ESG a division of TechTarget

Enterprise Strategy Group | Getting to the bigger truth.™

How to Build a Cyber-resilient Business Ready to Innovate and Thrive

Adam Demattia, Senior Director, Custom Research

MARCH 2022

CONTENTS

Research Objectives and Methodology

OBJECTIVES:

This eBook discusses if, and to what degree, an organization's adoption of a strong cyber-resiliency strategy is correlated with IT predictability, business innovation, and success. These relationships will be uncovered based on peer-based data. When you read this eBook, you will:

- Understand how we define and measure cyber resiliency and where your organization stands today.
- Quantify what highly resilient organizations gain over their peers, both in terms of IT and business performance.
- Finally, by understanding what cyber-resilient organizations do, you will see how your organization needs to evolve its practices and priorities to perform like a market leader.

METHODOLOGY:

In the first quarter of 2022, ESG conducted a double-blind survey[1] of 750 IT and security decision makers knowledgeable about the cybersecurity and resilience technologies in place to protect both data center and end-user device environments.

Organizations represented spanned midmarket and large enterprises and the sample was composed of a horizontal mix of industry verticals. The research was also global in nature, spanning North America (N=187), Western Europe (N=185), APAC (N=179), and LATAM (N=199).

[1] Respondents were anonymous and not informed ESG was conducting the survey or that it was commissioned by Dell Technologies.

Highlighted Findings

In this eBook, Prepared organizations are those with an optimal level of security technology investment, staffing level, and rigorous third-party risk inspection. Our research shows only 10% of organizations surveyed have reached this level of resiliency today, underscoring the need for organizational focus and improvement.

Cyber-resilient organizations minimize disruption. Prepared organizations are:

7.3x more likely
to rate their resiliency posture as excellent.

2.5x more likely
to deliver 99.99% uptime or better for their business-critical apps, equating to an estimated US$33.3M cost of downtime advantage.

Far more agile
when it comes to incident detection (20% faster mean time to detect [MTTD]) and responses (35% mean time to recover [MTTR]).

Cyber resiliency is correlated with improved business performance. Prepared organizations are:

8.5x more likely
to say their end-user satisfaction scores typically outpace their goals, driven by better service and end-user experience.

7.7x more likely
than Exposed organizations to get new offerings to market ahead of the competition.

Forecasting that their organization’s revenue will grow at
2x the rate
of their peers.

Defining and Measuring Cyber Resiliency

Four characteristics of a Prepared (or highly resilient) organization

To determine if a respondent's organization could be categorized as Prepared, we looked at their responses to four key questions related to resiliency staffing levels, skill gaps, technology investment, and risk assessment processes:

PEOPLE

How would you describe the level of staffing in your cybersecurity team?

☑ No open positions

□ Poorly staffed, short staffed, or adequate

How would you describe the level of skills in your organization's cybersecurity team?

☑ No skill gaps

□ Many skill gaps, several skill gaps, or adequate

RESILIENCY TECHNOLOGY

How would you characterize your organization's investment in products and services to secure its systems, applications, and data?

☑ Optimal

□ Poor, needs improvement, or adequate

THIRD-PARTY RISK

Does your organization audit or inspect the security of its partners/IT vendors?

☑ Formally and rigorously

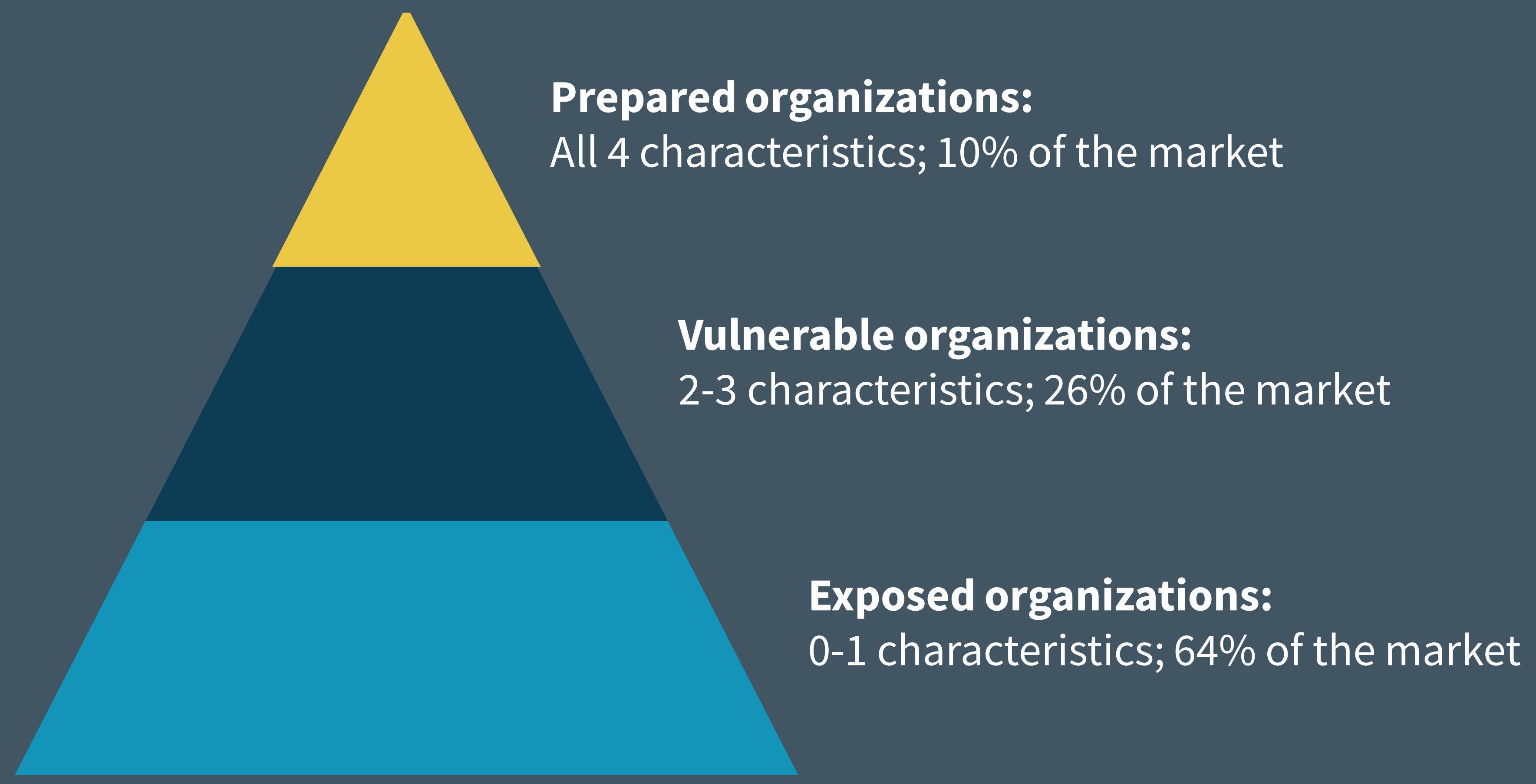
□ Informally, casually, or not at all

Organizations by their resiliency
(Percent of respondents, N=750)

ESG created a data-driven model that segments respondents' organizations into three levels of resiliency:

Prepared organizations, Vulnerable organizations, and Exposed organizations.

The model uses the four questions at left from the survey as inputs to determine an organization's status. 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. The more characteristics the organization has in place, the greater their resiliency, as noted below:



Prepared organizations:
All 4 characteristics; 10% of the market

Vulnerable organizations:
2-3 characteristics; 26% of the market

Exposed organizations:
0-1 characteristics; 64% of the market

Back to Contents

Cyber-resilient Organizations Minimize Disruption

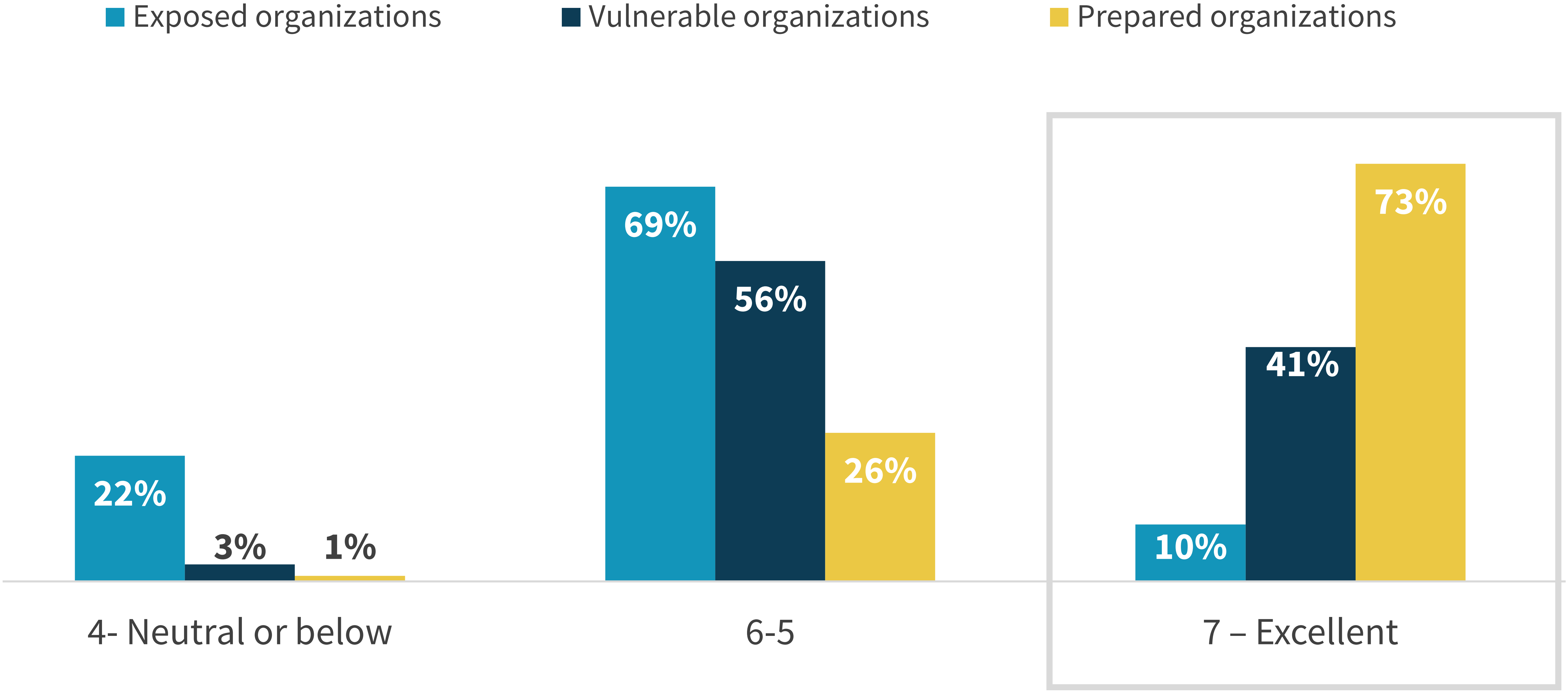
Prepared organizations are much more confident in their stage of cyber resiliency than their peers

While qualitative, measuring IT and cybersecurity leaders' confidence in their organizations' resiliency posture is important. These individuals shape and drive their organizations' strategies and are best positioned to evaluate success executing those strategies.

To measure confidence, we asked respondents to rate their cyber resiliency from 7- excellent down to 1- poor. Respondents were generally positive, but only 24% of organizations rated their cyber resiliency as "excellent," reflective of a cautiously optimistic tone in the aggregate.

However, confidence varies significantly by organizations' resiliency level. Nearly three-quarters of Prepared organizations (73%) rate their resiliency as excellent.

How would you rate your organization's overall cyber resiliency (i.e., your ability to withstand a cyber attack and continue business operations)? (Percent of respondents)



Prepared organizations are
7.3x more likely
than Exposed organizations to rate their resiliency posture as "excellent."

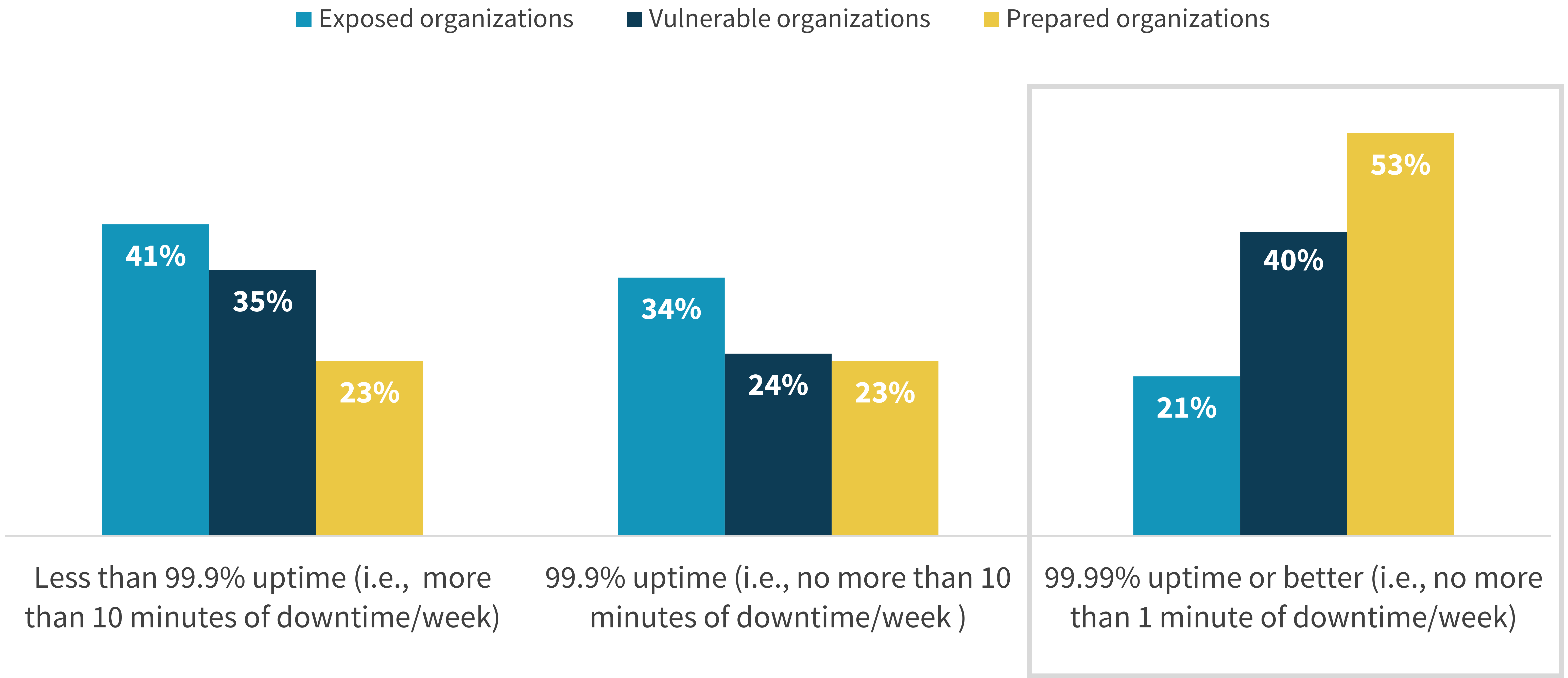
Comparing business-critical application uptime achieved across cyber-resiliency levels

Just as, if not more important than, qualitative measures of resiliency are quantitative measures like uptime, mean time to detect (MTTD) incidents, and mean time to recover (MTTR) from them. Each is benchmarked by the research.

At the heart of organizational resiliency is the protection of business-critical processes. For IT and security teams, that means keeping business-critical application workloads that underpin those processes up and running.

When we compare organizations' success in this area, it's clear to see the divide: Prepared organizations are 2.5x more likely than Exposed organizations to deliver 4 9s of uptime or better for their business-critical apps (equating to not more than 1 minute of downtime per week, 53% versus 21%).

What is the typical uptime SLA your organization delivers for business-critical workloads?



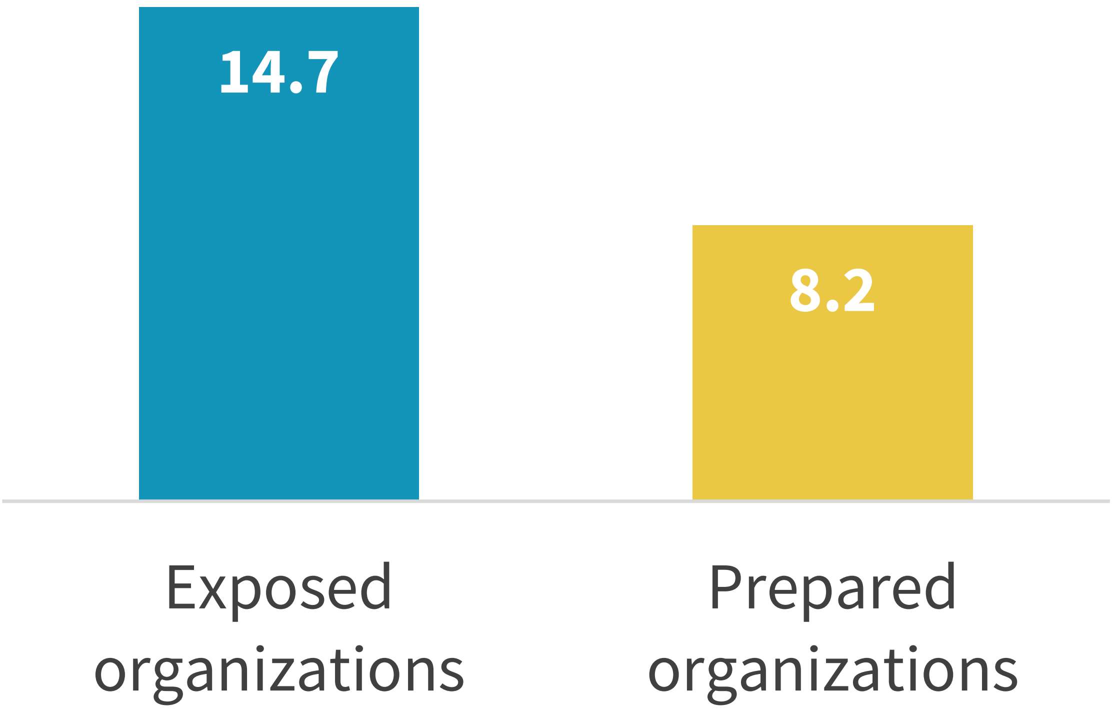
Prepared organizations are
2.5x more likely
to deliver 99.99% uptime or better for their business-critical apps.

What’s the cost of downtime advantage Prepared organizations achieve?

The research allows us to answer this key question. Clearly staffing up, investing in more resilience technologies and rigorous inspection of third-party risk has a cost component. However, the data shows us there is a significant return on that investment: Prepared organizations reduce business-critical application downtime by 44%. Combining that data with the average hourly cost of downtime reported by respondents in the research and multiplying that economic impact by the total number of business-critical applications, the data shows that Prepared organizations achieve a US$33.3M per year cost of downtime advantage over Exposed organizations.

DOWNTIME

Average hours of downtime per-app per-year



×

AVERAGE HOURLY COST OF DOWNTIME[1]

×

AVERAGE TOTAL NUMBER OF BUSINESS-CRITICAL APPLICATIONS[2]

=

Cost of downtime
ADVANTAGE
for Prepared organizations:

$33.3M/Yr

[1] Mean reported hourly cost of downtime by respondents = US$205K, [2] Assumed average number of business-critical applications supported: 25 (a conservative assumption)

Back to Contents

Alert handling and incident response agility across cyber-resiliency levels

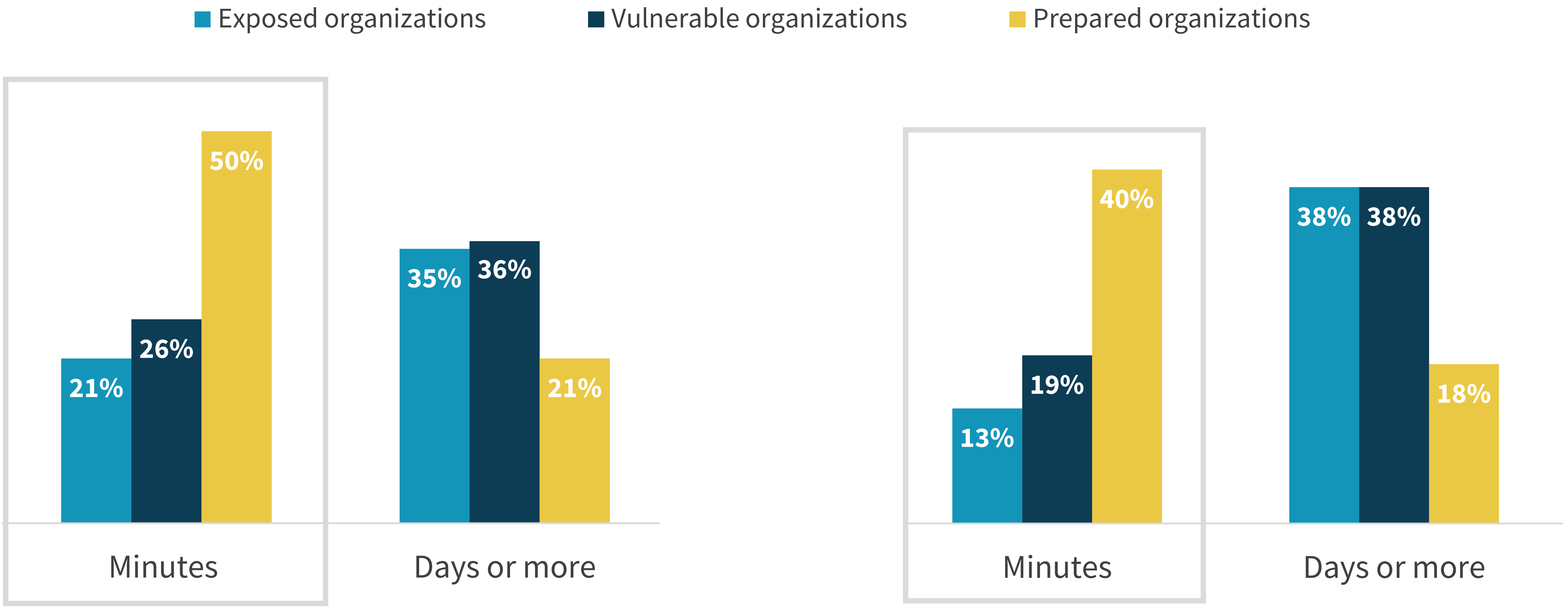
When it comes to how Prepared organizations deliver greater uptime and availability, the data is once again clear: they have far greater agility than their peers when it comes to investigating, identifying, and responding to incidents.

When it comes to investigating and identifying cyber incidents, we defined MTTD as the amount of time that transpires from when an alert is generated until your organization fully investigates it to determine whether a security incident has taken place. Here, Prepared organizations are 2.4x more likely than Exposed organizations to be able to investigate alerts in a matter of minutes (resulting in a 20% faster average MTTD).

To measure response agility, we defined MTTR as the average amount of time that elapses from cyber-incident notification until full restoration of information system operations. On this measure, Prepared organizations are 3.1x more likely than Exposed to typically recover from incidents in a matter of minutes (resulting in a 35% faster average MTTR).

What is your organization's MTTD for business-critical workloads? (Percent of respondents)

What is your organization's MTTR for business-critical workloads? (Percent of respondents)



Prepared organizations are
2.4x more likely
to typically investigate alerts in a matter of minutes.

Prepared organizations are
3.1x more likely
to typically recover from incidents in a matter of minutes.

Back to Contents

Cyber-resilient Organizations Outperform their Peers in Terms of Business Outcomes

Resilient organizations deliver market-leading end-user experience

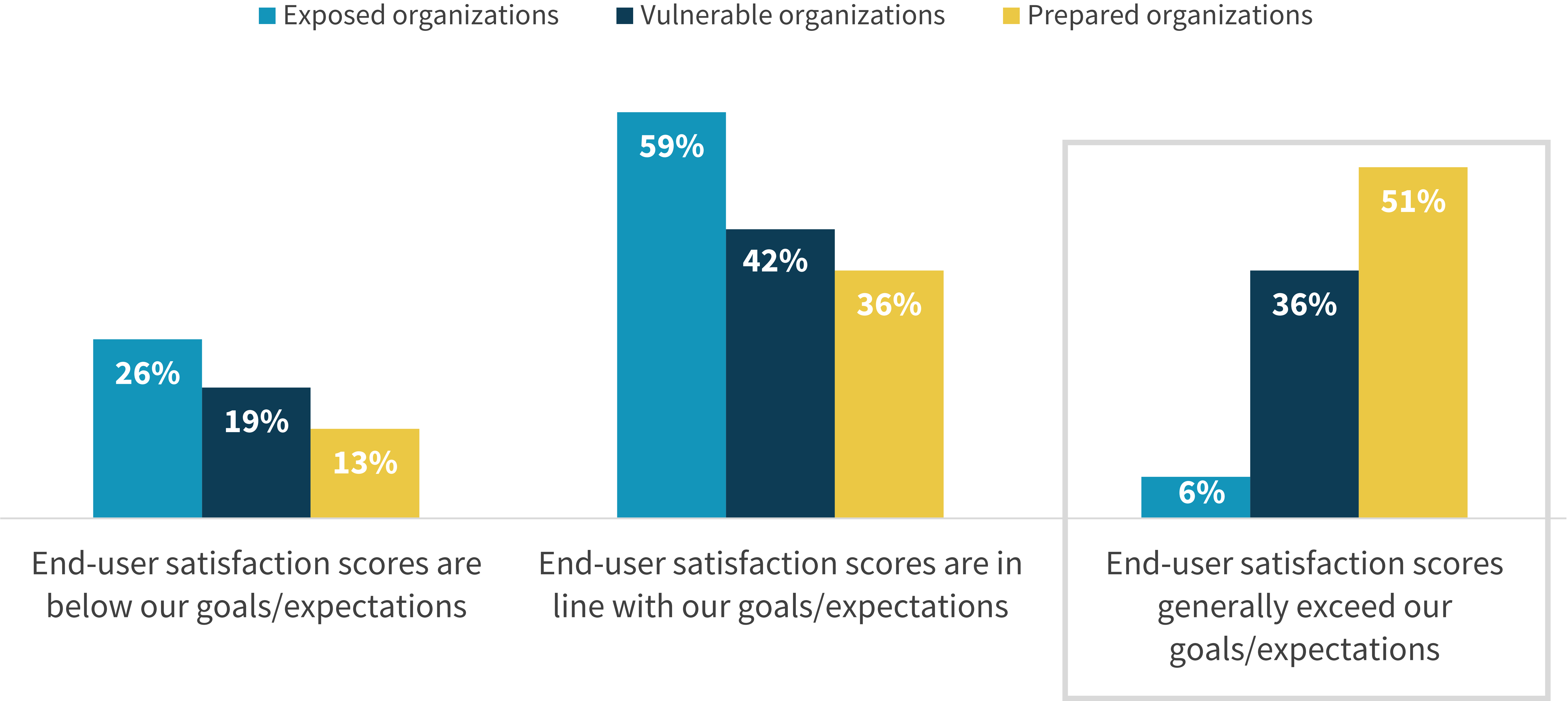
Resiliency, like many aspects of IT, has the goal of being invisible to end-users. It's when the unexpected happens that resiliency gaps are felt.

The data shows Prepared organizations do a superior job (relative to their peers) at limiting disruption. And the data shows it results in improved end-user satisfaction.

We asked respondents how the IT organization performs against its end-user satisfaction goals. The majority of Prepared organizations report generally outstripping their targets. In fact, Prepared organizations are 8.5x more likely than Exposed organizations to say their end-user satisfaction scores typically outpace their goals.

There is a clear correlation between resiliency level and the ability of IT to deliver the end-user experience line-of-business constituents demand.

How does your IT organization generally perform in terms of formal end-user satisfaction goals? (Percent of respondents)



Prepared organizations are

8.5x more likely

to say their end-user satisfaction scores typically outpace their goals.

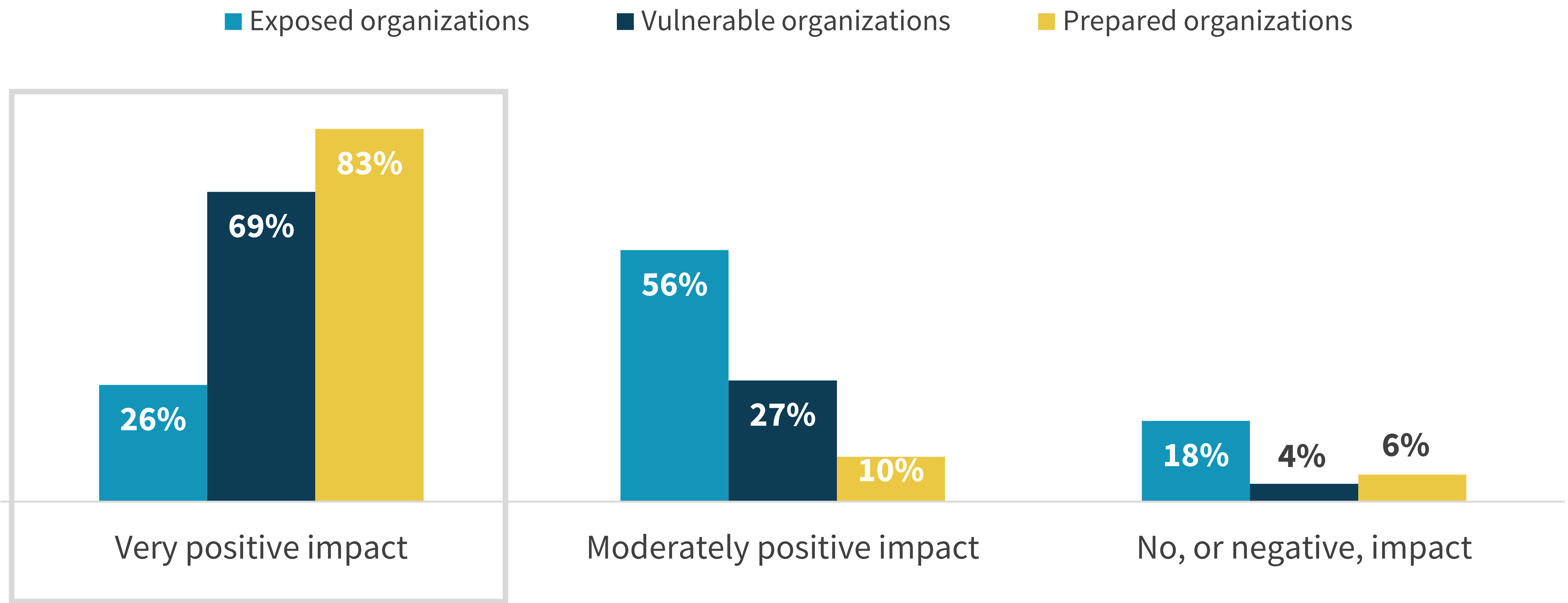
More than just correlation, resiliency drives EUX improvement

Of course, correlation does not equate to causation, but the research provides evidence of a definitive causal link between investments in resilience and improved EUX.

We asked if respondents believe their organizations' investments in resiliency have had a positive, neutral, or negative impact on things like agility, innovation, and end-user experience, and 87% reported a positive impact.

Going a layer deeper and examining the data by resiliency level, Prepared organizations are 3.2x more likely than Exposed organizations to say their resiliency investments have very positively improved EUX, agility, and innovation.

Have your organization's investments in resiliency had a positive/neutral/negative impact on agility, innovation, and end-user experience? (Percent of respondents)



Prepared organizations are

3.2x more likely

to say their resiliency investments have a very positive impact.

How investing in resilience moves the needle for businesses

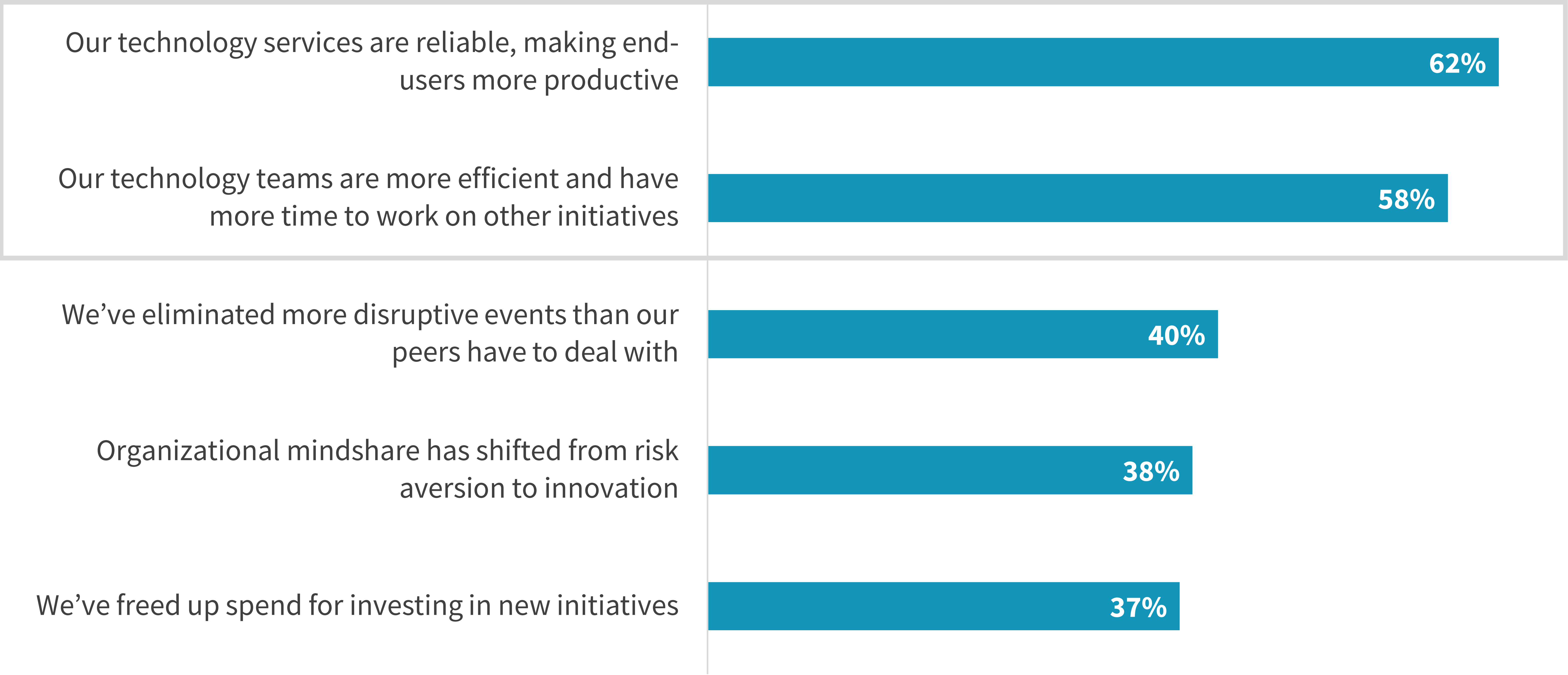
The question of how resiliency improves business capabilities is an interesting one and answered by the research.

Two key, and complementary, impacts stand out. First, resiliency gets your business stakeholders and profit centers humming: 62% of respondents report their investments help ensure the technology services end-users rely on to be effective and efficient are available and performant.

Second, 58% of respondents report investing in a strong foundation of resiliency means technology teams are fighting fewer fires, allowing them to turn their efforts to supporting and accelerating innovative projects and initiatives that will give their organizations a competitive edge.

> “Two key, and complementary, impacts stand out.”

How are investments in resiliency helping your business succeed? (Percent of respondents)

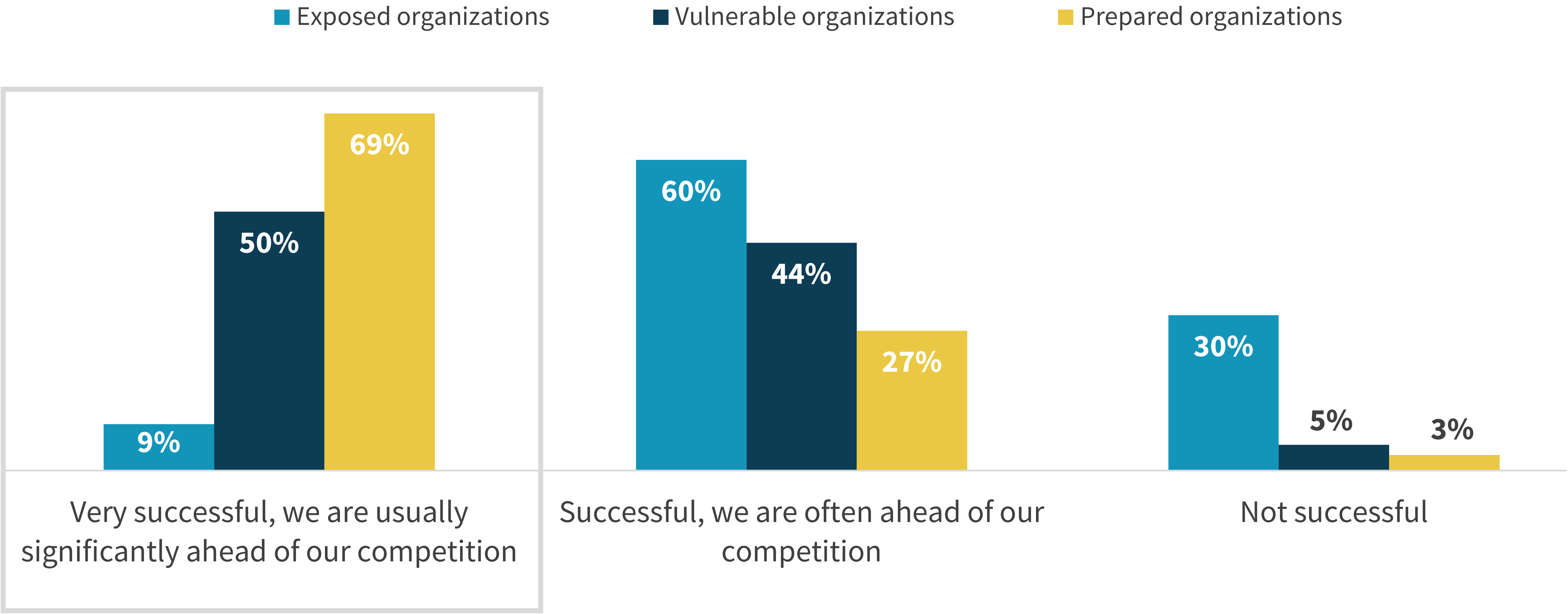


Resilient organizations are better able to support innovation

The data pointing to resiliency's ability to support organizational innovation is strong. Prepared organizations are 7.7x more likely than Exposed organizations to usually get new offerings to market. ahead of the competition.

When asked to further discuss this advantage, in the aggregate, Prepared organizations on average report their organizations are typically over 8 months ahead of their competitors in time to market, a dramatic first-mover advantage.

How successful is your organization at developing and launching new products and services, relative to its competition? (Percent of respondents)



Prepared organizations are

7.7x more likely

to usually get new offerings to market ahead of the competition.

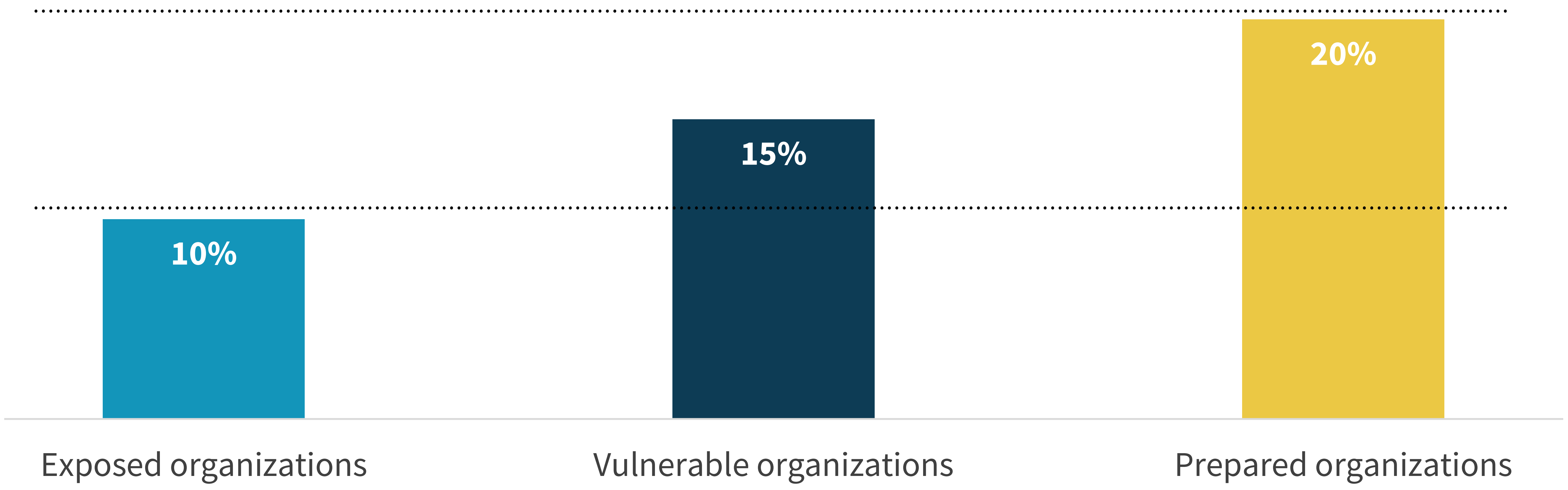
Resilient organizations are more bullish in terms of future revenue growth

Beyond innovation, resiliency has a compelling correlation with growth.

We asked respondents to forecast the rate at which they expect their organizations' top-line revenue to change over the next few years.

On average (median), respondents at Prepared organizations expect their companies' revenue to grow at twice the rate of Exposed organizations. The ability of these organizations to eliminate disruption, keep staff productive, and help the organization innovate all play a significant role in enhancing respondents' business optimism.

At what annual rate do you expect your organization to grow (or contract) its top-line revenue over the next few years? (Median annual growth rate)



Prepared organizations forecast that their organization's revenue **will grow at 2x the rate** of Exposed organizations.

How to Become a Cyber-resilient Business

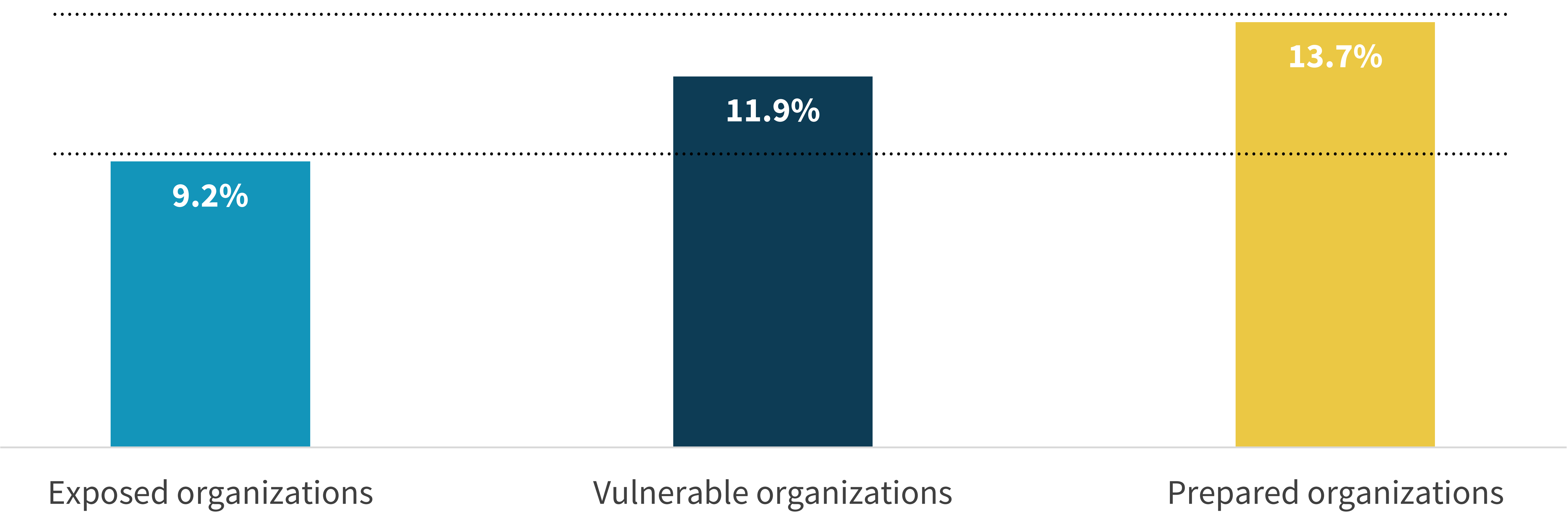
Prepared organizations allocate more of their tech spending to cybersecurity than their peers

We know based on our segmentation criteria that Prepared organizations fund cybersecurity and resiliency technologies at what they feel is an “optimal” level, while Vulnerable and Exposed organizations see room to improve.

But this data in a vacuum is not actionable for IT and security leaders. To go a click deeper, we asked respondents what percentage of their technology spending is allocated to cybersecurity. What we saw is that Prepared organizations spend nearly 14% of their technology budgets on cybersecurity, 49% more than their Exposed peers.

Organizations spending below this threshold should reallocate funding to align with market leaders.

What percentage of your organization’s IT budget is allocated to cybersecurity? (Estimated mean)



On average, Prepared organizations invest

49% more

of their technology budgets in the areas of cybersecurity/resiliency.

Prepared organizations apply more human capital to security and resiliency

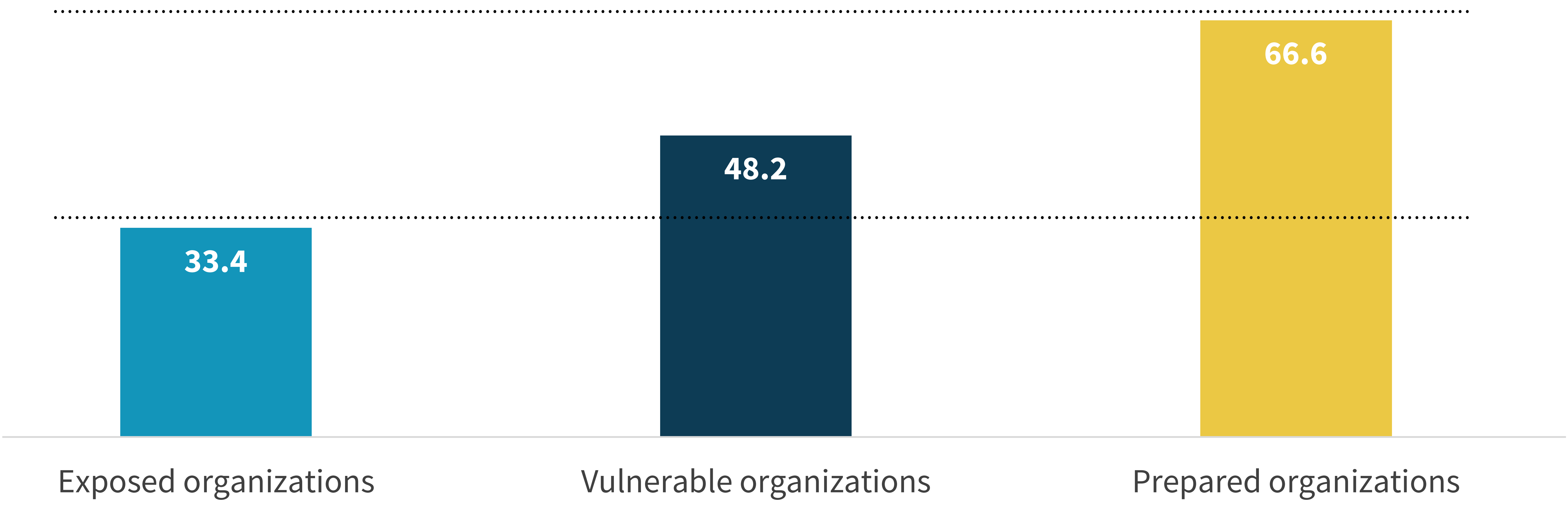
Similar to funding, we know Prepared organizations feel their security teams (inclusive of security-focused IT professionals) are well staffed. However, when we look at the average number of FTEs allocated by resiliency level, we see just how broad the disparity is.

On average, Prepared organizations employ twice as many FTEs in their security teams as Exposed organizations (66.6 FTEs versus 33.4).

Looking at this data by company size helps make this information even more actionable.

- Prepared midmarket and mid-size enterprises (250 to 4,999 employees) employ 62 FTEs versus their Exposed counterparts' 27.7 FTEs.
- Prepared large enterprises (5,000+ employees) employ 76.8 FTEs versus their Exposed counterparts' 47.8 FTEs.

Approximately how many dedicated FTEs are part of your organization's in-house cybersecurity team (inclusive of IT roles focused on cybersecurity)? (Estimated mean)



On average, Prepared organizations employ **twice as many FTEs** in their security team.

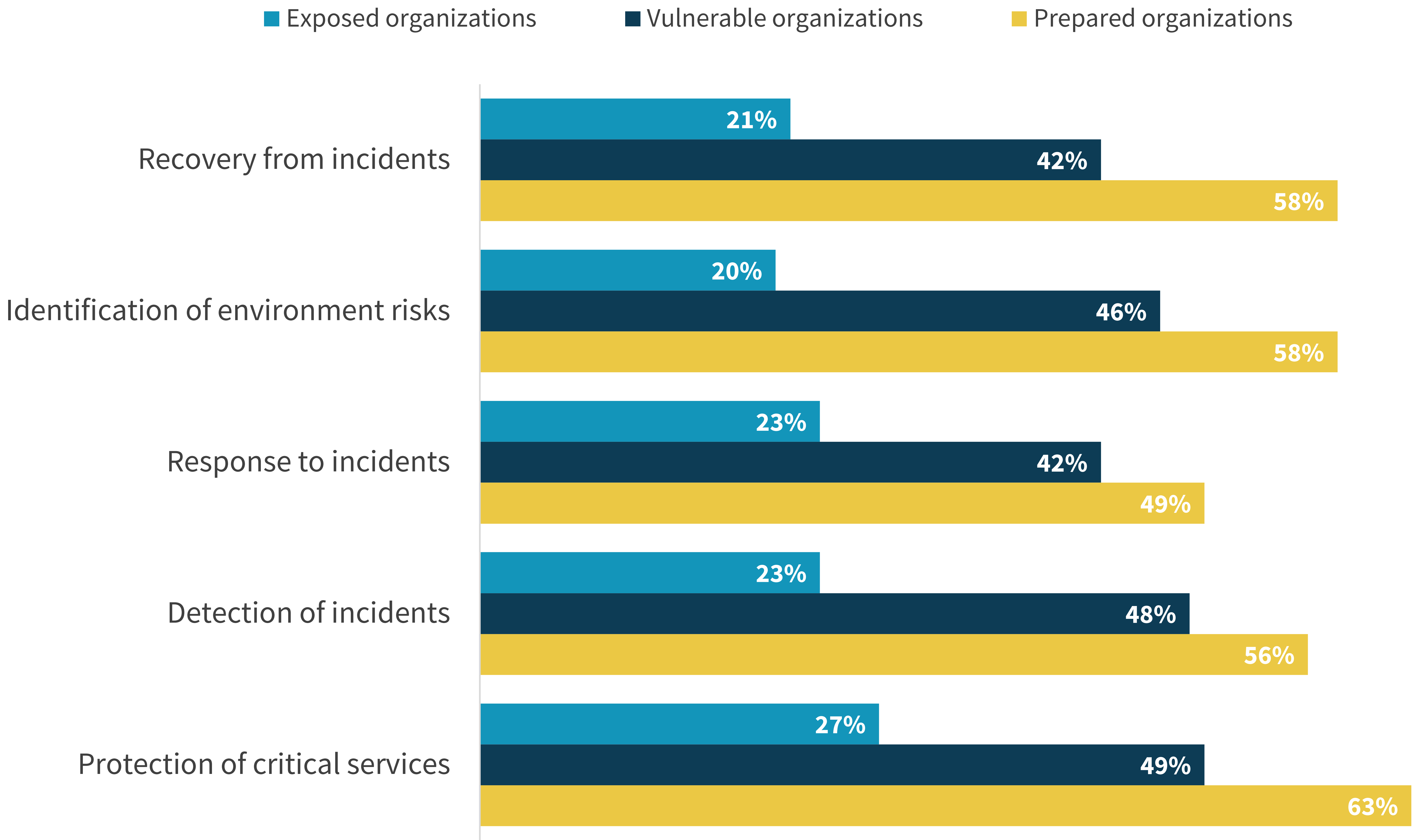
Prepared organizations have been ramping investments across the risk lifecycle

The survey asked respondents to think of their investments across the risk lifecycle (as defined by the NIST CSF), from identifying risks all the way through to recovering from incidents.

The common theme? Prepared organizations are much more likely than their peers to have increased investment in all areas by more than 15% year-over-year.

This behavior underscores the criticality of a defense-in-depth risk posture that gives organizations the resources to mitigate risk at every step.

In which of the following risk mitigation areas has your organization's level of new investment over the last 12-24 months exceeded 15% year-over-year? (Percent of respondents)



Back to Contents

Prepared organizations harden their environment with intrinsically secure technologies

This eBook focuses on the concept of organizational resilience and associated results at a high level. The research further delved into aspects of organizations' environments from storage, to servers, to client devices.

In each area, Prepared organizations lead the market in terms of their adoption of technologies with intrinsic security features and drive superior performance from less downtime, fewer instances of downtime, to less frequent device corruption.

Prepared organizations reduce outages and data loss in their storage environment with storage solutions with intrinsic data protection capabilities.

READ THE BRIEF

Prepared organizations promote innovation with intelligent security automation in their compute environment.

READ THE BRIEF

Prepared organizations reduce device corruptions and limit data loss with client technologies with intrinsic security capabilities leading to compelling employee experience outcomes.

READ THE BRIEF

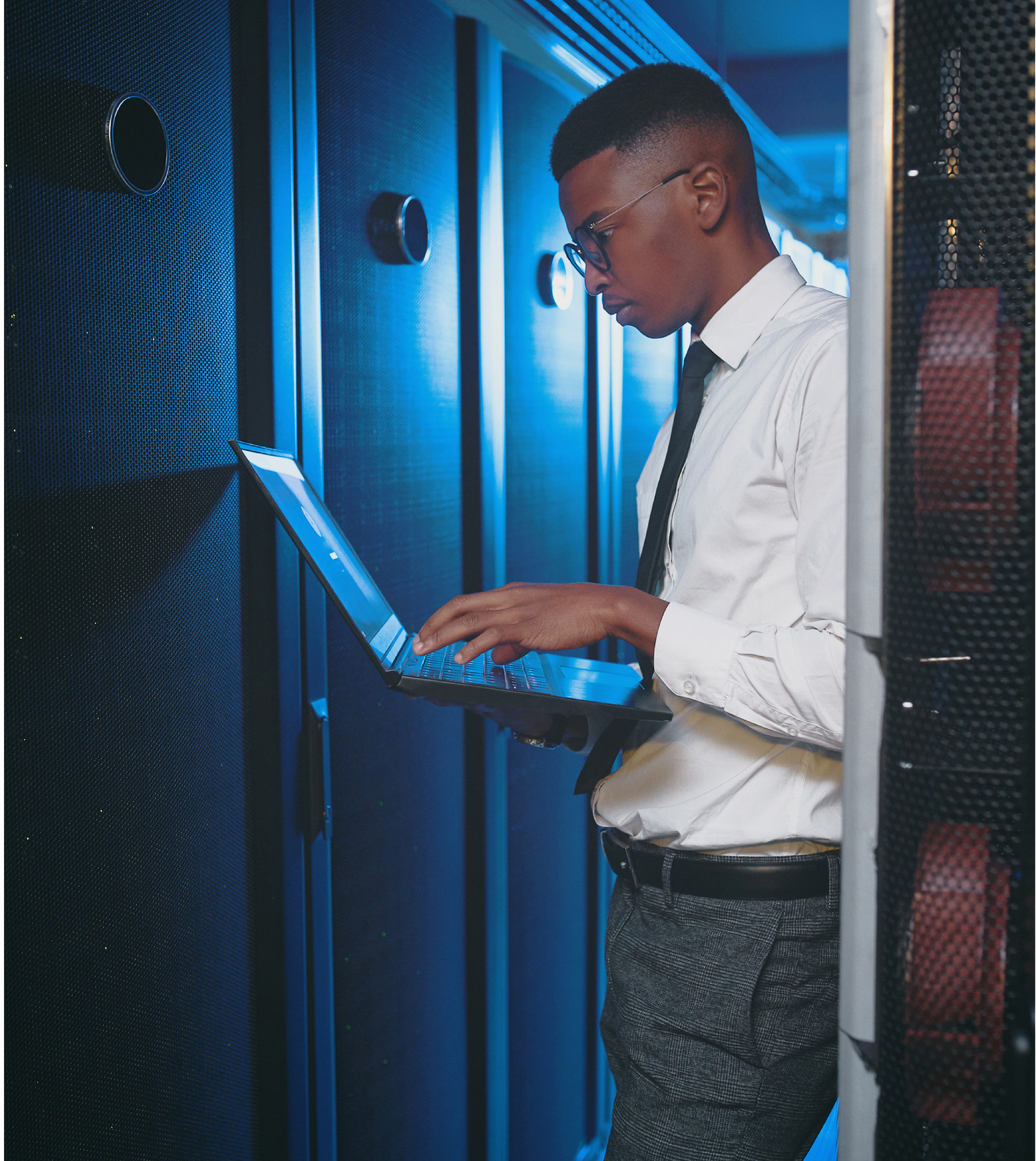
Prepared organizations prioritize the adoption of technology solutions with intrinsic security. Learn more about this concept and find out why.

READ THE BRIEF

Conclusion

Whether due to their ability to keep end-users productive, respond to security incidents with speed, or free up technical teams to advance critical IT transformation initiatives, prepared organizations provide a compelling, data-driven, argument to all organizations to strive to reach a highly resilient status. Depending on where your organization is today, this journey may seem daunting, but this research can help build the business case.

How Dell Technologies can help



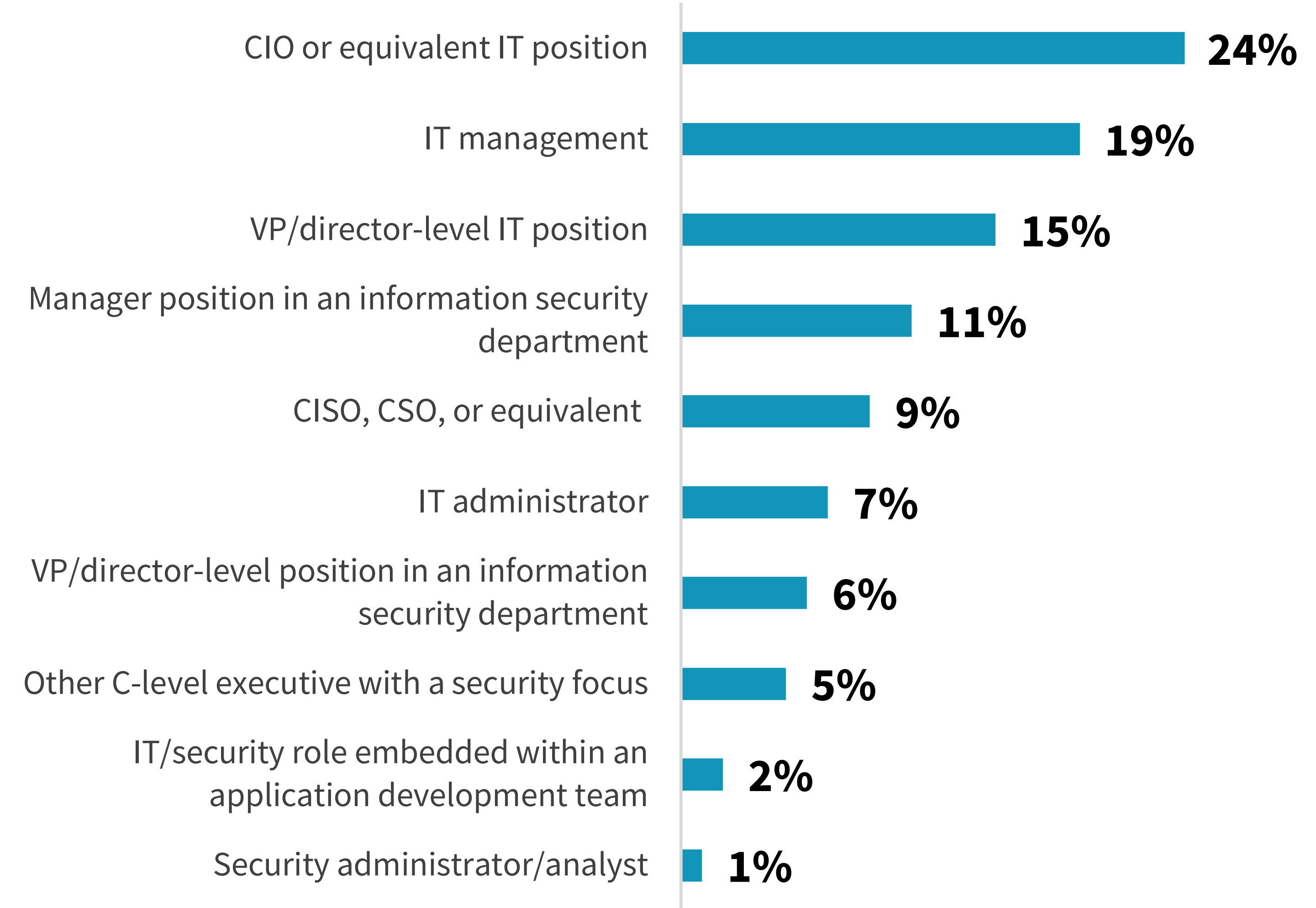
Demographics

The data in this report was derived from a survey fielded between January 11 and February 7, 2022. These figures detail the demographics of respondents to the survey located in North America (N=187), Western Europe (N=185), APAC (N=179), and LATAM (N=199).

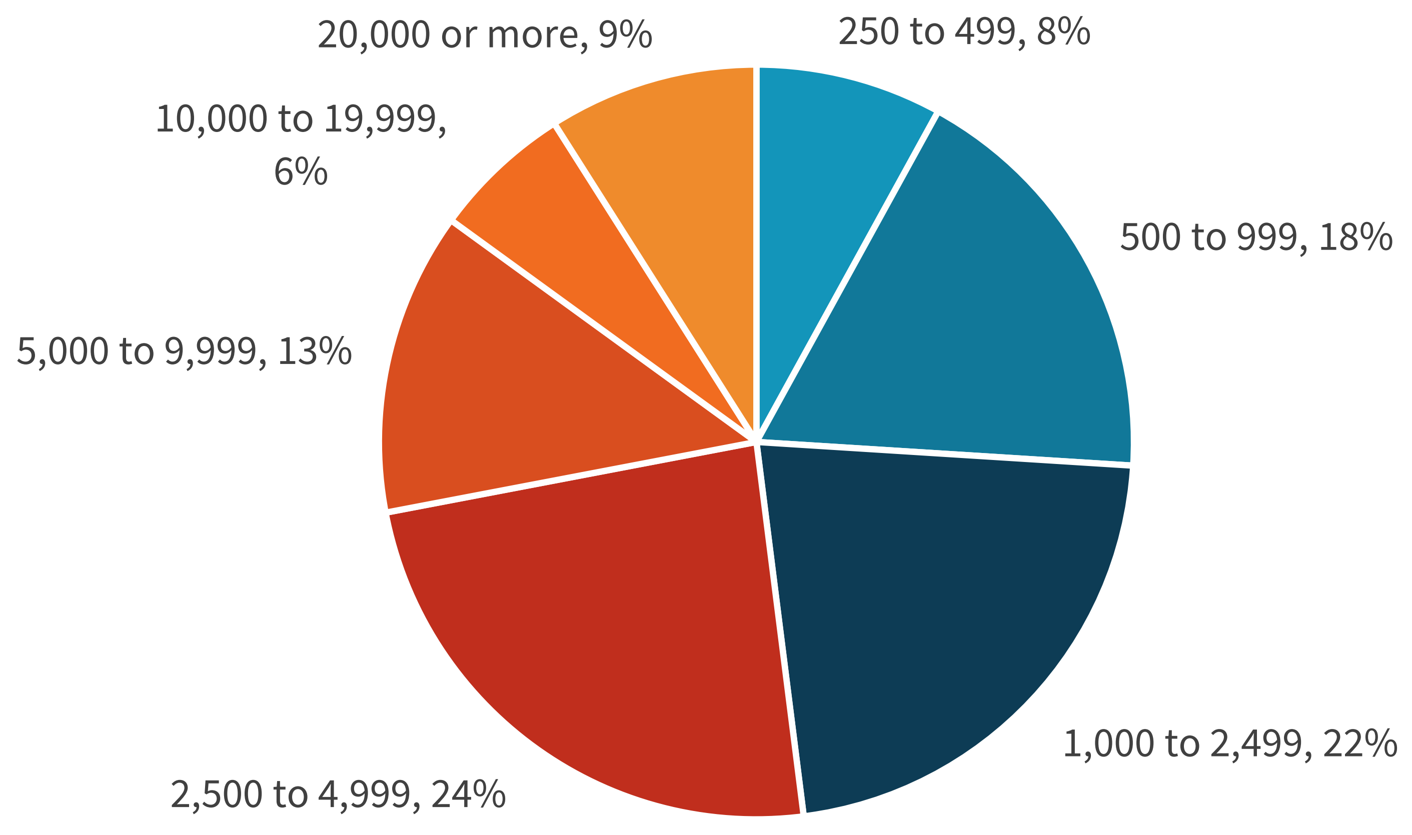
Totals in figures and tables throughout this report may not add up to 100% due to rounding.

The margin of error for a sample size of 750 at the 95% confidence level is + or - 4 percentage points.

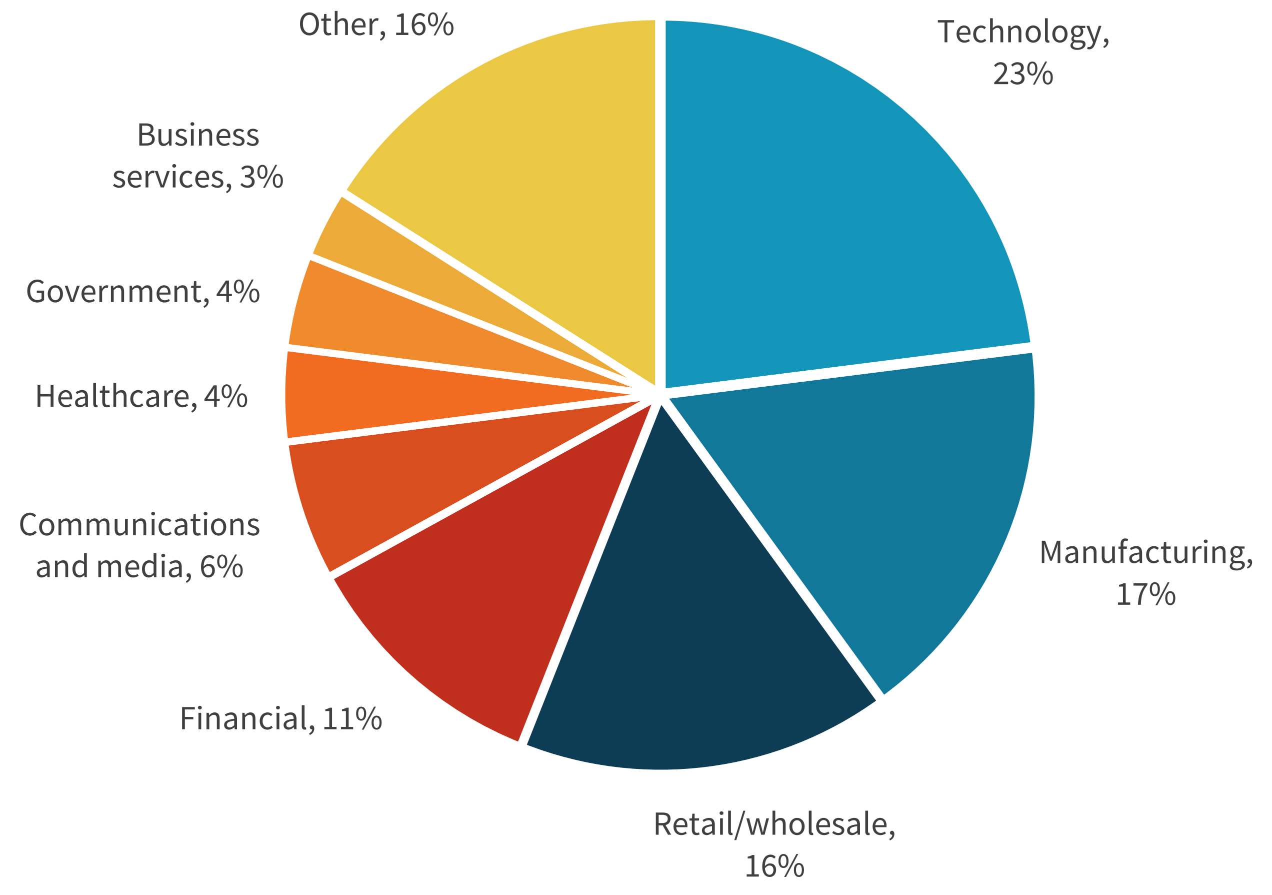
RESPONDENTS BY JOB TITLE



RESPONDENTS BY COMPANY SIZE



RESPONDENTS BY INDUSTRY



About Dell Technologies, Intel, and VMware

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.

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.

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.

a division of TechTarget

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