ESG RESEARCH SUMMARY

A Focus on Cyber Resiliency Enables Business Innovation

Date: April 2022 **Author:** Adam DeMattia, Senior Director, Custom Research

ABSTRACT: CIOs are tasked with driving their organizations' use of technology to modernize and remain competitive. As technology continues to reshape the way business is done, CIOs are often responsible for the success or failure of their organization's ability to adapt, innovate, and thrive. But innovation cannot proceed without a counterbalancing focus on risk. CIOs must strike a balance between the two, and new research uncovers that a focus on cyber resiliency to mitigate risk allows innovation to accelerate without disruption.

Introduction

The modern CIO is placed in a unique position to both enable their company to adopt new technologies that allow the organization to compete and win and also manage the tools and teams that protect the organization from being disrupted by cyber incidents or outages. Oftentimes, this dual mandate can seem at odds with itself: A focus on risk mitigation argues for predictability and minimal change over time, while a focus on innovation promotes the use of new, unproven technologies to drive change.

However, ESG's recently completed research shows how resiliency actually promotes innovation. The research can be used by CIOs as a roadmap for how to build a more resilient *and* innovative company.

CIOs Are Acutely Focused on Resiliency

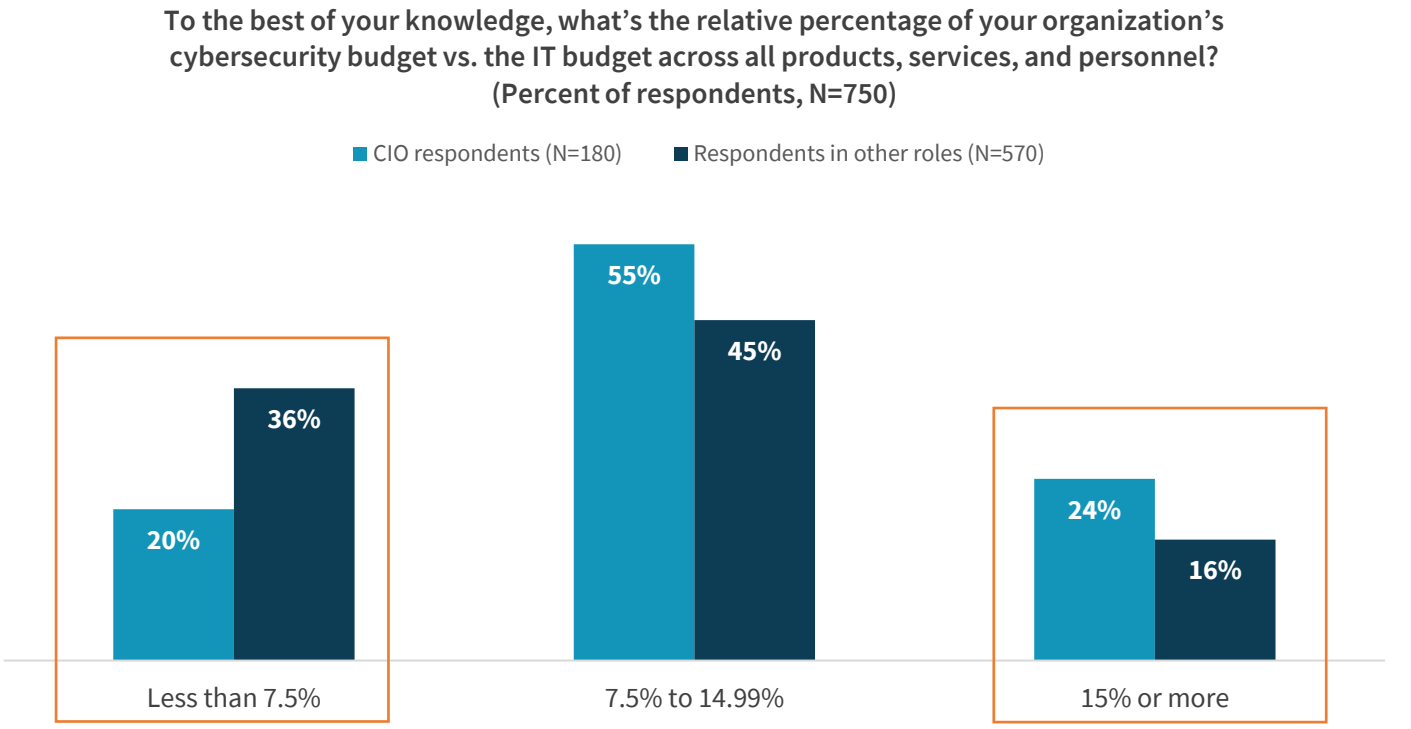
The research uncovered three key sets of findings that show just how focused CIOs are on creating cyber-resilient organizations.

Budget: CIOs Are Focused on Ramping Cybersecurity Investments

The research quantified the percentage of organizations' technology budgets—spanning people, services, and technologies—that are allocated to cybersecurity specifically. While this question was asked of all respondents, the CIO is the owner of organization-wide technology investments and thus should be able to provide the most accurate answer to the question. When we compare the responses of CIOs in the survey to other respondents (e.g., IT and cybersecurity managers and practitioners), we see a statistically significant difference: CIOs report that their organizations are investing more in cybersecurity (see Figure 1).

This shows that the individuals in the organization with the most knowledge of, and the most influence over, their company's technology spending place greater emphasis on security investments.

Figure 1. Percent of Technology Budget Reported to be Allocated to Cybersecurity, by Respondent Role



Source: ESG, a division of TechTarget, Inc.

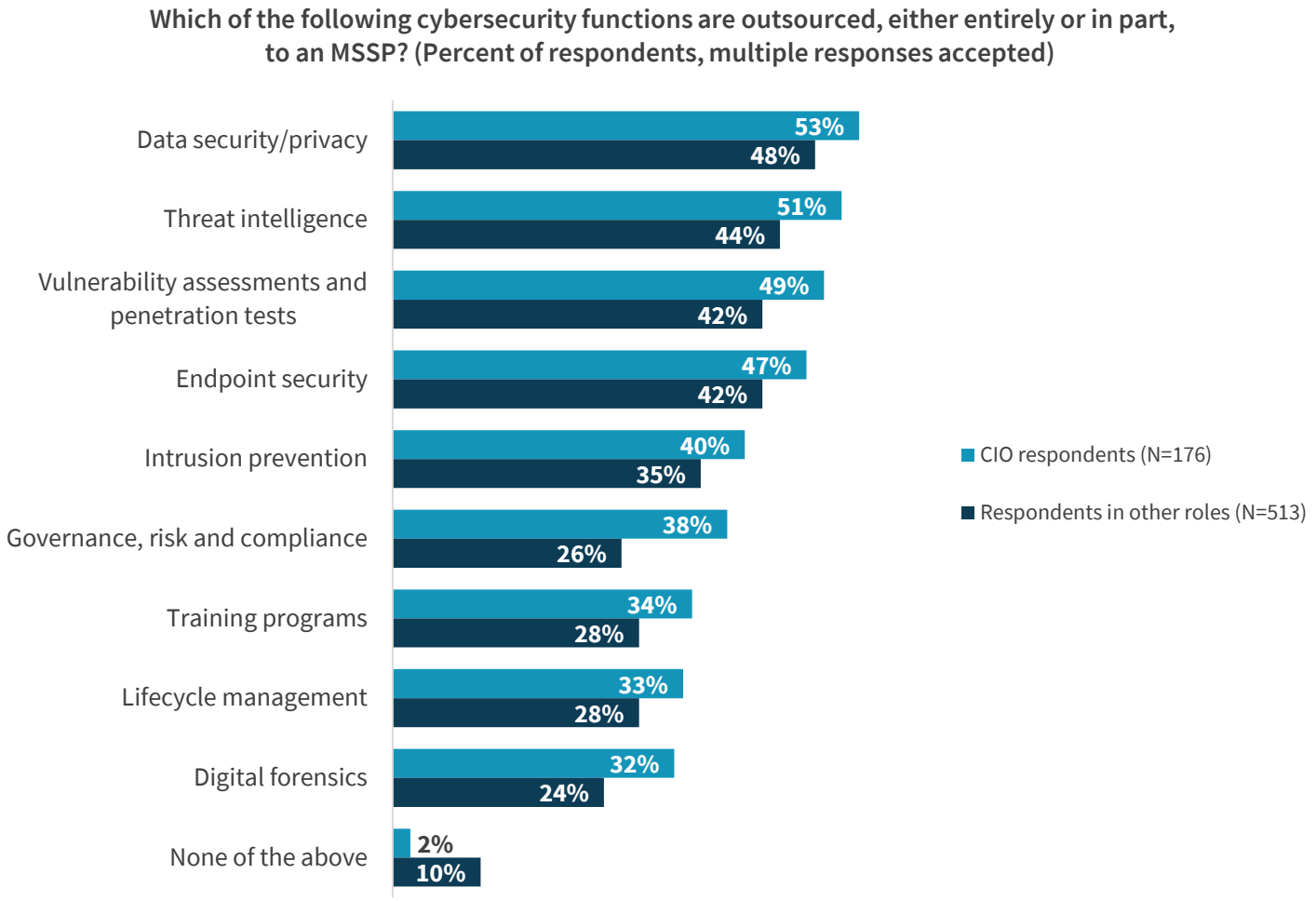
CIOs Report Numerous Strategic, Risk-focused Partnerships

The research covered the use of managed security service providers (MSSPs), including not only whether the organization partners with those service providers, but in what areas. The data implies that these risk-focused partnerships are more top of mind for CIOs, with 98% reporting that some aspect of their cybersecurity program is bolstered by MSSPs (versus 90% of respondents in other roles).

In addition to being more likely to report their organization is reliant on these partnerships, CIOs were significantly more apt to say they are leveraging MSSPs in specific areas: to help with governance, risk, and compliance (GRC) and for digital forensics (see Figure 2).

The implication of the data is that CIOs recognize there are aspects of the security program that their internal staff are not equipped, or not as well as equipped as an MSSP, to conduct. In these cases, opportunistically adding MSSPs to the program can improve efficiency and efficacy. However, it is worth noting that third parties must be inspected from a risk perspective: 71% of CIOs report they rigorously inspect partners' third-party risk.

Figure 2. Security Services Provided or Bolstered by Managed Security Service Providers, by Respondent Role

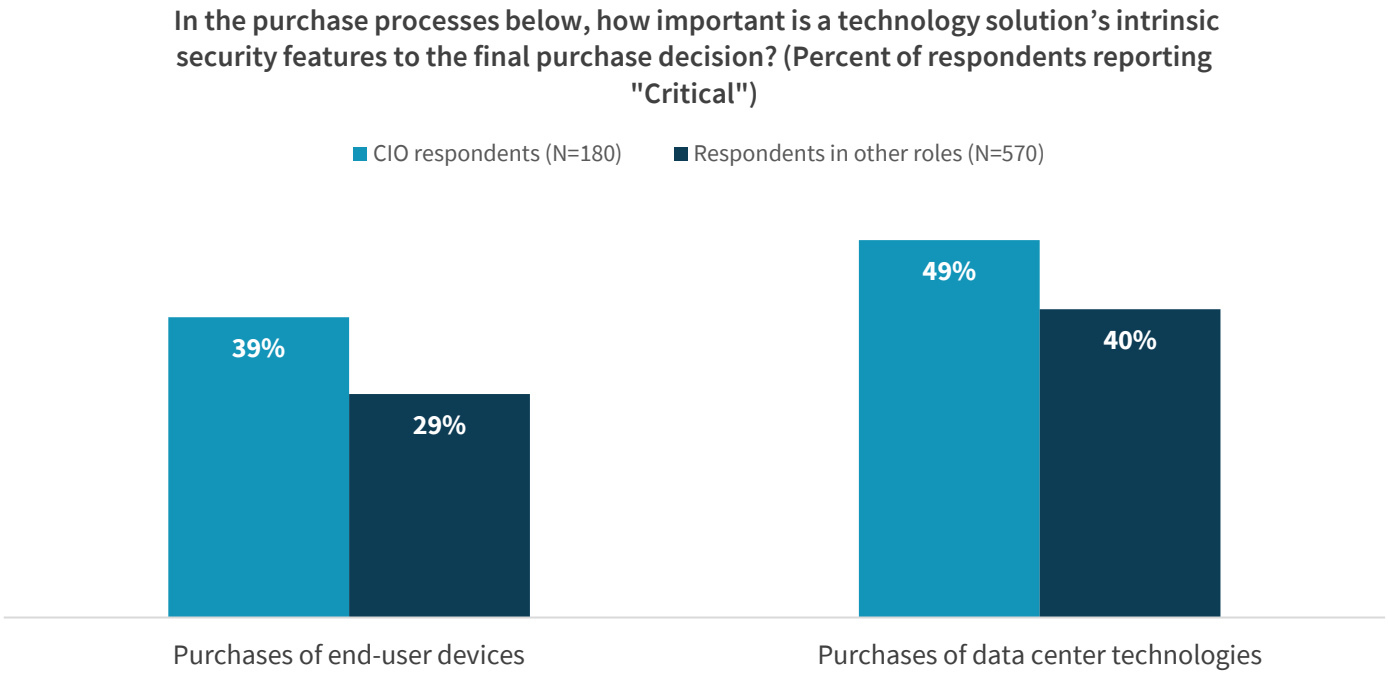


Source: ESG, a division of TechTarget, Inc.

CIOs Put an Emphasis on Technologies with Intrinsic Security Capabilities

Intrinsic security refers to security features "baked into" technology hardware, independent of third-party protection and security products. These features can include a secure supply chain for technology components, automated security checks, built in data protection capabilities, secure configurations out of the box, and signed firmware updates, among others. All respondents were asked how important a product's intrinsic security capabilities are in the purchase process. CIOs in the survey were significantly more likely than their less-senior counterparts to report that these features are critical to a final purchase decision (see Figure 3). This holds true whether CIOs were evaluating data center infrastructure (e.g., servers, storage, HCI, etc.) or client devices (e.g., laptops, desktops, etc.).

Figure 3. The Importance of Intrinsic Security Features in the Technology Purchase Process, by Respondent Role



Source: ESG, a division of TechTarget, Inc.

Why do CIOs place a premium on these technologies? A high percentage of CIOs surveyed associate benefits like greater administrator efficiency (74%), reduced organizational risk (57%), and a measurable reduction in cybersecurity incidents (56%) directly tied to their investments in technologies with intrinsic security features.

Ransomware: A Convincing Example of How High the Cyber-Resiliency Stakes Have Become

A ransomware attack is when malware blocks access to data or systems by encrypting them until a monetary payment is made to the perpetrator. Recent high-profile attacks on organizations like Kaseya, JBS USA, and Colonial Pipeline have captured headlines, and rightfully so, given the disruption they've caused.

While there are steps organizations can take to make themselves more resilient to such attacks (for example, maintaining an air-gapped copy of critical data), the research shows that many organizations are targets and a meaningful subset have been victims: 47% of respondents reported uncovering and remediating attempted ransomware attacks prior to access being lost in the last 24 months, and 24% of respondents reported that their organization had fallen victim to a successful ransomware attack over the same time horizon.

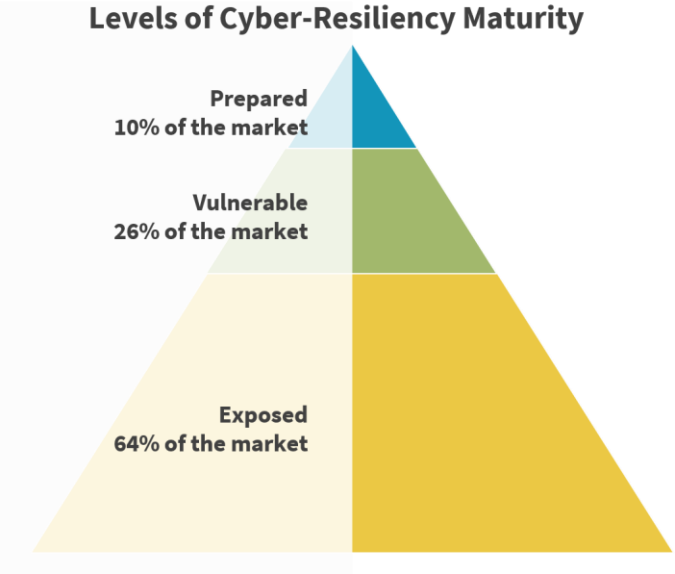
Among those affected, the most common response has been to pay the perpetrators, with 30% saying they have typically paid ransoms directly and another 34% reporting their cyber-insurance company has typically made the payment. In the aggregate, respondents report the average largest payment their organization had made was over $560,000.

Whether due to the direct financial implications of potentially numerous successful ransomware attacks that can plague organizations or the business fallout from disrupted operations, ransomware is a case study in why CIOs are so focused on cyber resiliency today.

Research Shows Resiliency Enables Rather than Stifles Innovation

Improved cyber-resiliency capabilties help to reduce risk. However, returning to the dual mandate of the CIO, what is the impact on an organization's ability to foster innovation and deliver greater business success?

The research discussed in this summary answers this question. In total, 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.

Figure 4. Benefits Correlated with Cyber-Resiliency Preparedness

Source: ESG, a division of TechTarget, Inc.

The Bigger Truth

CIOs are highly focused on cyber resiliency. And given their dual goals of promoting innovation while also ensuring uptime and security, it is clear that a continued focus in this area has related advantages in gaining a competitive advantage, revenue growth, and overall business performance.

Read the full research report

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