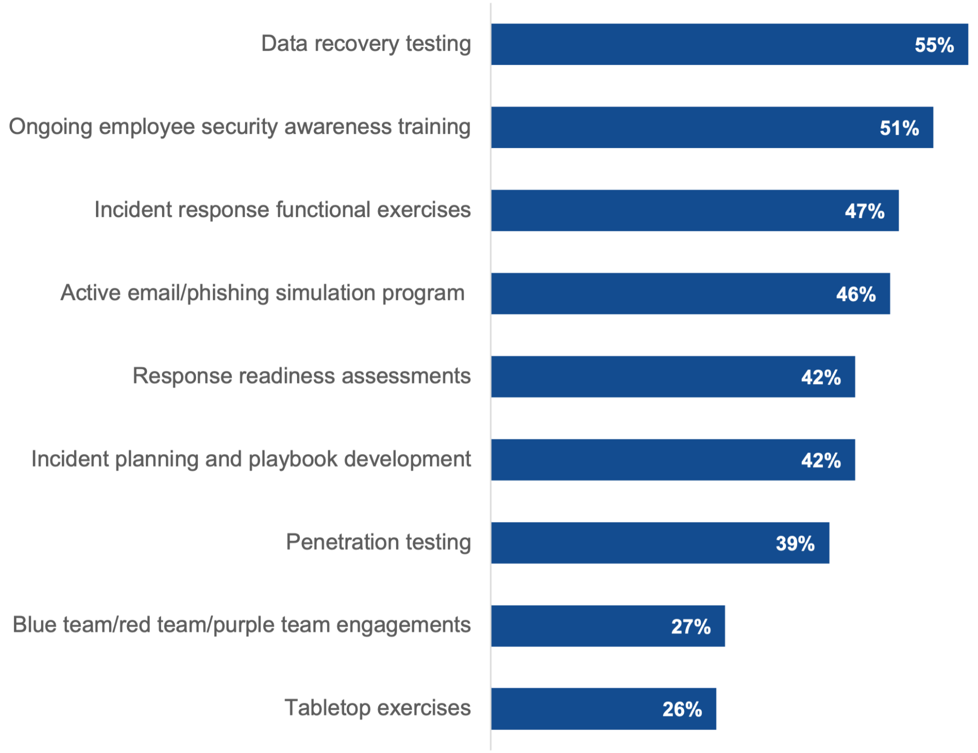
Readiness

Readiness includes the strategy, technologies, people, plans, playbooks, processes, and/or workflows associated with the continuing preparedness to protect and recover systems and business operations by detecting and executing remedial actions for a ransomware attack. These activities are foundational to an effective cyber resilience program and lay the groundwork for defensive strategies for ransomware. While ransomware shares similarities with other cyberattacks, the immediacy and variable nature of ransomware requires specialize readiness activities.

Ransomware readiness begins with a commitment and support from an organization's leadership team. Working together with the IT, security, risk and compliance, and legal teams, the readiness process is one of collaboration and ongoing planning and rehearsal. Readiness planning can begin with a team leader, identified team members, and an aspiration to strengthen ransomware preparedness. Most readiness planning and operations take place over many years, evolving and maturing as the team focuses on risk mitigation and incident response planning.

But planning alone is not enough. Operationalizing preparedness means ongoing investment in proactive testing of threat and IR capabilities. The team must rehearse the many aspects of the plan, ensuring each is actionable, repeatable, and all with the urgency required to mitigate and recover from a successful ransomware attack. Of note is the focus on data recovery testing, a critical dimension in which most organizations, even the best, are still struggling.

Figure 3. What ongoing ransomware preparedness activities does your organization engage in at least once per year? (Percent of respondents, N=600, multiple responses accepted)



Your score for ransomware Readiness was 57%.While your score is far below those that are most prepared, it aligns with the current state of the market based on Enterprise Strategy Group's research. It should be noted that, overall, the market's "grade" is almost at, and only slightly above, 37% (out of 100%). Ransomware readiness is a work in progress for most, with only 40% reporting that they have a well-defined incident response strategy that they have thoroughly tested. 52% say they have a well-defined plan but have not thoroughly tested it or are still making adjustments, highlighting the prevalence of incomplete, untested readiness programs.

While you fall into a category with many of your peers, your score should be a wake-up call that you are unlikely to recover from a ransomware attack without facing significant financial and operational damage to your organization.

There are a number of ways your score can improve, which should be a key priority for your organization:

- Expand your cyber resilience program to include representation from each key operating unit.
- Reassess your current ransomware readiness plan, leveraging third-party partners, such as IR service providers, consultants, integrators, and vendors like Cohesity, to enhance your cyber recovery capabilities.
- Set specific readiness and preparedness growth goals and share them with your senior team at regular readiness reviews.
- Identify key gaps in people, process, and technology, and prioritize investments to improve them.
- If you don't already leverage cyber insurance as a risk mitigation strategy, consider how cyber insurance could help both guide your readiness program and mitigate financial risk.

How Cohesity can help:

Organizations place a high priority on safeguarding their backup data, as hackers frequently target it. Cohesity employs a multilayered preventative approach to protect your backup data, including Cohesity DataProtect. This secure, high-performance backup and recovery solution is designed to defend against advanced cyberthreats by providing comprehensive policy-based protection for cloud-native, SaaS, and traditional data sources. Cohesity also follows Zero Trust principles to control access to its platform and settings with MFA, RBAC, and quorum approval, ensuring no unauthorized administrative changes.

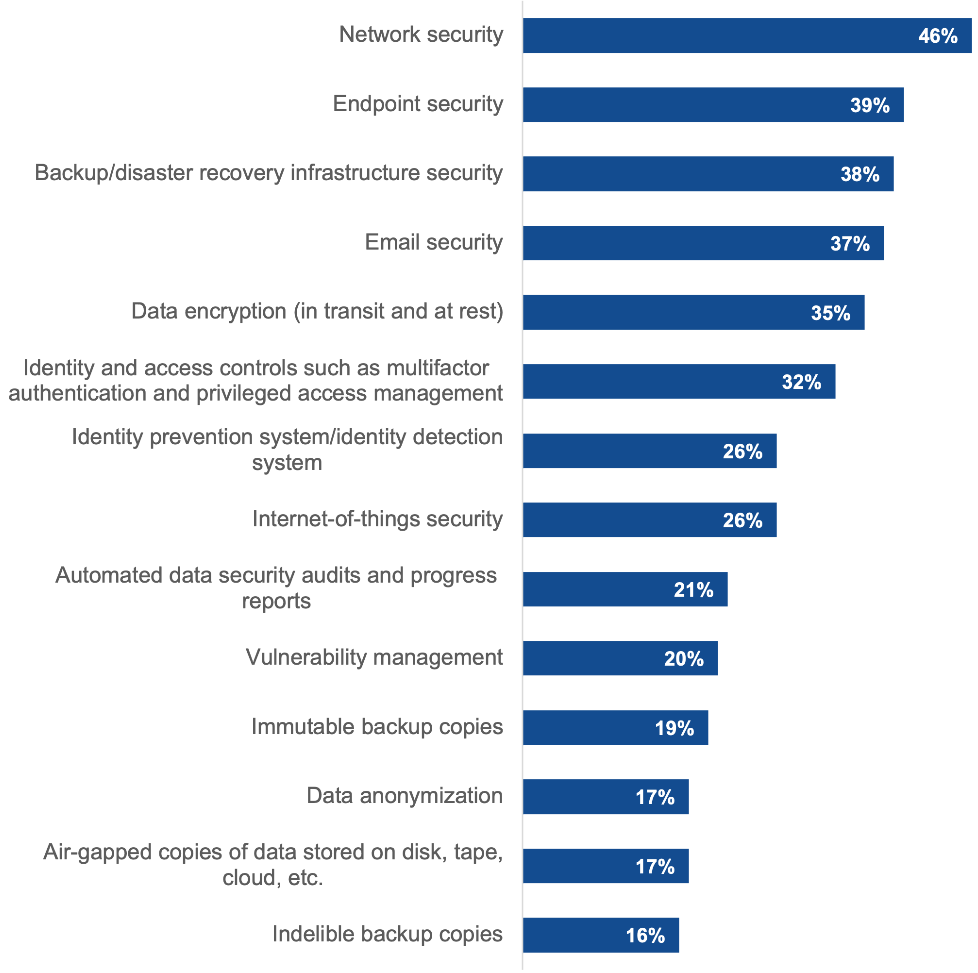
Prevention

Prevention includes the technologies, people, workflows, and processes in use to block ransomware at all stages of a potential attack. Preventative strategies have long been used to defend individual attack vectors, informed by both historical attack patterns and behavioral anomaly detection often powered by AI/ML. While prevention continues to be critical to modern cybersecurity strategies, most believe that prevention alone cannot defend against today's attacks. Paired with detection and response strategies, prevention plays a critical role in filtering out a large percentage of attacks, enabling security operations teams to focus on the small number of remaining threats that manage to evade these controls.

A variety of preventative security controls must be considered and are currently deployed by organizations in their fight against ransomware. The threat vectors considered most important to implement preventative controls for include the network, endpoints, email, and identities.

The most salient controls also happen to be the ones that show the most gaps (i.e., technology, skills, and processes) today. While network security is the most commonly recognized deficiency in preparedness (likely reflecting the nature of our interconnected economy), those gaps in the security of endpoints and "traditional" email systems can significantly expand attack opportunities for cybercriminals as well. Also of critical importance is the backup and disaster recovery infrastructure: without this infrastructure in a fully functional state, no recovery can be undertaken, which is a perfect scenario for attackers seeking to optimize their profits. Protecting the "protector" is an area where there is work ahead for many.

Figure 4. Which of the following preventative security controls are most critical to protecting your organization against ransomware? (Percent of respondents, N=600, five responses accepted)



Your cyber Prevention score was 75%.While your score is far below those that are most prepared, it aligns with the current state of the market based on Enterprise Strategy Group's research. It should be noted that, of the five dimensions assessed in Enterprise Strategy Group's research, organizations were, in many cases, over-rotated with prevention solution investments when compared to other key program functions.

While you fall in the middle of the pack, your prevention weaknesses leave doors open for crafty ransomware attacks to penetrate and successfully move laterally to find, encrypt, and put your data at risk. You also likely lack visibility or control of parts of your operating infrastructure, translating into the likeliness that ransomware attacks will progress further before you are able to detect and shut them down. Your score should be a wake-up call that you are at a high risk of experiencing one or more successful ransomware attacks in the coming months. There are a number of ways your score can improve, which should be a key priority for your organization:

- Engage a cybersecurity service provider to help assess and guide you through prioritizing and implementing the right set of security controls to protect your infrastructure.
- Consider the potential of a lower-cost approach, leveraging tools and infrastructure that can be provided by third-party solutions and service providers or by consolidating controls into a more integrated security platform.
- Know that the ultimate prize for ransomware attacks is your data and ensure that you have effective security controls for your critical and sensitive data assets.

How Cohesity can help:

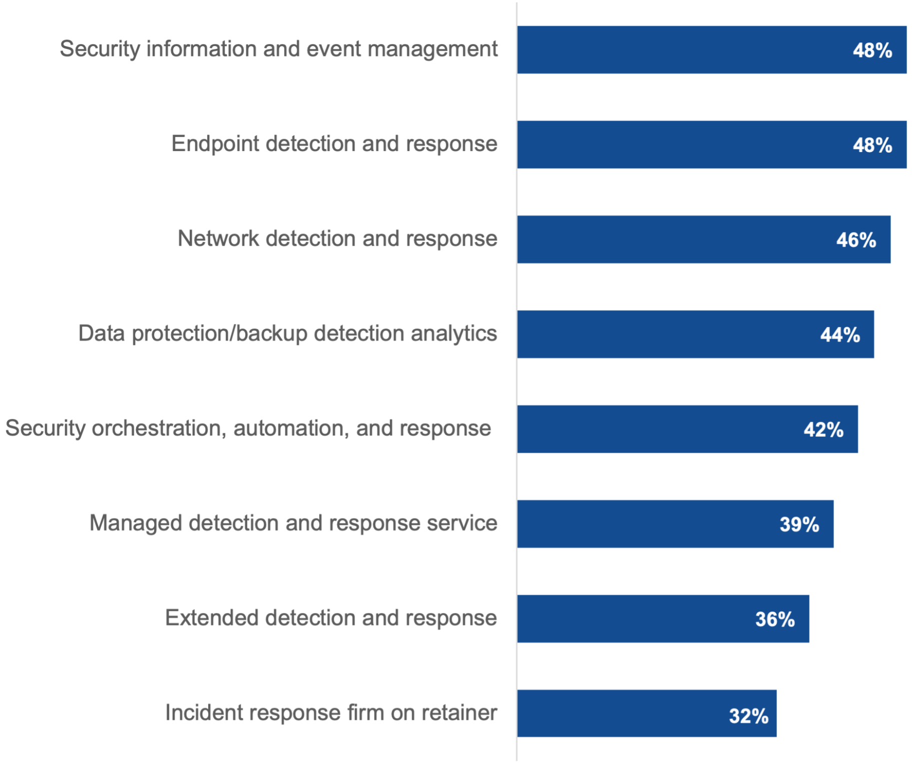
Cohesity can proactively identify sensitive data with AI/ML-powered data classification and scan backup data for vulnerabilities and threat exposure. Additionally, Cohesity can detect elusive threats using AI/ML-driven threat intelligence for the latest variants of ransomware and other cyberattacks.

Response

Response includes the technologies, people, and, processes used to detect and respond (D&R) to a ransomware attack (either still in progress or fully executed) that has successfully evaded preventative controls. Until recently, D&R tools have long been aligned with specific parts of the operating infrastructure, most notably network and endpoints. As the more sophisticated threats leverage attack strategies that move laterally across the many operating components, newer extended detection and response solutions are spanning much of the attack surface, including endpoint, network, identity, cloud, email, and more.

Once an initial ransomware foothold is obtained, most attackers carry out encryption activities in less than one week, so early detection and response is critical to mitigating risk. Therefore, investments in detection and response mechanisms and services are core to ransomware response activities. In terms of incident response in the event of a ransomware attack, the majority of organizations are augmenting their own internal capabilities with services from a third-party IR service provider. While less than one in five organizations currently hold at least one cyber insurance policy, the majority of organizations are either actively planning or researching how to incorporate cyber insurance into their overall risk mitigation strategy.

Figure 5. What mechanisms does your organization have in place to detect and respond to an active ransomware attack? (Percent of respondents, N=600, multiple responses accepted)



Your cyber resilience Response score was 56%. While your Response score is far below those that are most prepared, it aligns closely with the current state of the market based on Enteprise Strategy Group's research. It should be noted that, overall, the market's "grade" is almost at, and only slightly above, 52% (out of 100%).

While you fall in the middle of the pack, you lack aspects of detection and response strategies and operations that the most prepared organizations employ. Those most prepared typically employ one or more managed detection and response service providers to supplement coverage, skills, and capabilities. They also typically possess one or more cyber insurance policies to mitigate financial risk.

Your average score here should remind you that this function further exposes you to the likelihood of experiencing additional successful ransomware attacks in the coming months. There are a number of ways your score can improve, which should be a key priority for your organization:

- Engage a cybersecurity service provider to help assess and guide you through prioritizing and implementing effective detection and response mechanisms across all facets of your operating infrastructure.
- Consider more modern approaches to aggregating and correlating security signals across your attack surface.
- Look for opportunities to leverage GenAI as an accelerant to your detection and response program growth.

How Cohesity can help:

Cohesity can proactively identify sensitive data with AI/ML-powered data classification and scan backup data for vulnerabilities and threat exposure. Additionally, Cohesity can detect elusive threats using AI/ML-driven threat intelligence for the latest variants of ransomware and other cyberattacks. Cohesity has also partnered with leading security vendors across the industry to create the Data Security Alliance ecosystem. Integrations with Palo Alto, CrowdStrike, Tenable, Qualys, Mandiant, Okta, Cisco, Splunk, PWC, Securonix, CyberArk, BigID, NetSkope, ServiceNow, and Zscaler are essential to delivering an integrated security architecture.

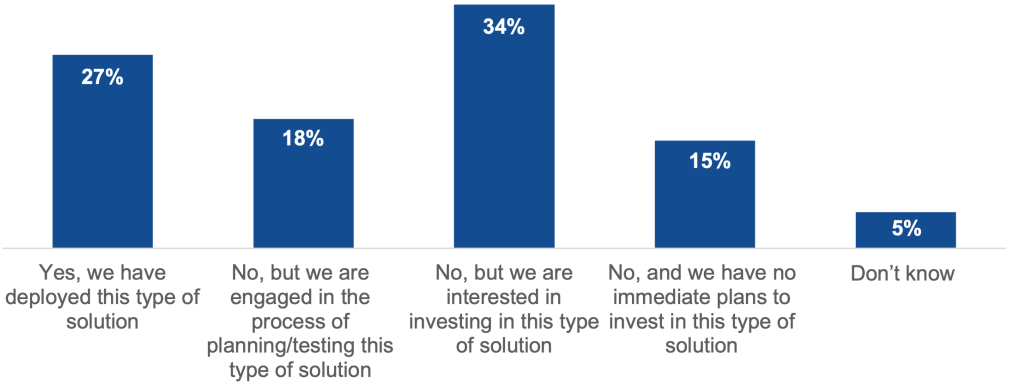
Recovery

Recovery is a critical component of any cyber resilience strategy. By allocating adequate resources and attention to recovery, businesses can minimize the impact of ransomware attacks and quickly return to normal operations. A comprehensive recovery approach that combines the right technologies, skilled personnel, established runbooks, and efficient processes can ensure the swift restoration of data and applications to a “clean” state.

Recovering from a cyberattack is not a matter of if but when. Ransomware can affect many different parts of the operation in different ways, which means that organizations must consider a number of recovery scenarios and strategies to optimize their recovery capabilities and service levels. According to Enterprise Strategy Group research, only 1 in 7 organizations can restore 100% of their data, demonstrating that recovery processes must be re-engineered for ransomware. While data and applications are disseminated across a hybrid infrastructure today, the good news is that many techniques and capabilities are available to recover data, metadata, and applications. It should be noted that most respondents in the research indicate that they naturally turn to the backup and recovery mechanisms already in place as their planned recovery method. Air-gapped backups are a crucial best practice to prevent cyberattackers from stealing or destroying backup data. Air-gapped backups should be stored in volumes inaccessible to applications, databases, users, or workloads currently running on the production environment. However, only 58% of organizations have deployed this solution. Though 11% are testing and deploying an air-gapped solution, more work is needed to ensure that the majority have it in place.

While having access to multiple mechanisms may contribute to complexity if not carefully planned, this can be an advantage. IT leaders must turn to vendors and implementation service providers for advice.

Figure 6. Can your organization isolate or air-gap some of its protection storage capacity to mitigate the effects of ransomware events? (Percent of respondents, N=341)



Your score for Recovery was 100%. This is better than the current average state of the market, based on Enterprise Strategy Group's research. It should be noted that, overall, the market's "grade" is almost at, and only slightly above, 29% (out of 100%). The market is facing a major issue: the deficient recoverability of ransomware events. This deficiency can lead to a range of significant negative impacts on businesses, from the loss of mission-critical data and applications to reputational damage, legal issues, and compliance repercussions.

While your score places you in a much more desirable spot than other organizations, there is plenty of work ahead in this critical dimension for you and your team. We encourage you to continue the following to keep your recovery score high:

- Continue to invest in aligning people, processes, and technology as you take a holistic view of ransomware recovery in your organization, including all your data, whether on premises or in the cloud.
- Practice makes perfect, and leveraging very frequent testing and dedicated recovery environments can go a long way in supporting stringent recovery requirements

How Cohesity can help:

Cohesity employs a multilayered approach to protect your backup data, including Cohesity DataProtect. This secure, high-performance backup and recovery solution is designed to defend against advanced cyberthreats by providing comprehensive policy-based protection for cloud-native, SaaS, and traditional data sources.

Leveraging Cohesity's Instant Mass Recovery solution further enables hundreds of files, objects, and VMs to be recovered at scale across the entire data landscape, enabling organizations to bounce back from severe attacks with minimal effort. Snapshots used are immutable, ensuring the integrity and rapid recovery of data and applications from any point in time snapshot.

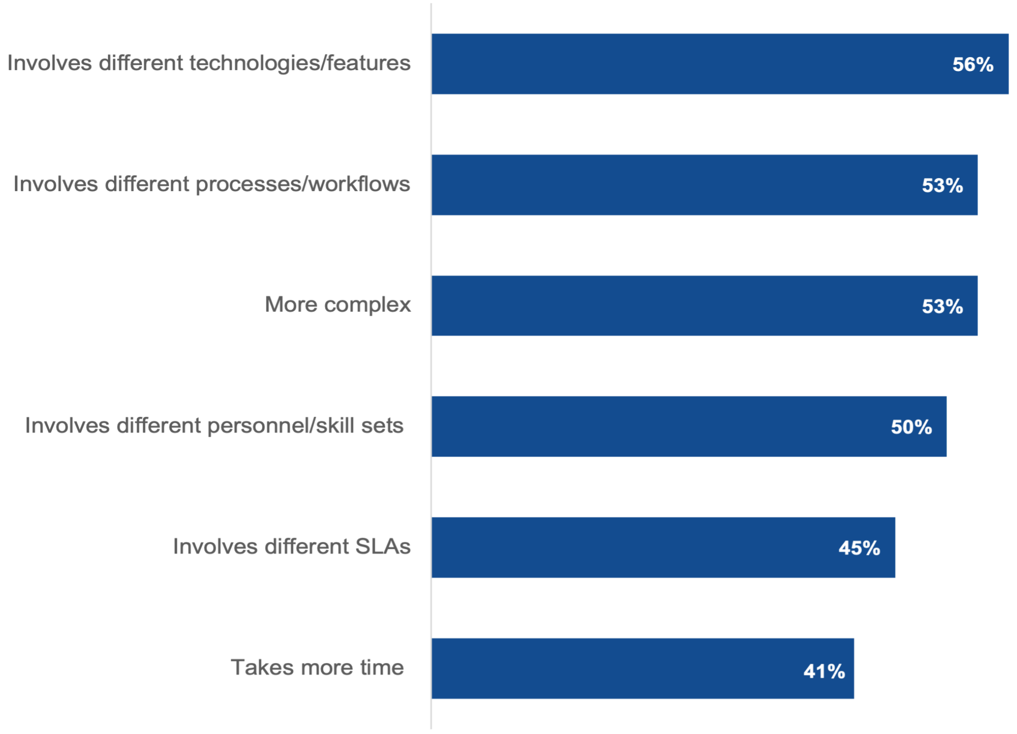
For added security, Cohesity offers a SaaS cyber vaulting and recovery solution called Cohesity FortKnox, which delivers an extra layer of protection against cybersecurity threats when on-site data is not available for recovery.

Business Continuity/Resilience

Business Continuity/Resilience is a critical aspect of any organization's operations: a ransomware attack can be devastating for an organization of any size, causing significant financial and reputational damage that can continue for long periods of time. That's why it's essential to have a robust business continuity plan to minimize such an event's impact. This plan should include measures to identify and contain the ransomware, restore data, and resume operations as quickly as possible. It involves a set of technologies, processes, and people responsible for ensuring that the organization can recover from or mitigate the impact of a ransomware attack. The focus is on resuming business-critical functions swiftly and seamlessly despite a disruption event, particularly ransomware.

Organizations struggle to recover their data to a production-like state, meaning that they can resume business operations and ensure their continuity. Most of these organizations will lose a valuable window of data, which can result in significant losses for large-scale operations. In today's competitive and regulated business environment, these unacceptable levels pose a significant business risk. Enterprise Strategy Group's ransomware preparedness research also shows that respondents have confirmed the changing nature of disaster recovery due to cyberattacks' impact. We are now in the era of cyber resilience, one in which technologies, workflows, and skillsets, among other factors, have to be revisited.

Figure 7. How is recovering from a cyber event different from recovering from a "traditional" outage or disaster? (Percent of respondents, N=415, multiple responses accepted)



Your score for Business Continuity/Resilience was 85%. It is above average for the current state of the market based on Enterprise Strategy Group's research. It should be noted that, overall, the market's "grade" is almost at, and only slightly above, 51% (out of 100%).

Your plans and programs are actively mitigating the potential of severe consequences ranging from data loss and reputation damage to compliance issues and legal action. Ransomware and cyber resilience are a marathon; constant efforts are needed even for the best-positioned organizations.

As an IT or security leader, you should consider a few key steps:

- Benchmark your plans, processes, and skillsets against peers in your industry. Your ability to deliver on business and cyber resilience efforts can be differentiating in a competitive market where most organizations are heavily invested in digital transformation and, therefore, potentially more exposed to cyber risk.
- Continue to fund and prioritize cyber resilience budgets.
- Consider increasing the frequency of organization-wide simulations, testing, and recovery exercises.
- It is a good idea to fine tune your internal processes as you evaluate how you will respond to cyberattacks. This could include creating isolated "clean room" environments which allow more efficient response and recovery.

How Cohesity can help:

Cohesity's clean room design provides a trusted foundation that speeds up incident recovery and augments investigations by SecOps teams while minimizing the risk of secondary attacks. Cohesity's modular design creates an isolated environment in minutes, supporting the response and recovery process and allowing teams to mitigate threats faster.

Conclusion

Ransomware has wide-ranging impacts beyond data-related issues, affecting business processes, compliance exposure, and financial and reputational loss. Most organizations are not adequately prepared. Due to the complexity of these threats, new processes and technologies to ensure cyber recoverability and resilience are needed.

Taking this cyber resilience self-assessment is a great step for your organization. The next step is to consider partnering with a vendor that has already bridged the gaps and built a cyber resilience platform. That's where Cohesity can help.

Cohesity's unique proposition is it's single platform for both data management and security. With a tightly integrated suite of security controls and data management capabilities, Cohesity empowers organizations to quickly identify potential risks, protect their data, and respond to attacks with seamless recovery at scale, all while ensuring visibility and control. Cohesity's advanced cyber recovery solutions seamlessly integrate with existing security controls, enabling organizations to detect and respond to incidents promptly. The platform leverages cutting-edge technologies to protect the world's most critical data and workloads, ensuring the highest levels of security and manageability across data centers, edge, and clouds.

Cyber resilience is a collaborative effort that requires an ecosystem of partners and integrations to ward off cyberattackers and improve ransomware preparedness. To this end, Cohesity has partnered with leading security vendors across the industry to create the Data Security Alliance ecosystem. Integrations with Palo Alto, CrowdStrike, Tenable, Qualys, Mandiant, Okta, Cisco, Splunk, PWC, Securonix, CyberArk, BigID, NetSkope, ServiceNow, and Zscaler are essential to delivering an integrated security architecture. Overall, Cohesity's advanced cybersecurity solutions offer an effective and efficient way for organizations to protect their critical data and workloads. This ensures regulatory compliance and maintains control over their data.

About Cohesity

Cohesity is a leader in AI-powered data security. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including 47 of the Fortune 100.

LEARN MORE

COHESITY

© 2024 TECHTARGET, INC. ESG, A DIVISION OF TECHTARGET, SUITE 1-150, 275 GROVE STREET, NEWTON, MA 02466 I 508.482.0188