IDC

SPOTLIGHT

Sponsored by: Lumen

Cyber resilience is not just backup, or threat detection, or data recovery. It is a holistic approach to the technology stack that balances each factor to both reduce risk and bolster cyber defense and recovery.

Getting to cyber-resilience through managed services

December 2025

Written by: Phil Goodwin, Research Vice President, Infrastructure Software Platforms, Worldwide Infrastructure Research

Introduction

Cybercriminals have numerous avenues to attack organizations. They may enter systems using compromised credentials or by finding unpatched and vulnerable systems, improperly secured edge devices, or other weaknesses. While attacks are often thought of as serial events, in fact, multiple attackers may be probing from every angle simultaneously.

Once inside, these criminals use a variety of attack strategies. By making the attack multipronged, attackers increase their chances of success. Most will spend time learning about the systems and finding additional vulnerabilities. They will search for the most valuable data to use as their primary target.

When the actual attack is triggered, cyber criminals may choose to attack Active Directory or Entra ID to prevent user access and cause maximum disruption to business operations. At the same time, these criminals may seek to steal (exfiltrate) or corrupt data in primary storage. According to IDC data, almost half of attacks seek to compromise the backup systems, even before attacking primary storage. The goal is to make data recovery impossible without paying the ransom. It is increasingly common that cyberattackers deploy multiple strategies, such as both data exfiltration and corruption, to demand larger ransoms and further complicate recovery efforts.

IDC research has found that only 31% of organizations were able to fully recover from a cyberattack without losing data, paying the ransom, or — worse — both. Our research further finds that organizations struggle to find and retain the human talent necessary to adequately respond to crisis situations. Many are starting to involve third-party organizations to help fulfill the necessary response requirements. The adage "You don't know what you don't know" certainly applies to IT teams regarding cyber-resilience and explains why these teams are engaging third parties that have specific cyber-resilience expertise.

Too often, recovery from a cyberattack can take a week or more to simply restart critical operations; full recovery takes even longer. Several reasons exist for these slower-than-expected recoveries, including threat identification and isolation,

AT A GLANCE

WHAT'S IMPORTANT

Modern cyber-attacks can target the network, primary storage and backup systems. Organizations must address all three holistically to ensure the best possible response.

KEY TAKEAWAYS

Limited network bandwidth can stymie the recovery of large volumes of data. Organizations need to restore data quickly to avoid costly business downtime.

recovery point determination, and a lack of sufficient network bandwidth to efficiently move large volumes of data from recovery sites to production systems.

Some organizations may have one group that focuses on network intrusion and detection, another on data protection and recovery, and yet another on primary storage anomaly detection. This can lead to organizational silos, resulting in exploitable gaps. As stated above, attacks come from all directions simultaneously. Organizations must take a holistic approach to cybersecurity prevention, detection, and recovery to become fully cyber-resilient. While organizations can do this in-house, many IT leaders are turning to managed service providers (MSPs) to ensure comprehensive cyber-resilience.

Definition

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

Options and Benefits

All infrastructure vendors have their own perspective. Backup vendors consider the backup environment, network vendors consider networks, storage vendors consider storage, and so on. Each may offer important cyber-resilience capabilities in the context of their own systems, but without sufficient integration with adjacent technologies. Because vendors may lack visibility into other systems, there may not be sufficient coordination between them, which could lead to gaps exploitable by cybercriminals.

A comprehensive cyber-resilience solution begins with the six pillars of the NIST cybersecurity framework. These pillars are: identify, detect, protect, respond, recover, and govern. Infrastructure vendors usually address a limited part of the framework, such as respond and recover (i.e., backup vendors), identify and detect (i.e., SEIM), or standalone governance tools.

In contrast, a solution provider, such as a managed service provider, can bring in all parts of the framework and integrate them into a comprehensive solution. MSPs often bring together a mix of their own intellectual property and IP from third-party vendors. MSPs can integrate systems or provide human capital and eliminate or mitigate gaps between technology stacks.

Essential elements that contribute to cyber-resilience and rapid recovery include:

- Rapid detection and isolation: Attacks that are detected and isolated quickly often incur minimal damage. When attackers have days, weeks, or months to execute their attack, the damage can be significant, making full recovery extremely difficult.
- Full-stack coverage: While many vendors may include detection, prevention, and recovery in their products, without communication between security, storage, the network, and data protection, silos may develop, which may hamper detection and recovery.
- Clean recovery without restoring the ransomware: IDC's research shows that ransomware reinfects 60% of organizations after the initial recovery. Cleanroom isolation and forensic analysis are essential to performing system recoveries without reinfection.

- Recovery point determination: Ransomware attacks are asymmetrical, meaning some systems are compromised while others are not. Being able to determine what was attacked, when it was attacked, and how it was attacked allows precise recovery point determination for faster recovery and less data loss.
- Rapid data access – Once the proper and clean recovery point and inspection has been identified, organizations need to move and restore that data as fast as possible to minimize downtime. In cases where significant volumes of data require restoration, insufficient network bandwidth hampers moving the data in a timely manner. Slow network speeds can lead to recovery delays of days or weeks.

Considering Lumen

Lumen is a global communications services company that offers solutions for infrastructure, networking, edge cloud, cybersecurity, and numerous other capabilities. The company is a managed service provider that can integrate not only its own intellectual property and solutions but also solutions from other leading providers to offer a full stack of hardware, software, and services. By managing the whole stack, Lumen has visibility into every element, ensuring end-to-end coverage and plugging gaps between technologies. As a managed service, Lumen is fully staffed with cyber-resilience experts and able to respond to customer crisis events.

Lumen's vast communications network of high-speed and high-bandwidth channels allows the company to burst capacity as needed. For customers needing to move large volumes of data quickly, whether for cyber-recovery, disaster recovery, or other reasons, the company can very quickly apply those resources where needed.

Lumen's core cyber-resilience strength is its network security and protection:

- Lumen's Network-as-a-Service (NaaS) can quickly scale network connectivity from any source to any destination, whether a datacenter or a hyperscaler. This on-demand network bandwidth is key to rapid data transfer and recovery.
- Lumen Black Lotus Labs keeps the company at the forefront of threat detection and defense.
- Black Lotus leverages Lumen's global network visibility for threat monitoring and detection in a way that few other organizations can.

Lumen partners with key storage and data protection vendors to supply the storage and data protection technology components for a cyber-resilient infrastructure. Lumen provides the systems qualification, compatibility, and integration for the entire technology stack, as well as the management services to support it. These include:

- NetApp: NetApp is a leading storage supplier for integrated file, block, and object storage arrays. NetApp features integrated cyberdetection for primary storage. It is also based on a zero trust architecture to reduce the risk of attackers accessing different systems. NetApp storage can be both encrypted and immutable.
- Commvault: Commvault is a leading data protection vendor that offers data recovery solutions for almost any contingency, from a single file up to disaster recovery and cyber-recovery. Commvault has extensive cyber-recovery capabilities, including threat detection, cleanroom recovery, and recovery orchestration. Commvault backups can be encrypted, immutable, and air gapped.

Challenges

Cyber-recoveries can be extremely challenging. While certain attacks have commonalities, attackers are constantly making subtle changes in an attempt to find new methods of attack, points of attack, or ways to thwart recovery. Systems are predominantly trained to detect known threats, which may allow never-before-seen attack methods to be successful.

While prior field experience is a significant benefit in cyberpreparedness and response, no vendor can ensure 100% attack detection or recovery. Moreover, recoveries may be highly complicated, and any single step in the process may delay or compromise the recovery. No organization or team, no matter how experienced, can plan for every possible contingency.

Even though MSPs either provide or integrate the whole technology stack and manage it on an ongoing basis, their product and partner choices may differ from the customer's current solutions. These differences may lead to some degree of conversion or migration. It is also important that customers align their business operations with the technology choices and processes the MSP establishes to avoid any internal gaps between them.

Conclusion

Cyber-resilience is not a technology or single program; it's an organization wide effort involving people, processes, and technology. With the ubiquity of cyberattacks, organizational leaders have too often learned the high cost of inadequate preparation.

Cyber-resilience is not a technology or single program; it's an organization wide effort involving people, processes, and technology.

Managed service providers can bring broad experience, technical expertise, and competent personnel to deliver immediate improvements to many organizations' cyber preparedness. This expertise will aid intrusion prevention and rapid response in the event of a breach. To minimize the impact of attacks, organizations need rapid detection and recovery. Where large data transfer volumes have the potential to stymie or extend recoveries, rapidly scalable, on-demand, and high-bandwidth networks can reduce recoveries by days or weeks, leading to significantly less downtime and a faster return to normal business operations.

About the Analyst

Phil Goodwin, *Research Vice President, Infrastructure Software Platforms, Worldwide Infrastructure Research*

Phil Goodwin is Research Vice President within IDC's worldwide infrastructure research organization and global research lead for the infrastructure software platforms practice. He leads a team of analysts that provide detailed insights and analyses on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption. Mr. Goodwin's own research focuses on multi-cloud data management, data logistics, on-premises and cloud-based data protection as-a-service, cyber protection

	and recovery, and recovery orchestration. He takes a holistic view of these markets, and covers risk analysis, service level requirements and cost/benefit calculations in his research. Mr. Goodwin also contributes regularly to IDC's CIO advisory practice.

MESSAGE FROM THE SPONSOR

At Lumen, cyber resilience is treated as essential. Modern cyber threats move quickly, and protecting mission-critical assets requires preparation for both prevention and recovery. Organizations need a holistic approach to safeguard data, maintain continuity, and stay ready for what comes next. Lumen solutions for Cyber Resiliency bring together layered data protection, rapid restoration, and the flexibility to adapt as threats evolve. The goal is to help organizations remain resilient, confident, and in control as the landscape continues to shift.

Learn more about how Lumen is enabling organizations to combat the new era of cyber-threats at Edge Computing | Storage Solutions | Lumen

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
blogs.idc.com
www.idc.com