ESG RESEARCH SUMMARY

Cyber Resiliency and End-user Performance

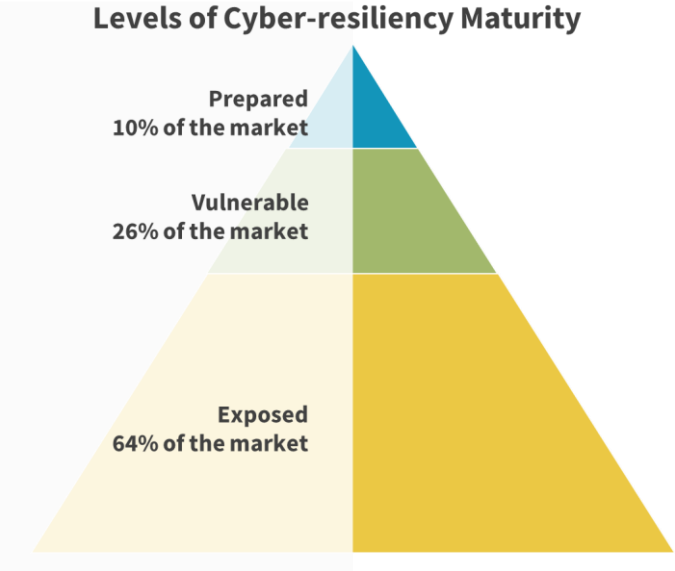
Date: March 2022 **Author:** Dave Gruber, Principal ESG Analyst

ABSTRACT: Cyber resiliency is an essential requirement for any business. Given organizations face larger attack surfaces with users working from anywhere, businesses must invest in mature strategies to reduce risk and unencumber workers. New research from ESG finds that cyber-resiliency investments are even more valuable than previously thought: In addition to minimizing risk, they are critical to innovate and thrive in a do-from-anywhere world.

Research Overview

Improved cyber-resiliency 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 of 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 end-user device environment to improve their cyber-resiliency maturity.

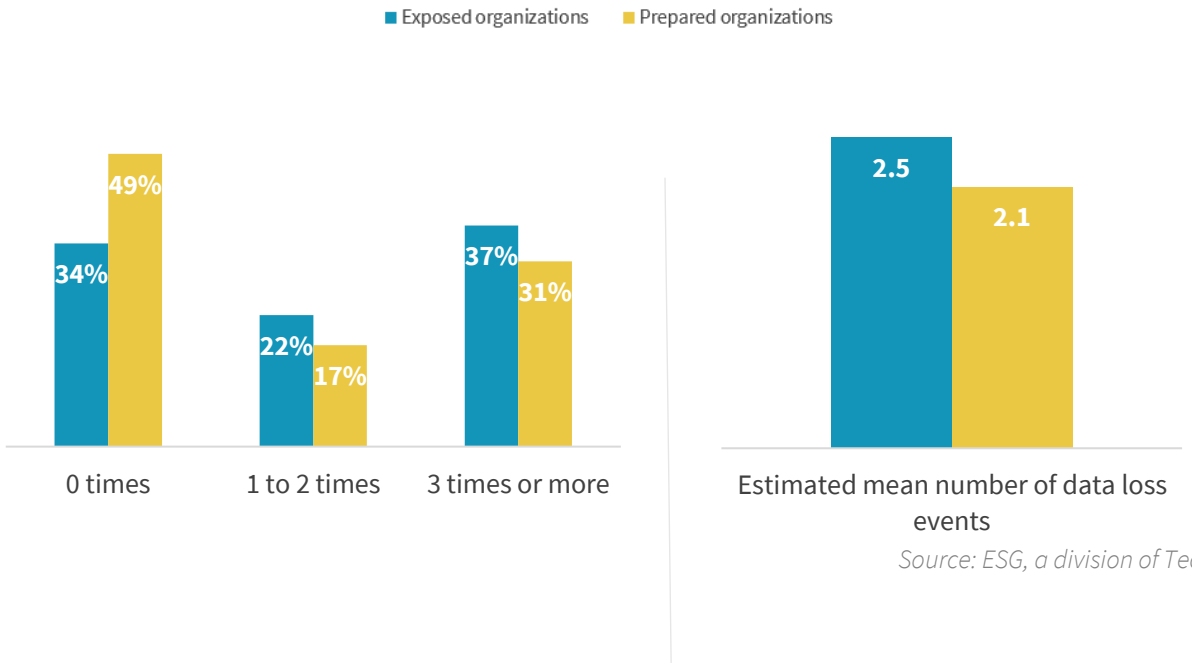
End-user Device Security and Its Impact on Cyber-resilient Organizations

ESG found several key differences between Prepared organizations and organizations with lower levels of cyber-resiliency maturity specific to their value and use of end-user device security across the modern, hybrid workforce. Specifically, ESG found that:

- Prepared organizations are 44% more likely to report no data loss due to device compromise in the last 12 months (see Figure 1).
- Prepared organizations are nearly 2x more likely than Exposed organizations to report less than 1% of their users have suffered a security issue that required device reimaging. As a result, Prepared organizations are 44% more likely to report no data loss due to device compromise in the last 12 months.
- Prepared organizations, on average, shrink their unprotected device footprint by 33%.

Figure 1. Cyber-resilient Organizations Suffer Less Data Loss Due to Device Compromise

How many times in the last 12 months has your organization suffered sensitive data loss or the exfiltration of sensitive data due to a malware infection or other laptop/desktop compromise? (Percent of respondents and estimated mean number of data loss events)

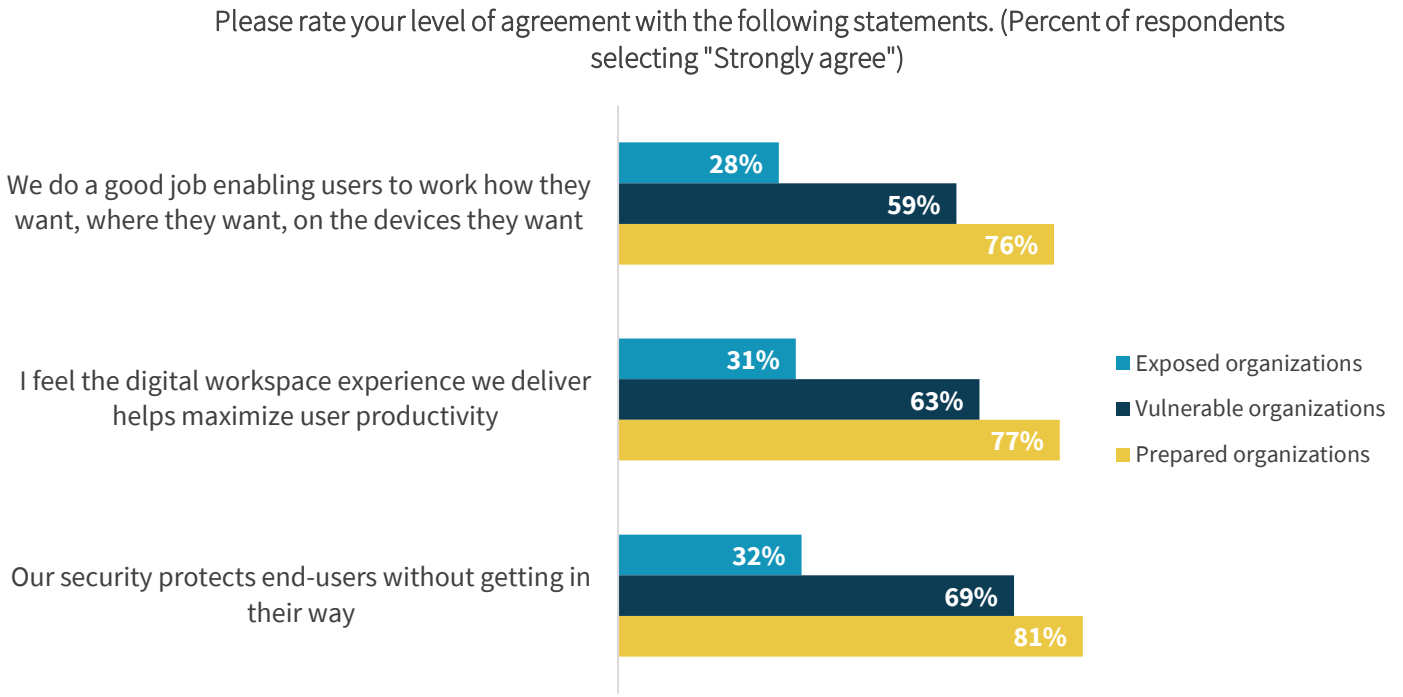


Source: ESG, a division of TechTarget, Inc.

Prepared Organizations Report More Satisfied Workers

Prepared organizations report that they are doing a better job providing workers the choice to work where and how they choose, leading to higher satisfaction scores for digital work experiences. Specifically, ESG found that Prepared organizations are 2.7x more likely to feel that they do a good job enabling workers to do their jobs where, and on the devices, they choose (see Figure 2).

Figure 2. Cyber Resiliency Leads to More Productive Workers



Source: ESG, a division of TechTarget, Inc.

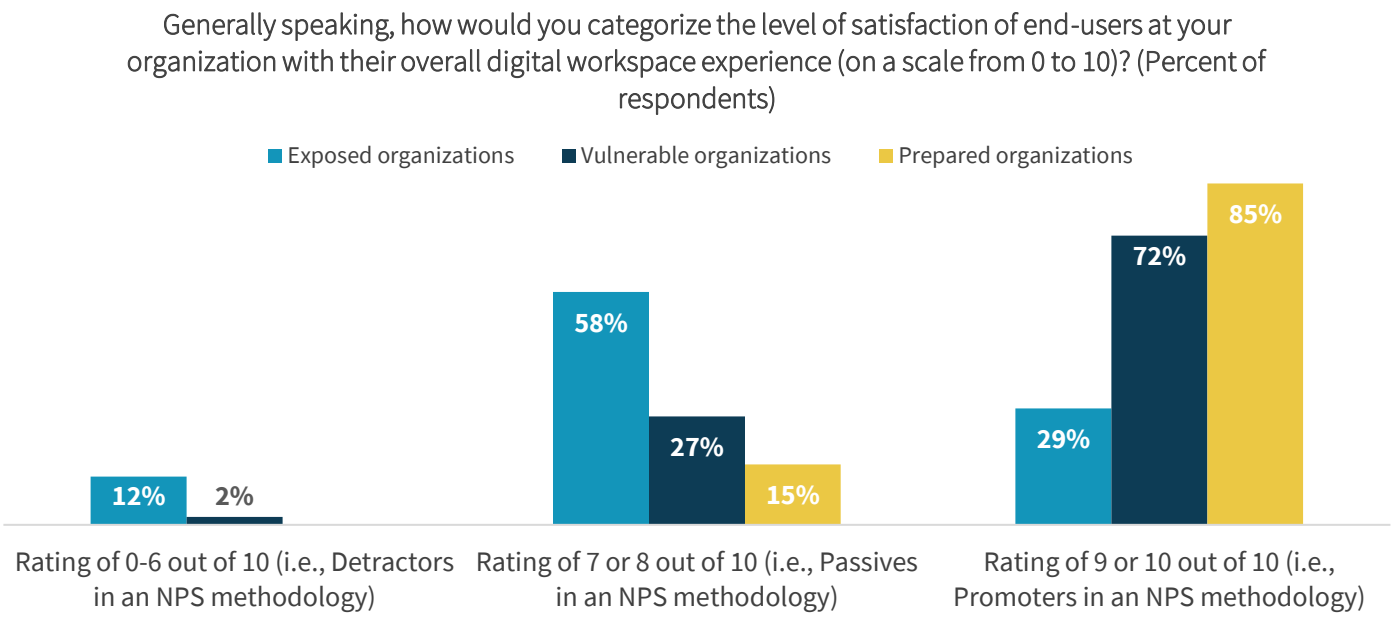
The Tie between Cyber Resiliency and End-user Satisfaction

When workers have the freedom to work where and how they choose without friction, they can stay focused on core organizational objectives. The research shows that Prepared organizations' workers give their IT teams a 5x higher satisfaction score than Exposed organizations' users when it comes to enabling the digital work experience (based on an NPS methodology) (see Figure 3).[1]

Prepared organizations' users give their IT teams a 5x higher satisfaction score than Exposed organizations' users.

1 85% of Prepared organizations say their end users are "promoters," giving their digital work experience a rating of 9 or 10, while 0% say their end-users are detractors, resulting in a +85 NPS for the Prepared organization cohort. By contrast, just 29% of Exposed organizations say their end-users are "promoters," while 12% are detractors, resulting in a +17 NPS for the Exposed organization cohort.

Figure 3. Cyber Resiliency Leads to More Satisfied Workers



Source: ESG, a division of TechTarget, Inc.

The Bigger Truth

Cyber-resiliency investments are a necessity given the critical roles that IT and security teams play across the entire organization. Given the increasing volume of threats, cyber resiliency is already a high priority within each organization.

This ESG research, however, finds that the value of cyber resiliency provided through intrinsic security extends well beyond just minimizing operational risk. Investments in cyber resiliency translate into a better, more positive environment for productivity and innovation. When employees can securely and confidently work anywhere, they are free to focus their greatest efforts on innovation.

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