ESG
a division of TechTarget
Enterprise Strategy Group | Getting to the bigger truth.™

ESG RESEARCH SUMMARY

Intrinsic Security and Cyber Resiliency

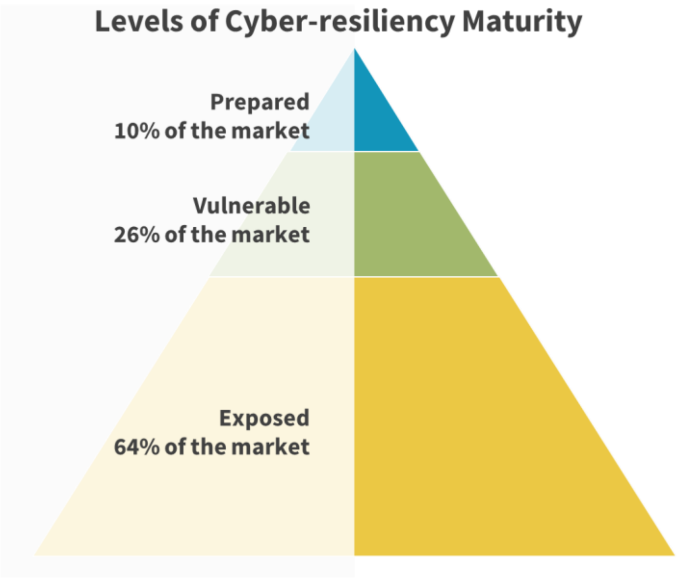
Date: March 2022 **Author:** Dave Gruber, Principal ESG Analyst

ABSTRACT: Cyber resiliency is now an essential requirement for any business. Given the persistent, ongoing threat to data, IT infrastructure, and operations, 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 use of intrinsic security within data center technologies and end-user devices to improve their cyber-resiliency maturity.

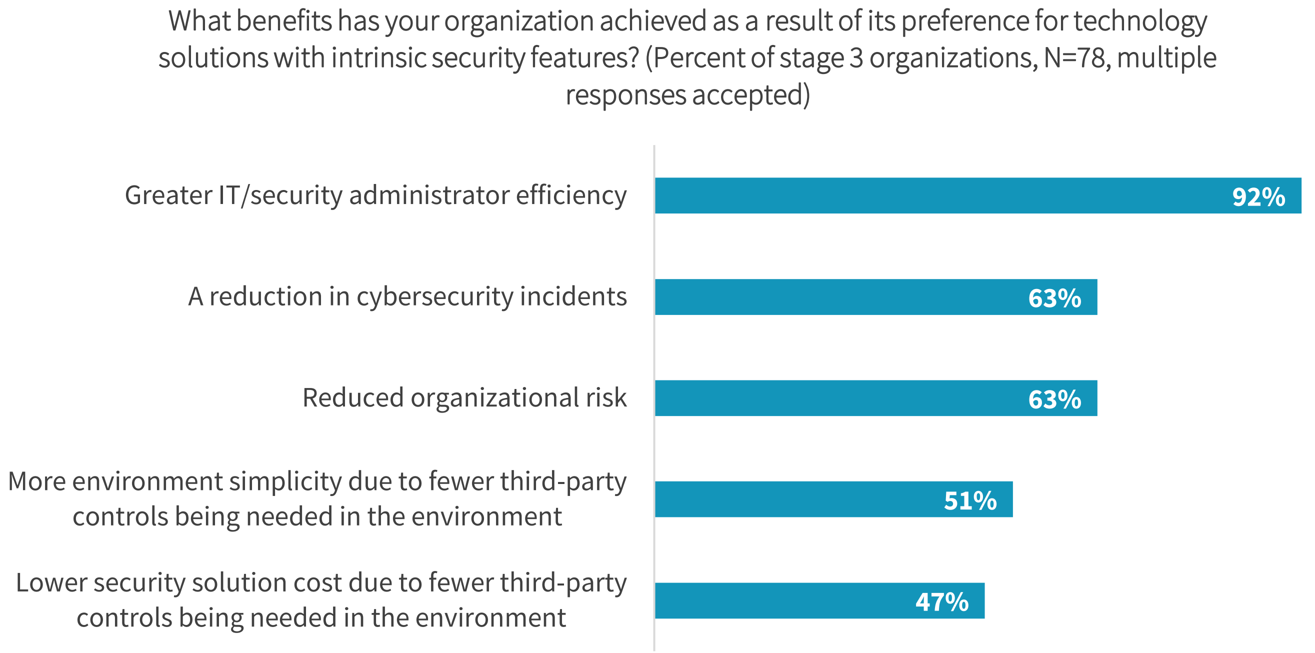
Intrinsic Security and Its Impact on Cyber Resiliency

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 IT spectrum within a modern, hybrid workforce.

Specifically, ESG found that:

- 90% of Prepared organizations report that they have achieved greater IT and security administrator efficiency when managing technology with intrinsic security features (see Figure 1).
- 63% of Prepared organizations report a reduction in organizational risk.
- 51% of Prepared organizations report lower security solutions costs due to fewer third-party controls being needed in the environment.
- 95% of Prepared organizations say intrinsic security is either critical or important to the end-user device purchase process; 90% say the same about data center technology purchases.

Figure 1. Intrinsic Security Results Improve Efficiency While Reducing Incidents and Risk



Source: ESG, a division of TechTarget, Inc.

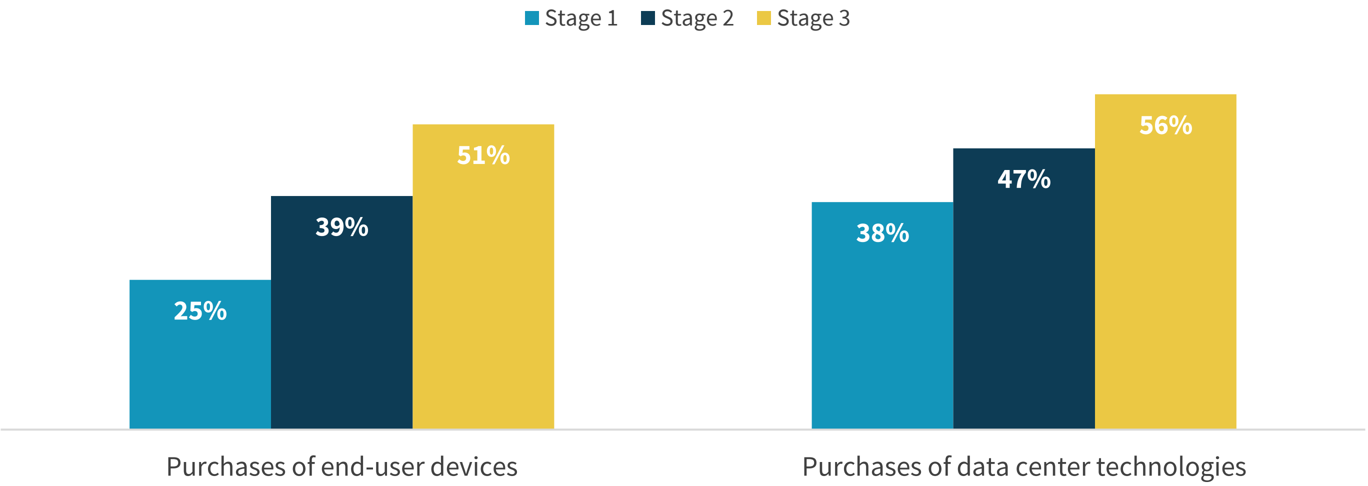
Prepared Organizations Place a Higher Value on Intrinsic Security

A majority of Prepared organizations rate technology solutions' intrinsic security features as critical to the purchase process. Specifically, ESG found that:

- For end-user device purchases, Prepared (Stage 3) organizations are 2x more likely than Exposed (Stage 1) organizations to rate intrinsic security features as critical (see Figure 2).
- For data center technology purchases, Prepared organizations are 47% more likely than Exposed organizations to rate intrinsic security features as critical.

Figure 2. Criticality of Intrinsic Security to Technology Purchasing by Stages

In the purchase processes below, how important is a technology solution's intrinsic security features to the final purchase decision? (Percent of respondents selecting "Critical")



Source: ESG, a division of TechTarget, Inc.

The Tie between Cyber Resiliency and Innovation Success

Organizations that ensure their entire data center and end-user environment have strong resiliency through intrinsic security technologies minimize the number of fire drills and other unplanned incidents that take focus away from innovation.

By standardizing on secure and intelligent technologies that mitigate cyber risk, IT teams enable workers to focus their greatest efforts on innovation and create new value for the organization. In fact, ESG found that Prepared organizations are 6x more likely than Exposed organizations to report their server environment is ready to support their innovation initiatives.

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

The Bigger Truth

Cyber-resiliency investments are a necessity given the critical roles 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. By reducing the burden on IT and security resources via fewer incidents, organizations elevate their innovation potential and enable their people to focus on vital initiatives.

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