ESG RESEARCH SUMMARY

Cyber-resiliency Maturity in Data Storage

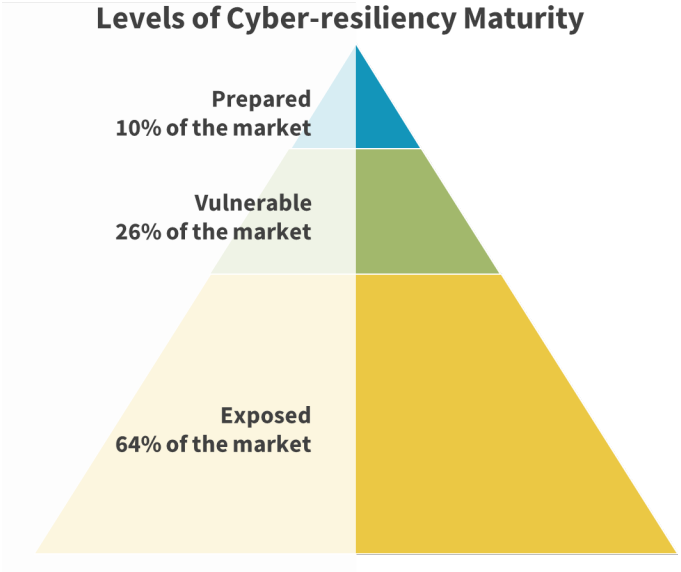
Date: March 2022 **Author:** Scott Sinclair, Practice Director

ABSTRACT: As the scale and volume of cyberattacks continues to rise, application environments become more dispersed, which increases businesses' risk of exposure to these attacks. As a result, cyber resiliency must be an essential requirement for any business. Given the ever-increasing threat to data and IT servers, businesses must invest in cyber-resiliency strategies to reduce operational risk. New research from ESG, however, finds that cyber-resiliency investments are even more valuable than previously thought: In addition to minimizing risk, they improve a business's ability to innovate.

Research Overview

Improved cyber-resilency capabilties help to reduce risk. But does an organization's level of cyber-resiliency maturity also help foster innovation and deliver greater business success?

To answer this question, ESG surveyed 750 IT decision makers and then segmented the respondents into cyber-resiliency stages (see graphic on right). This classification was driven by how respondents answered four questions about their organization. Each of these questions represents a characteristic of a Prepared organization (i.e., an attribute of a highly resilient organization) in terms of the teams in place to protect it, the funding for technologies to mitigate risk, or the organization's focus on minimizing third-party risk.



- How would you describe the level of staffing in your cybersecurity team?
- How would you describe the level of skills in your organization's cybersecurity team?
- How would you characterize your organization's investment in products and services to secure its systems, applications, and data?
- Does your organization audit or inspect the security of its partners/IT vendors?

Only organizations reporting that they have no open positions they are looking to fill on their security team, that their security team has no problematic skills gaps, that their organization funds security technologies at an optimal level, *and* that their organization formally and rigorously audits third-party risk were considered Prepared. Those with 2 or 3 of these attributes were considered Vulnerable, while those with 0 or 1 these attributes were considered Exposed.

According to the data, only 10% of organizations represented were classified as Prepared organizations with the highest level of cyber-resiliency maturity.

In comparing technology and business performance both quantitatively and qualitatively across these cohorts, the research validated that greater cyber resiliency correlates to improved IT service uptime, faster incident discovery and response, improved IT service uptime, higher end-user satisfaction, more agile organizational innovation, and a more positive business outlook. The research also provides an empirical roadmap for organizations to follow to improve their own capabilities and results. This research summary paper focuses on the practices organizations should consider for their on-premises data storage environment to improve their cyber-resiliency maturity.

Characteristics of Prepared, Cyber-resilient Organizations

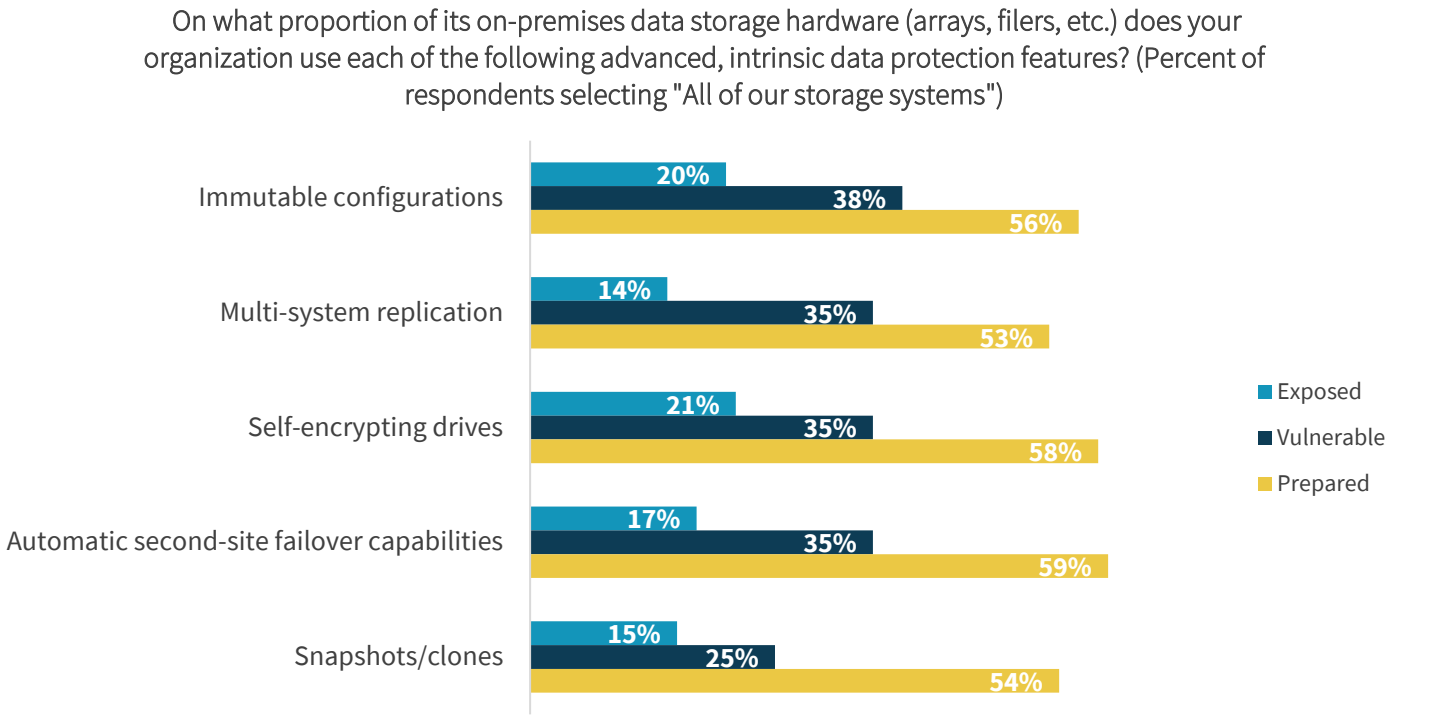
ESG found several key differences between Prepared organizations and organizations with lower levels of cyber-resiliency maturity specific to their on-premises data storage environments. Specifically, ESG found that:

- Prepared organizations have **invested heavily in storage solutions with intrinsic data protection capabilities**, **reducing both outages and data loss** that can be attributed to their storage environments.
- Prepared organizations have **reduced their risk from outages and data loss** due to investments in intrinsic data protection features.
- Prepared organizations are **7.1x more likely** than Exposed organizations to report their storage environment is ready to support their innovation initiatives.

Prepared Organizations Invest in Intrinsic Data Protection Functionality for Storage

Prepared organizations were at least 2.7x more likely than Exposed organizations to have invested in several advanced intrinsic data protection technologies, such as immutable configurations, multi-system replication, self-encrypting drives, automatic failover, and snapshots/clones across all their on-premises storage (see Figure 1). By ensuring that the entirety of the on-premises storage environment is protected, Prepared organizations reduce their vulnerability, and, as a result, reduce the burden on IT personnel—translating into more cycles for them to focus on innovation.

Figure 1. Intrinsic Storage Data Protection Investments by Cyber-resiliency Maturity



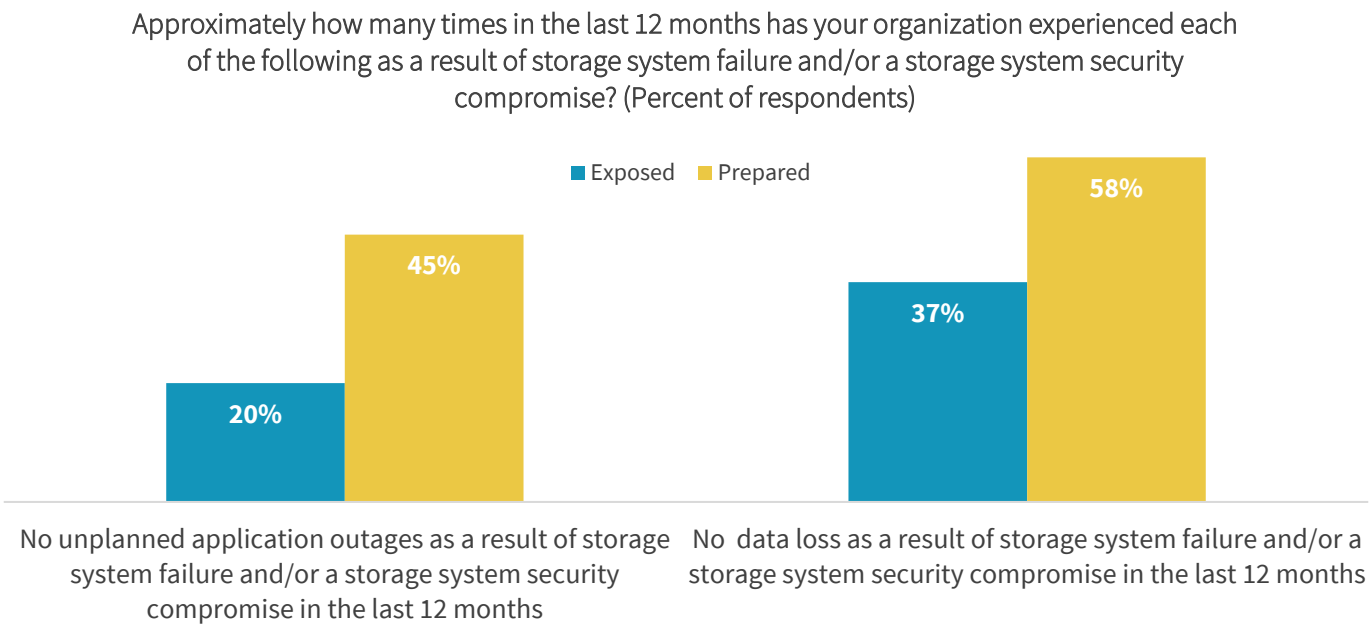
Source: ESG, a division of TechTarget, Inc.

Prepared Organizations Reduce Risk Due to Investments in Intrinsic Data Protection Features

By investing in cyber-resiliency technology across their entire data storage environment, Prepared organizations are far less likely to suffer application outages or data loss (see Figure 2). When compared to Exposed organizations, ESG found that:

- Prepared organizations are **2.3x more likely to report no outages** tied to their storage environment.
- Prepared organizations are **58% more likely to report no data loss** tied to their storage environment.
- Prepared organizations enjoy a **37% average reduction in outages** tied to their storage environment.
- Prepared organizations enjoy a **25% average reduction in data loss** tied to their storage environment.

Figure 2. Likelihood of Experiencing No Outages and No Data Loss by Cyber-resiliency Maturity



Source: ESG, a division of TechTarget, Inc.

The Tie between Cyber Resiliency and Innovation Success

By investing to ensure that the organization's data storage environment has strong resiliency through advanced, intrinsic protection technologies, Prepared organizations better equip IT to minimize the number of fire drills and other unplanned incidents that steal cycles from personnel resources and innovation initiatives.

Prepared organizations are 7.1x more likely than Exposed organizations to report their storage environment is ready to support their innovation initiatives.

Your IT personnel play a significant role in supporting innovation opportunities for your organization. Giving employees and IT more time to focus on innovating instead of time-consuming data storage tasks enables better business outcomes. In fact, ESG found that Prepared organizations are 7.1x more likely than Exposed organizations to report their storage environment is ready to support their innovation initiatives, such as accelerating infrastructure provisioning to support new application development, accelerating access to key data sets of line-of-business teams, or standing up storage infrastructure for a new project.

The Bigger Truth

Cyber-resiliency investments are a necessity given the critical roles of data and IT services in business operations today. This ESG research finds that the value of cyber resiliency extends well beyond minimizing business risk. By reducing the burden on IT resources via fewer unplanned incidents, IT personnel can focus on the vital digital initiatives that create new value for the business.

Investments in cyber resiliency translate into a better environment for fostering innovation. Given the increasing threats, you need an ever-evolving cyber-resiliency strategy to ensure you're always protected—even as you scale your IT environment. While the importance of security is unquestioned, these findings reveal new opportunities afforded to organizations with advanced storage strategies: They not only improve their overall security posture but are better equipped to innovate and differentiate.

Read the eBook

How Dell Technologies Can Help

About Dell Technologies

Technology has never been more important than in today's data-driven era, and Dell believes it is an overwhelming force for good. We're committed to helping safeguard technology's role in human progress by helping you plan, prepare, and protect against attacks so you can build your breakthrough with confidence.

About Intel

On-premises, in the public cloud, or at the edge, Dell Technologies and Intel work together to ensure optimal performance across a broad range of workloads. Intel's data-centric portfolio is built on decades of application optimizations, designed to help your business move faster, store more, and process everything from edge to cloud.

About VMware

Together, VMware and Dell provide unique value to our shared customers. Our integrated platforms and solutions, combined with global scale and deep customer engagements, accelerate the journey to digital transformation. VMware's innovative app modernization, multi-cloud, and Anywhere Workspace software work with Dell Technologies' broad IT portfolio spanning from endpoints to the cloud to help customers achieve secure, consistent operations and faster time to value.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188