ANALYST BRIEF

Sponsored by: Commvault and HCLTech

Ensuring recovery from cyberattacks is only getting more complicated. Data spread across hybrid, multicloud, and edge locations creates risks and makes recovery difficult. To maximize their digital transformation investments, organizations need proactive defense strategies to develop bulletproof recovery capabilities.

Cyber-Resilience Imperatives: Active Defense and Bulletproof Recovery

August 2023

Written by: Phil Goodwin, Research Vice President, Infrastructure Systems, Platforms, and Technologies Group

Introduction

Cyberattacks are a key concern of nearly every organization worldwide and have the attention of top organizational leaders. No company is immune to attack, regardless of geographic location, size, or industry. Cybercrime is highly profitable and therefore unlikely to go away anytime soon. IDC research shows that data security, risk, and compliance are the top priorities for organization investment, even in the face of macroeconomic headwinds (source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 1*, February 2023). Even factoring in inflation and higher interest rates, spending on cyber preparedness continues apace.

The consequences of a cyberattack can be severe, including:

- Loss of revenue, customers, and productivity
- Costs of ransom, downtime, and recovery
- Organizational embarrassment
- Shareholder lawsuits for negligence
- Class-action lawsuits from secondary victims

Cyberattackers have learned to attack the backup first because, if they can eliminate the ability to restore data, the odds of the victim paying a ransom increase.

Because of pervasive cyberattacks, organizations are focusing on becoming cyber-resilient (see IDC's definition of cyber-resilience in the Definitions section). Cyber-resilience goes beyond simply being able to recover after an attack, which is reactive in nature. It includes a proactive approach to cyberdefense to actively defend against attacks and limit or even

AT A GLANCE

KEY STATS

IDC research showed that 85% of survey respondents reported that they are well prepared for cyberattacks, but other IDC surveys have demonstrated that:

- Only 30% of organizations that have experienced successful attacks can fully recover without paying a ransom.
- 50% of respondents paid a ransom.
- 48% of respondents lost data as a result of the attack.

prevent damage or loss of critical data. Active defense involves considering cyberdefense at every layer of the data management stack and infrastructure, including authentication, data access, role-based access control, application, network, storage, and data protection systems.

It also means adopting technologies that can help organizations better manage data protection and recovery operations and leverage new tools to assess risk, classify sensitive data for security measures, and surface threats earlier, in both production and backup storage environments.

Cyber-resilience is not a "techie" function limited to ITOps or even SecOps groups. It is the effective coordination of people, processes, and technology. Cyber-resilience requires a companywide commitment of both technical and line-of-business teams to actively defend against attacks and respond quickly and effectively to an intrusion. End users are critical links in the defense chain since most intrusions are enabled either through phishing scams, malicious attachments, or stolen credentials from an unsuspecting or careless user. Active defense starts with executive sponsorship and requires the coordinated efforts of the CEO, CFO, CIO, CTO, CISO, and corporate counsel.

To embark on a cyber-resilience journey, IDC recommends the following steps:

1. Establish a cross-functional team whose task is to enhance defense and ensure recovery.
2. Conduct cyber-risk and gap analysis across the organization.
3. Identify and classify critical data.
4. Conduct dependency mapping of not only systems and applications but people and processes that are critical to business operations.
5. Develop a road map to implement changes.
6. Design zero trust principles for both technology and processes.
7. Engage technology partners and staff resources for implementation.
8. Evaluate technologies that can unify data security, protection, and recovery operations to accelerate incident response, automate countermeasures, and connect IT and security teams across complex data environments.
9. Conduct ongoing testing, review, and improvement of systems and operations.

Many IT organizations are learning that "they don't know what they don't know" until they experience a successful cyberattack — struggling to recover lost data and facing excessive recovery times. As a result, many companies with lessons learned are engaging the services of vendors and organizations that can supply critical expertise and experience beyond in-house capabilities in combination with the tools and systems to fill functionality gaps.

Definitions

- **Cyber-recovery** correlates with the fifth pillar of the National Institute of Standards and Technology (NIST) cybersecurity framework ("recover") and is the process of recovering from a cyberattack specifically as a subset of other recoveries.

» **Cyber-resilience** is an organization's ability to defend, deflect, or recover from a cyberattack and minimize the impact of a successful attack.

Benefits

Cyberthreats are so pervasive that it is not a matter of if or when an organization suffers an attack but rather how often and severely it experiences attacks. IDC research has also found that 60% of organizations that were successfully attacked become reinfected by the same malware after recovery.

Organizations that make a concerted, ongoing effort to prepare and defend against a cyberattack will have a better chance of minimizing damages. They are also more likely to deflect and thwart attacks and avoid consequences in the first place. IDC recommends using the NIST cyber-recovery framework, which specifies identify, protect, detect, respond, and recover as its primary pillars and describes the elements of proactive defense, rapid detection, and recovery.

Unfortunately, for many organizations, there is a gap between how well they think they are prepared and how well they are actually prepared. IDC research showed that 85% of survey respondents reported that they are well prepared for cyberattacks, but other IDC surveys have demonstrated that:

» Only 30% of organizations that have experienced successful attacks can fully recover without paying a ransom.

» 50% of respondents paid a ransom.

» 48% of respondents lost data as a result of the attack.

We believe this gap between perceived preparedness and actual outcome is a result of the insular perspective that derives from limited in-house knowledge. Third-party service providers and consultants have a breadth of knowledge and experience that they have gained across numerous clients and scenarios, and which is simply not possible with only in-house efforts.

Many consultants and service providers also have established frameworks, methodologies, and templates for common processes, as well as deep experience integrating technologies that are best fit to accomplish cyber-resiliency and business objectives. Although DIY cyber preparedness may seem more cost-effective, consultants and service providers can significantly reduce the required time to implement a solution, thus shortening the period during which organizations are at risk and, in many cases, reducing the total cost of ownership (TCO).

Considerations

Cyber protection is a game of cat and mouse: When IT learns to defend from one type of attack, the criminals devise a new one. No amount of preparedness can guarantee that an attack will not be successful, but maximum preparation and active defense are the best ways to minimize attack possibilities and opportunities for intrusion.

Too often, cyber-defense teams and cyber-recover teams operate as silos with little coordination between them. Backup/recovery vendors may also operate with little integration or consideration of proactive cyberdefense. IT organizations need integrated solutions that consider how to avert and react quickly to attacks. Qualified consulting organizations can help bridge this gap by facilitating communications and offering improved training and processes.

Consultants can also help reduce the silos of protection to create unified operations across on-premises, cloud, hybrid cloud, and multicloud environments. These steps reduce risk and improve recovery outcomes.

IDC recommends the following best practices for improving cyber-resilience:

- Follow a 3-2-1-1 backup strategy (three copies of the data, two different media types, one copy offsite, and one copy offsite and offline).
- Maintain immutable copies that cannot be altered or deleted.
- Encrypt data at rest and in flight (including backup copies).
- Maintain an air-gapped copy, ideally immutable and in coordination with 3-2-1-1 backup, to prevent physical access by attackers.
- Implement zero trust practices throughout the infrastructure and organization.
- Unify cyber-resiliency operations, including data protection, recovery, and operations to close security gaps and improve resilience.

Cyber-resilience efforts should not overlook cloud-native (SaaS) applications. Some organizations mistakenly believe that apps in the cloud are automatically protected and safe. Unfortunately, many cloud-native apps are backed up using minimal backup frequency and retention periods and few of the best practices in the previously mentioned list. IT leaders should secure data from these applications using the same principles as for on-premises apps.

Modern organizations commonly use a mix of on-premises and cloud resources. Larger organizations may also span geographies. Having a plan for how and where to recover specific applications based on regulations (e.g., GDPR) and data sovereignty must be worked out long before a recovery is required.

Trends

Enterprises continue to seek ways to improve cyber-resilience, yet macroeconomic pressures demand better TCO from solutions. A shortage of cybersecurity and protection skills also challenges organizations, requiring them to implement more automation and simplicity to allow existing staff to address issues now and in the future.

To meet these ongoing challenges, IT teams are looking for new, innovative solutions, such as:

- Data protection and cyber-recovery as services that allow IT teams to offload labor-intensive activities to service providers with the explicit skills to address them
- New cyber-resilience platforms that unify data security, protection, and recovery activities and offer scalability and workload protection across on-premises, cloud, and edge deployments
- Advanced technologies that can lure bad actors to attack and surface zero-day, unknown, and internal threats in production and backup environments with precision
- Robust protection for both production and data protection workloads

- Greater visibility and identification of risks, SLAs, and KPIs to help ensure compliance with cyber-resiliency objectives
- Capabilities to automate routine data protection and recovery activities with refined control to respond to changing recovery demands while managing costs
- Engagement with industry experts capable of reducing risk, accelerating solution implementations, and minimizing impacts during an attack

Conclusion

Too often, cyber-recovery efforts take a limited, reactive approach. IT organizations that believe they are fully prepared for cyberattacks may learn the hard way that their limited scope of knowledge was not sufficient to meet the rapidly evolving nature of these attacks. The consequences of this miscalculation can be severe for the organization.

To become a cyber-resilient organization, businesses need the foundational tools to meet the technological challenge.

To become a cyber-resilient organization, businesses need the foundational tools to meet the technological challenge as well as the expertise to implement them with best practices and zero trust standards. A unified platform for securing, protecting, and recovering data with leading security tools to accelerate incident response, automate countermeasures, and connect IT and security teams helps ensure that organizations address all aspects of the cyber-resilience framework, including identify, protect, detect, respond, and recover. Proactive efforts and modest investments can pay huge dividends in business outcomes.

About the Analyst

Phil Goodwin, *Research Vice President, Infrastructure Systems, Platforms, and Technologies Group*

Phil Goodwin is a Research Vice President within IDC's Infrastructure Systems, Platforms, and Technologies Group, with responsibility for IDC's infrastructure software research area. Mr. Goodwin provides detailed insight and analysis on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption. His focus is on multicloud data management, data logistics, on-premises and cloud-based data protection as a service, cyber protection and recovery, recovery orchestration, and more.

MESSAGE FROM THE SPONSOR

HCLTech and Commvault work to strengthen organizations' cybersecurity and resilience strategies and safeguard mission-critical data in today's hybrid and multi-cloud data environments. Together we're redefining cyber resilience with a comprehensive platform purpose-built to secure, defend, and recover data wherever it lives with true cloud simplicity, intelligence, and scale. Overall, we offer tremendous growth potential for enterprises across the globe and help modernize comprehensive security strategies.

HCLTech and Commvault: Cyber Resilience for Hybrid and Multi-cloud Environments | HCLTech

GSI Partners | Commvault

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com