Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH SUMMARY

Cyber-resiliency Maturity in Servers

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

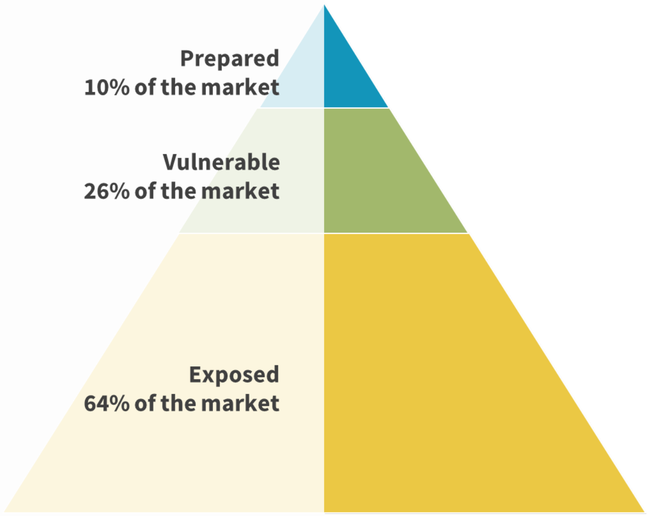
ABSTRACT: Cyber resiliency is now an essential requirement for any business. Given the threat to data and IT servers, businesses must invest in cyber-resiliency strategies to reduce operational risk. New research from ESG, however, finds that cyber-resiliency investments are even more valuable than previously 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.

Levels of Cyber-resiliency Maturity



- 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 server environment to improve their cyber-resiliency maturity.

Server-related 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 server environment. Specifically, ESG found that:

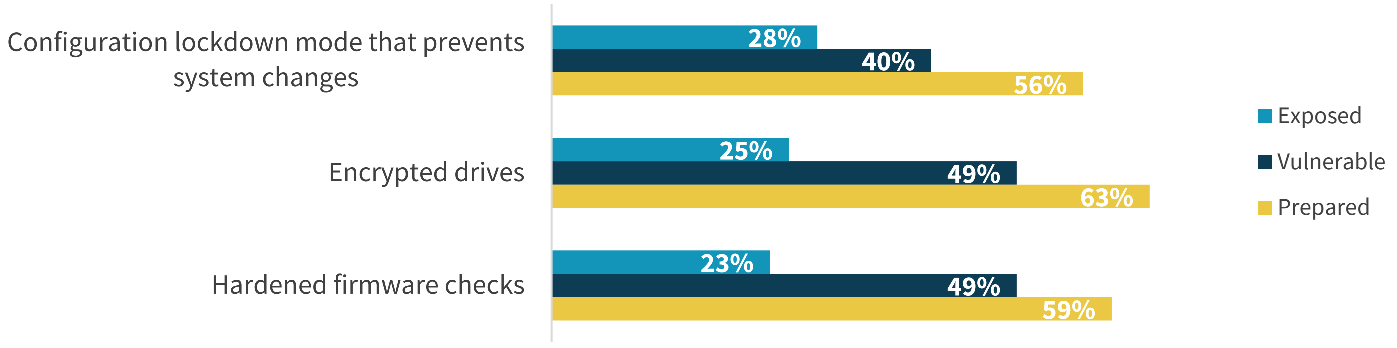
- Prepared organizations have **invested heavily in server solutions with intrinsic security capabilities.**
- Prepared organizations **automate server security/management** workflows, **freeing up more than 40 person-hours per week.**
- Prepared organizations are **6x more likely** than Exposed organizations to report their server environment is ready to support their innovation initiatives.

Prepared Organizations Invest in Intrinsic Data Protection Functionality for Servers

Prepared organizations were at least twice as likely to have invested in each of three advanced, intrinsic data protection technologies across all of their on-premises servers when compared with Exposed organizations (see Figure 1). By ensuring that the entirety of the on-premises server environment is protected, Prepared organizations reduce their risk exposure and, as a result, reduce the burden on IT personnel—which translates into more cycles to focus on innovation.

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

On what proportion of its on-premises servers does your organization use each of the following advanced, intrinsic data protection features? (Percent of respondents selecting "All of our servers")

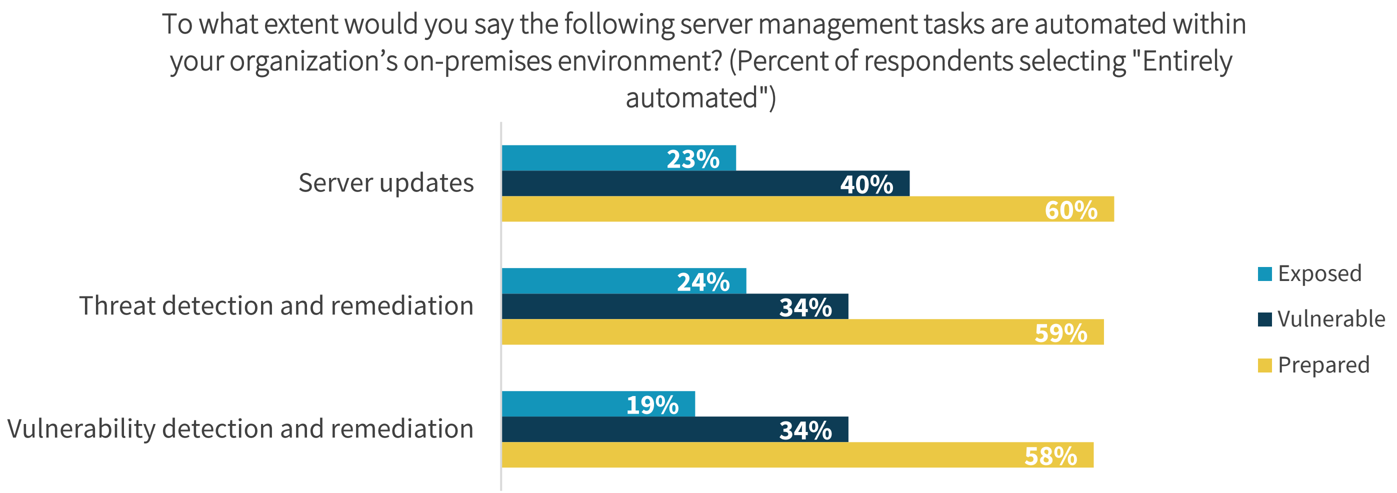


Source: ESG, a division of TechTarget, Inc.

Prepared Organizations Invest Heavily in Automation, Freeing Personnel Time

In addition to investing in cyber-resiliency technology, Prepared organizations were also more than **2x as likely to invest in server automation technology** than their Exposed counterparts (see Figure 2). Those investments led Prepared organizations to estimate that their automation investments freed up an average of 40.7 person-hours per week, 78% more time savings than was estimated by Exposed organizations.

Figure 2. Server Automation Investments 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 entirety of the organization's on-premises server environment has strong resiliency through advanced, intrinsic protection technologies, IT organizations enhance their security. That improved security then minimizes the number of fire drills and other unplanned incidents that often steal valuable cycles from personnel resources and innovation initiatives. ESG found that:

- Prepared organizations are 2x more likely to report no outages tied to their server environment.
- Prepared organizations are 40% more likely to report no data loss tied to their server environment.
- Prepared organizations enjoy a 36% average reduction in outages tied to their server environment.
- Prepared organizations enjoy a 33% average reduction in data loss tied to their server environment.

Prepared organizations also typically add an additional level of operational efficiency by increasing their investments in automation. Personnel play an incredibly significant role in driving innovation and digital business opportunity. By allowing more personnel to focus more time on innovating, businesses achieve superior results. In fact, ESG found that Prepared organizations are 6x more likely than Exposed organizations to report that their server environment is ready to support their innovation initiatives.

> **Prepared organizations are 6x more likely than Exposed organizations to report that their server environment is ready to support their innovation initiatives.**

The Bigger Truth

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

Investments in cyber resiliency translate into a better environment for fostering innovation. Given the increasing volume of threats, cyber resiliency should have already been a high priority within your organization. With these new findings highlighting the connection between cyber resiliency and improved innovation, there is simply no excuse for maintaining a sub-optimal cyber-resiliency strategy.

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.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.’s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

ESG a division of TechTarget

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