Enterprise Strategy Group™
by TechTarget

Preparedness Gap:
Why Cyber-recovery Demands a Different Approach From Disaster Recovery

Adam DeMattia | Senior Director, Custom Research
Dave Gruber | Principal Analyst, Ransomware, SecOps Services
ENTERPRISE STRATEGY GROUP

DECEMBER 2024

This Enterprise Strategy Group eBook was commissioned by Commvault and is distributed under license from TechTarget, Inc.

Contents

“Disruption of IT services has **a direct and measurable affect** on the success of operational objectives.”

Adam DeMattia
Senior Director, Custom Research
ENTERPRISE STRATEGY GROUP

Introduction

Organizations of all sizes, types, and industries are leveraging technology throughout their infrastructure to power virtually every aspect of their operations. For most, disruption of IT services has a direct and measurable effect on the success of operational objectives, putting technology and cyber resilience in the spotlight. Business continuity IT strategies are, therefore, paramount to achieving operating objectives.

> "**A new level** of cyber-recovery planning and preparation is needed."

While traditional disaster recovery (DR) planning and preparation is well established for many, it often fails to support the level and complexity of disruption that is commonly occurring from modern cyberattacks. Therefore, a new level of cyber-recovery (CR) planning and preparation is needed, one that prepares for the unknown in terms of scope, impact, and scale.

How Cyber-recovery Differs From Disaster Recovery

Cyber resilience, CR, and DR are interconnected components of an organization's overall strategy to mitigate and respond to digital threats. Cyber resilience focuses on the ability to prepare for, respond to, and recover from cyberattacks, emphasizing business continuity and the protection of critical assets. It's about building robust systems and processes that can withstand and adapt to cyberthreats.

CR, a subset of cyber resilience, specifically deals with the processes and technologies used to restore systems and data after a cyberattack. This includes backup and restoration strategies, incident response plans, and methods to minimize data loss and downtime.

DR, on the other hand, is a broader term that encompasses the strategies and plans for resuming normal operations after any type of disaster, whether it's a cyberattack, natural disaster, or other disruptive events. It involves maintaining or quickly resuming mission-critical functions following a disruption.

For most, CR requires different processes, people, and technology investments and readiness from traditional DR. While DR has many variables, CR is variable when it comes to understanding the scope, impact, and depth of disruption involved. CR mechanisms themselves are also at risk, as attack strategies often go after recovery infrastructure, making it even more difficult to get back to business.

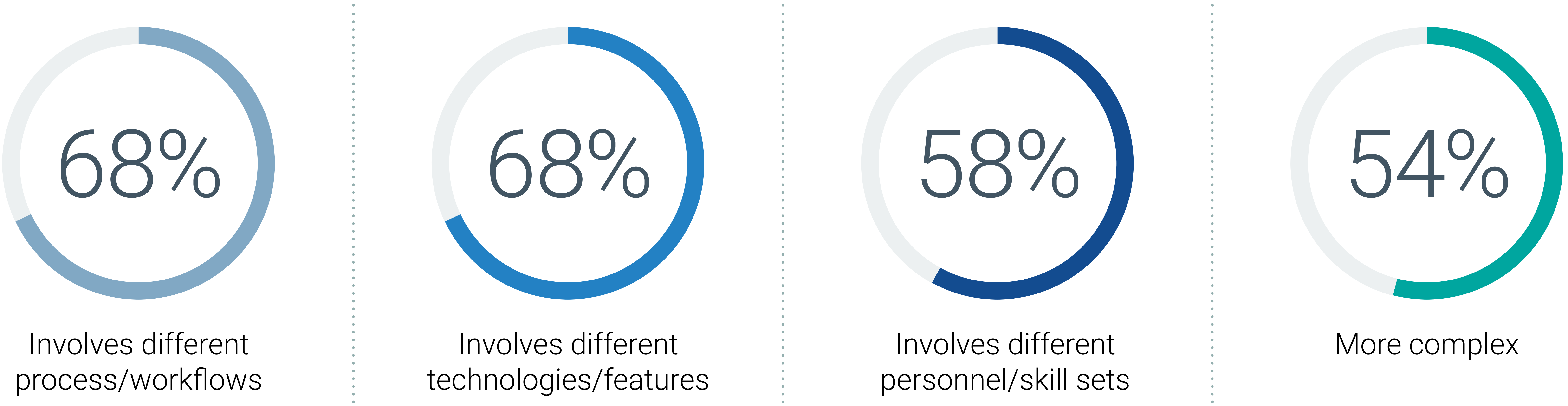
And while DR is focused on recovering from the fallout of an inadvertent event, cyberattacks are often criminally motivated, therefore requiring involvement of law enforcement, the legal system, and other risk-related and defensive tactics. The net result is often a more complex, time-consuming recovery cycle.

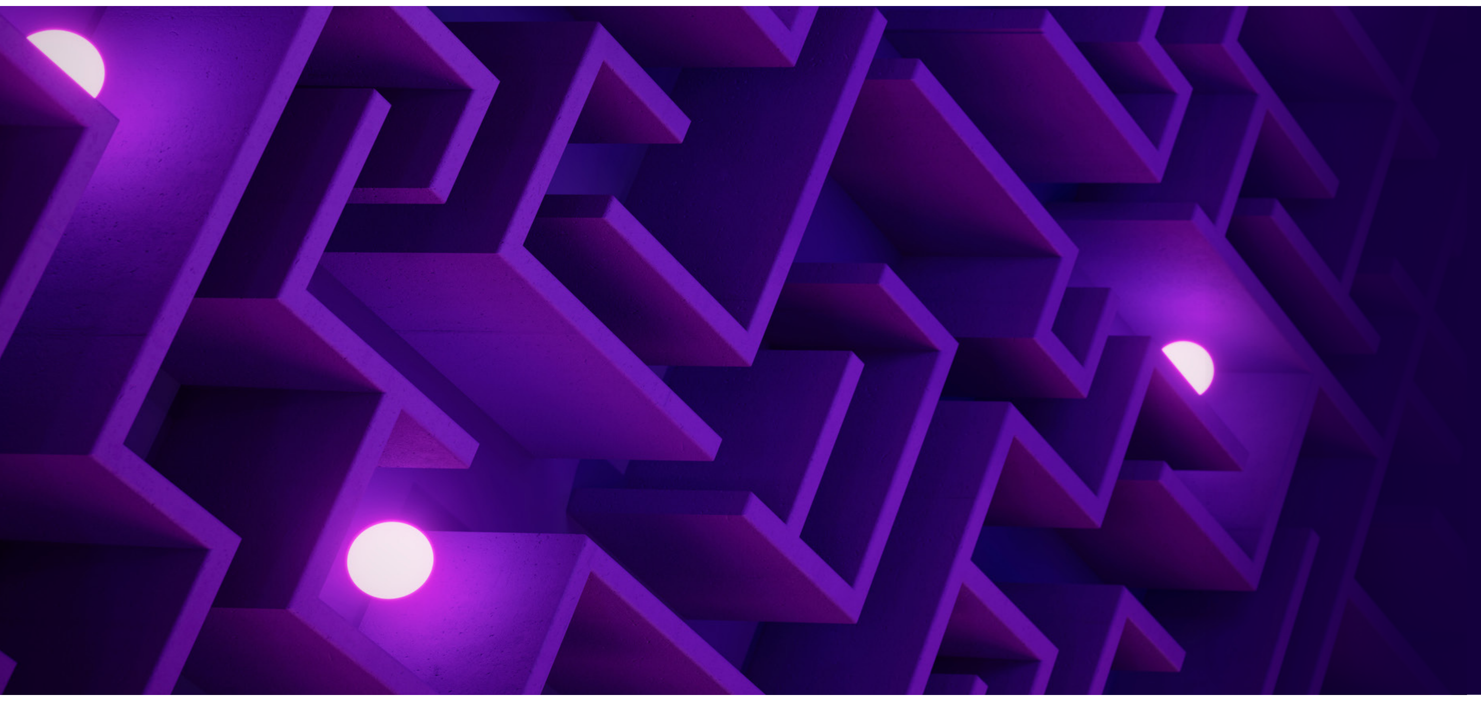
In essence, CR is a crucial part of both cyber resilience and DR, focusing specifically on the technical aspects of restoring digital assets. Together, these three concepts form a comprehensive approach to ensuring an organization's longevity and stability in the face of various threats.

How CR and DR Differ

While CR shares many of the characteristics of more traditional DR, IT and security leaders report that cyberevents are typically more complex than a traditional outage or disaster, requiring different processes and workflows, different technologies and features, and different personnel and skill sets for response and recovery.

Recovering From a Cyberevent Is Different From Traditional Outages.

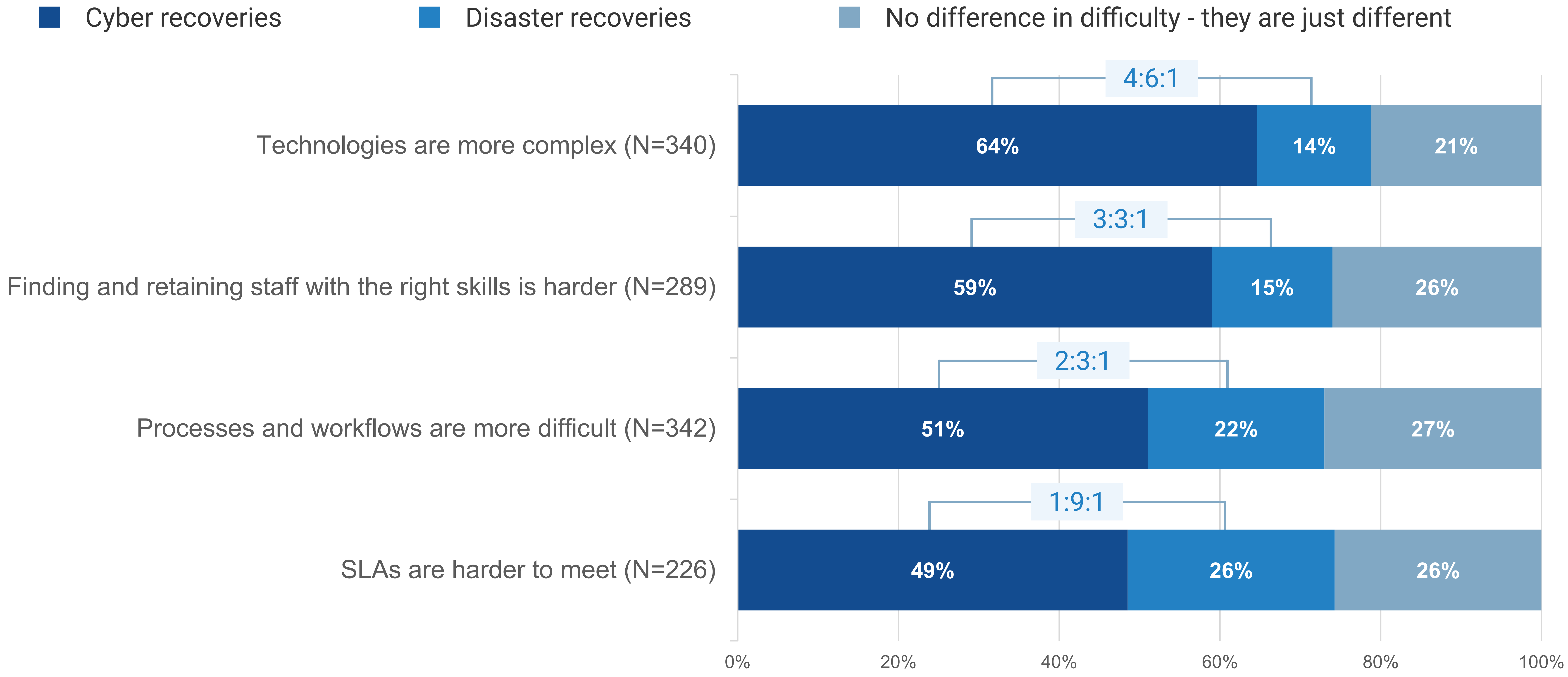




CR Is Seen as More Problematic and Stringent in Regard to Technologies, Staffing, Processes, and SLAs

Across the board, CR is seen as more difficult and complex than traditional DR, with nearly half of respondents reporting that CR service-level agreements (SLAs) are harder to meet.

How Much More Difficult Is CR?



4.6x more respondents said CR technologies are more complex.

3.3x more said finding and retaining staff with the right CR skills is harder.

2.3x more said CR processes and workflows are more difficult.

BACK TO CONTENTS

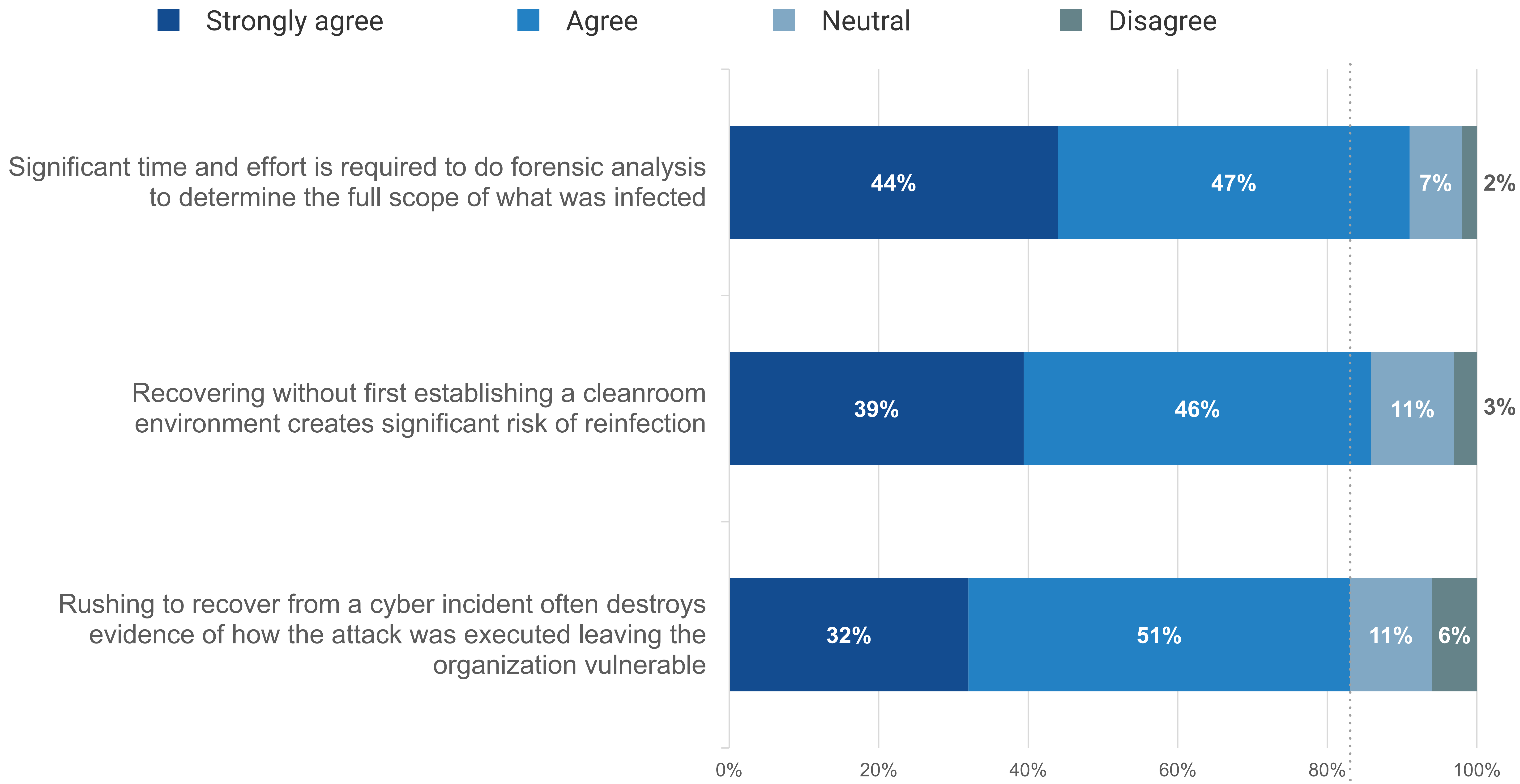
Why Is CR So Much More Challenging Than Traditional DR?

More than four out of five respondents agree that there are complexities specific to CR that, when handled incorrectly, create significant risk. The complexity begins with spending significant time and effort on forensic analysis to determine the full scope of what was infected from the attack. Without this critical information, recovery teams don't know where to focus to contain and recover from the attack. (91%)

And once the scope of an attack is understood, work is needed to establish a "cleanroom" environment to begin the recovery process. Starting the recovery without first establishing this clean room creates significant risk of reinfection for most organizations. (85%)

Careful attention to preserving evidence required to understand how the attack was executed adds more time and complexity during the response process. Rushing ahead to recover can inadvertently destroy key evidence, leaving an organization vulnerable to further attack and damages. (83%)

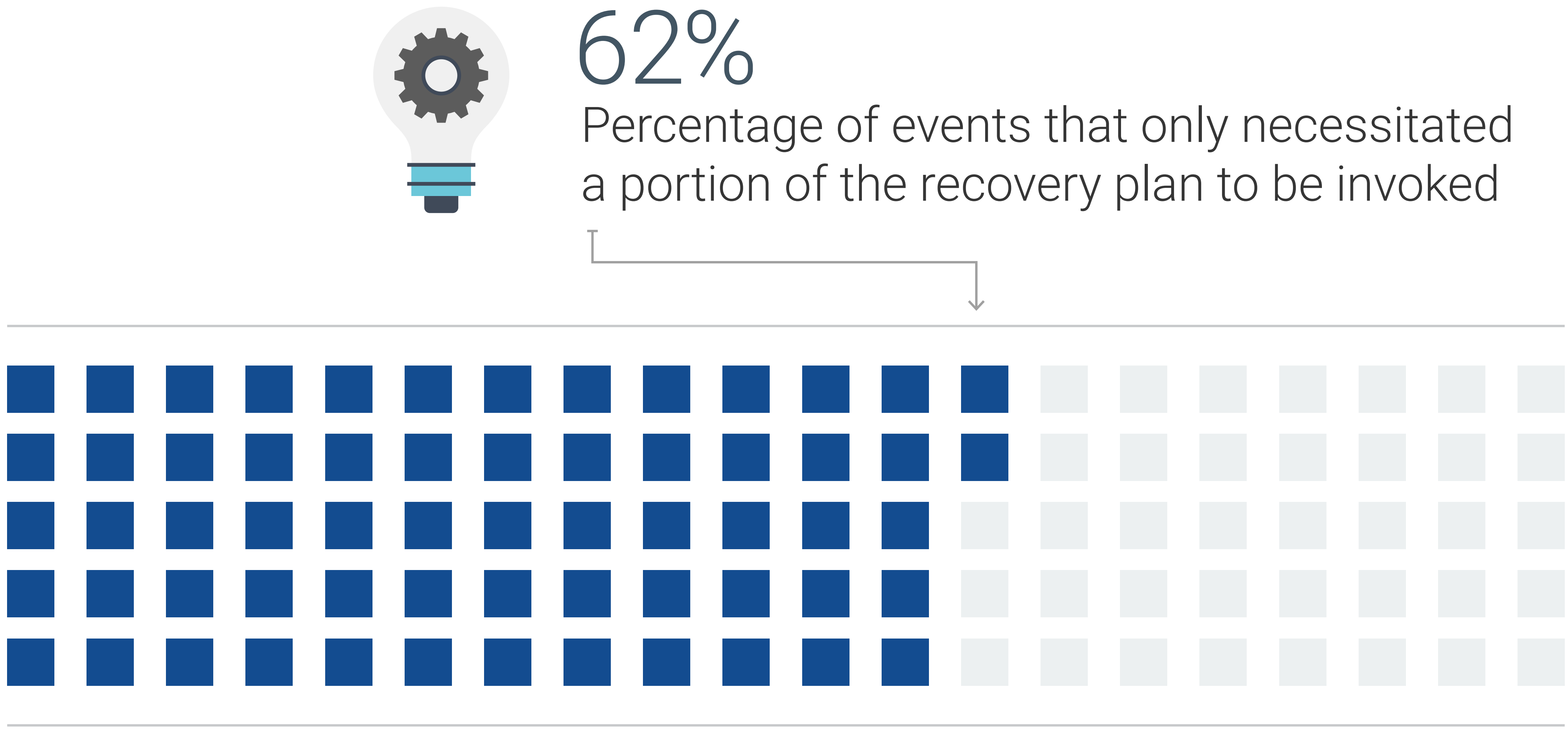
Why CR Is More Challenging Than Traditional DR.

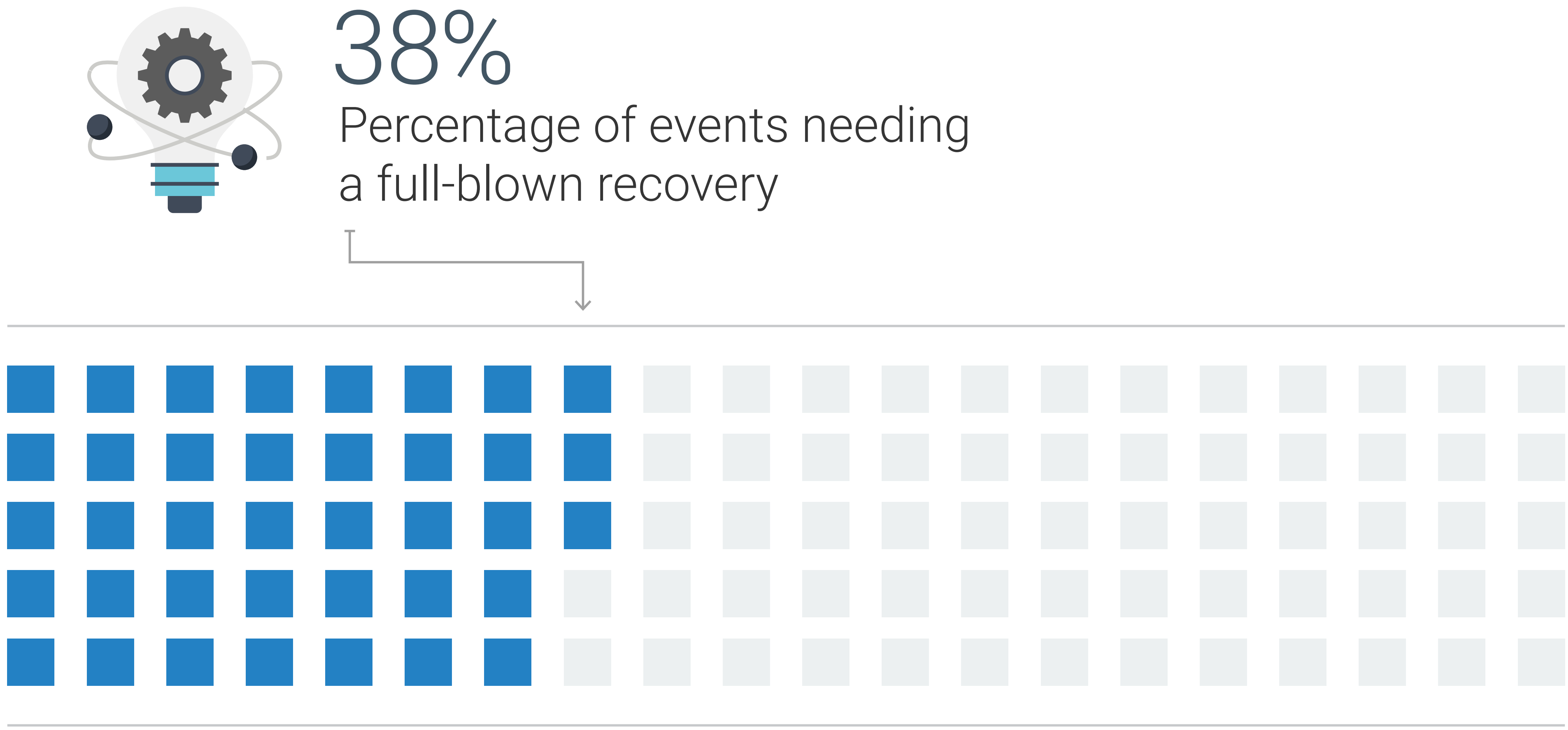


CR Actions Vary Based on the Scope and Scale of the Attack

Respondents reported that fewer than half (38%) of events necessitated a full cyber-recovery effort. That said, in many cases, determining and implementing a partial recovery increases the amount of customization and planning required before recovery tasks can begin. Regardless of whether the recovery is full or partial, the same level of preparedness activity is required, highlighting the complexity of cyberevents.

Cyber-recovery Needs: Full vs. Partial.



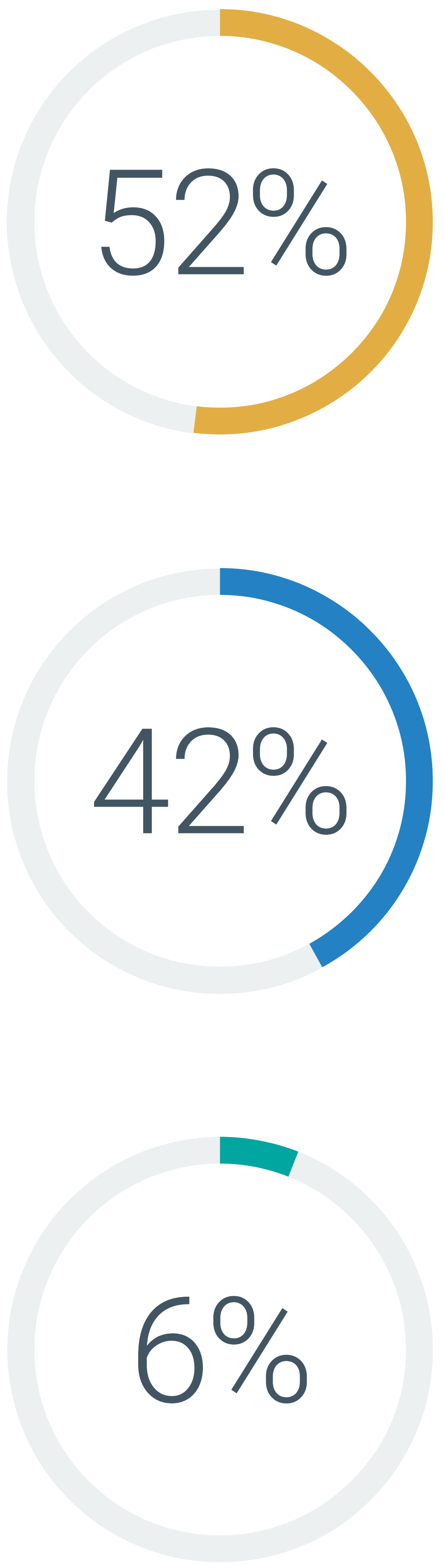


> “Despite differences and additional complexity, more than half (52%) of organizations **include CR planning as a part of their broader DR program. ”**

CR and DR: Separate or Components of a Combined Program?

Despite differences and additional complexity, more than half (52%) of organizations include CR planning as a part of their broader DR program. And even when planned and managed separately, most organizations report a high degree of alignment between CR and DR.

How CR and DR Programs Are Aligned.



52%: Our CR plan **is a part of our broader** DR program

42%: Our CR plan and DR plan are **separate, but there is a high degree of consistency** in processes and protocols

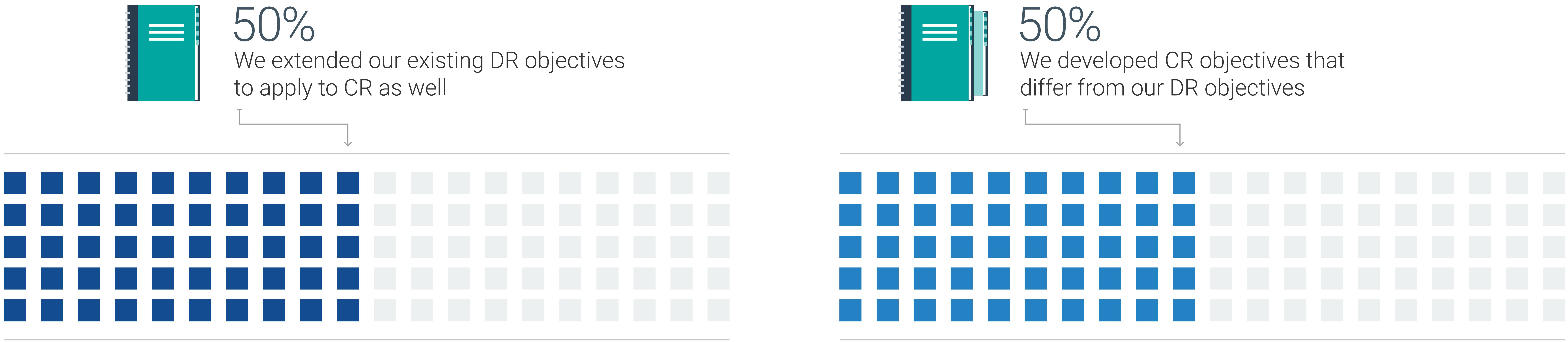
6%: Our CR plan and DR plan are **separate and there is a high degree of variability** in their processes and protocols

BACK TO CONTENTS

The Market Is Split in Terms of How to Develop CR SLAs

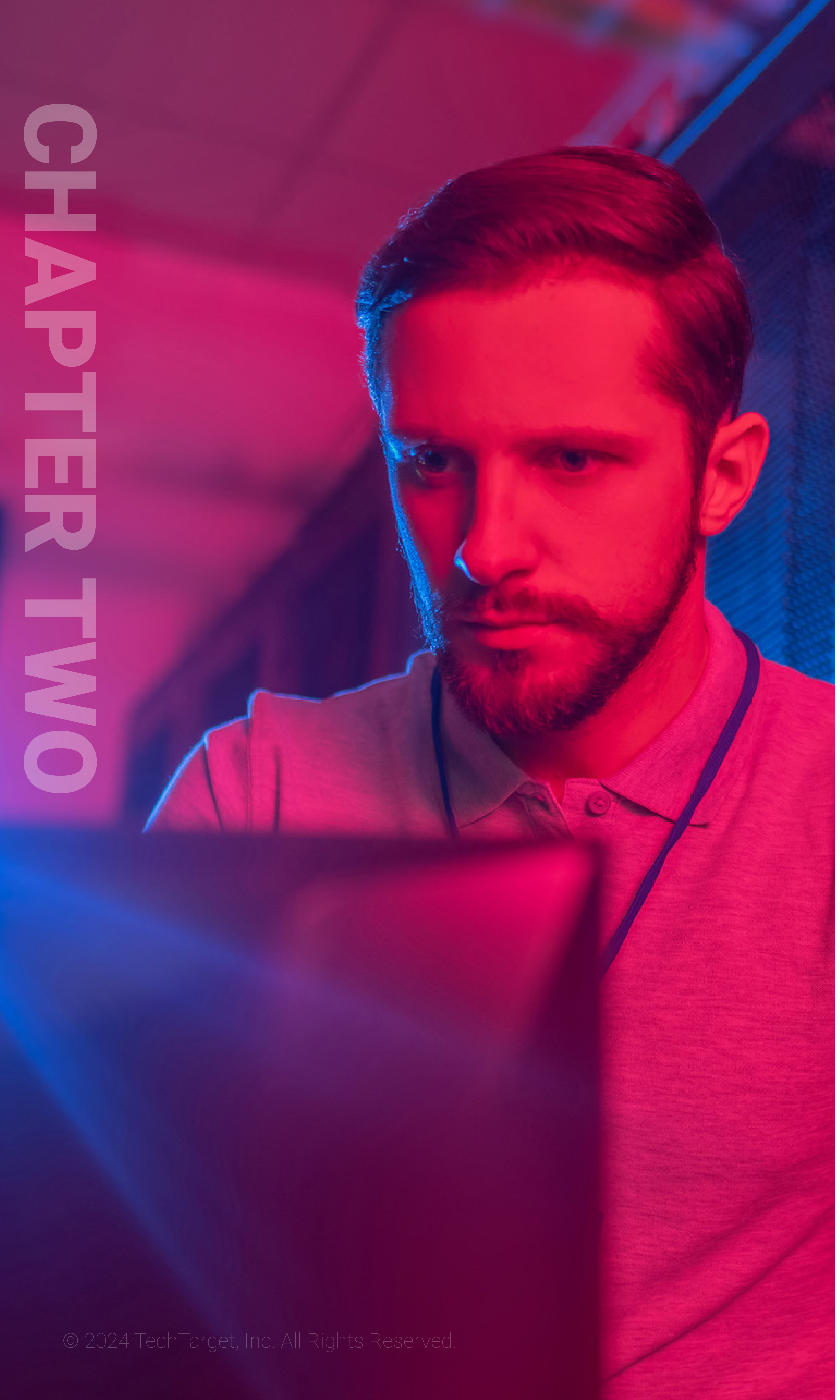
Similarly, when it comes to specific recovery-time objectives (RTOs) and recovery-point objectives (RPOs) aligned to DR versus CR, the market is split 50/50 on how to develop SLAs. There are exceptions, with financial services (59%), retail (70%), and healthcare (66%) extending SLAs for CR.

The Relationship Between CR and DR Objectives.



50%
We extended our existing DR objectives to apply to CR as well

50%
We developed CR objectives that differ from our DR objectives



CHAPTER TWO

> “The ramifications of a successful attack can **significantly hamper operational processes and cause impacts to the internal and external supply chain**, affecting employees and customers.”

Recovery Strategies

How Organizations Are Reacting to the Unique Issues Presented by CR Requirements

Recovering from a cyberincident requires recovery of all facets of the operating environment, including systems, infrastructure, and data. Attackers employ many different techniques and targets to motivate payment, resulting in various impacts, with potentially profound repercussions for the victim organizations. While it’s not surprising that more than half of organizations have cited data exposure (53%) and/or loss (51%) as effects of ransomware, the ramifications of a successful attack can significantly hamper operational processes and cause impacts to the internal and external supply chain, affecting employees and customers. These impacts are just too deep and broad to be ignored.[1] Data or access to it is the prize, and extortion or damage (e.g., encrypting it to bring the business to a halt) is in play.

[1] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023

BACK TO CONTENTS

Backups Are a High-value Target for Attackers

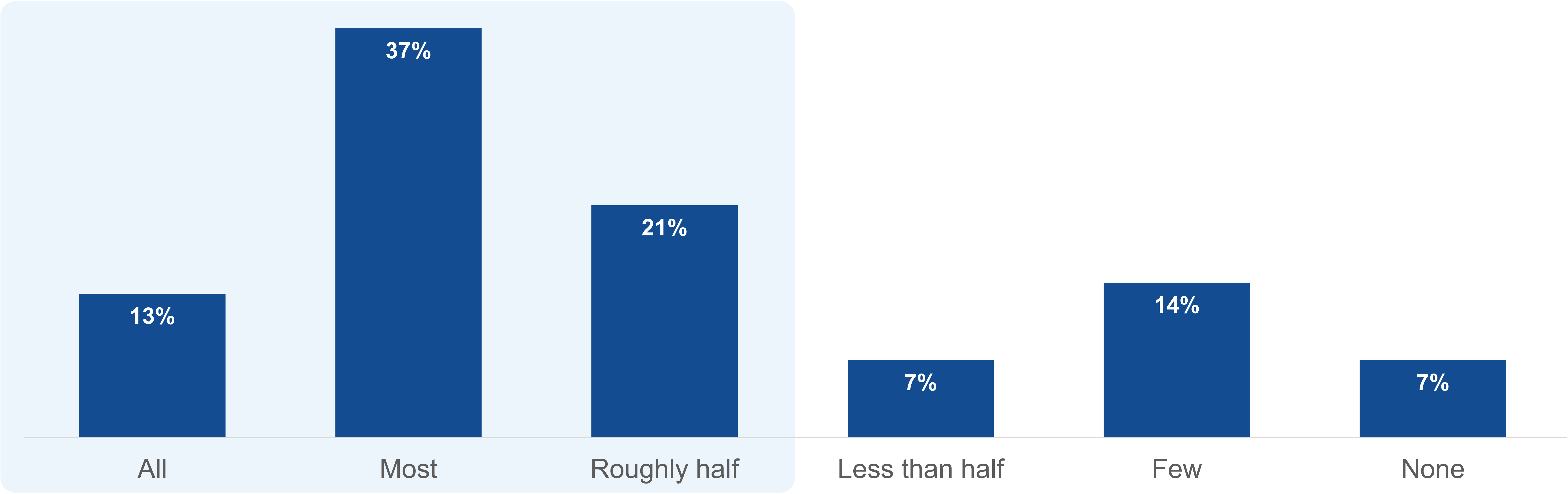
As cybercriminals target sensitive and potentially saleable data, data protection and recovery capabilities have become key cyber-resilience requirements.

Data backups are more than a means to recover from attacks on data used by applications and infrastructure; they've become a key target in the context of disabling or delaying recovery capabilities. Ransomware payouts are often motivated by RTOs: When attackers corrupt backups, they force longer recovery times, which often lead to ransom payments.

Prevention Extends to Data Protection Infrastructure

As organizations become aware of the vulnerabilities in their data protection processes for backup and recovery, many are taking extra precautions to safeguard their backup copies, which are crucial for recovery in case of a crisis.

Percent of Attacks Explicitly Targeting Backup Data.



> "Of respondents, 92% said they've **suffered from attacks explicitly targeting backups**, and 71% said those kinds of attacks accounted for **half or more of all attacks."**

The Vast Majority of Organizations Are Taking Action to Protect Backup Copies from Attackers

While 88% reported that extra measures are taken to protect all or most backup copies, this data might underestimate actual efforts, as both cybersecurity respondents (52%) and middle managers closer to the infrastructure (52%) more often reported extra measures are taken to protect *all* backup copies.

Steps Organizations Take to Protect Backup Copies.

52%

We take extra measures to protect all of our backup copies

38%

We take extra measures to protect most of our backup copies

6%

We take extra measures to protect some of our backup copies

3%

We only take extra measures to protect select backup copies (e.g., mission-critical data backup copies)

0%

We don't take any extra measures

> “Without tangible metrics that show **how and where investments make a difference**, establishing a case for specific investments can be challenging.”

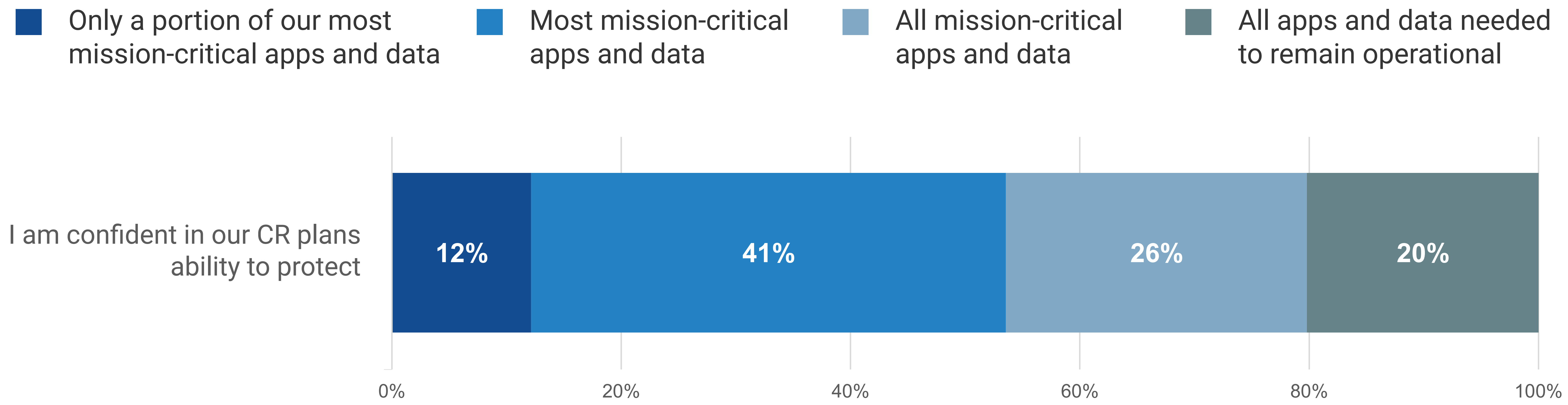
Cyber Resilience: More Needs to Be Done

IT and security leaders are investing in strengthening their preparedness to recover from cyberincidents; most agree that recovery of all facets of the operating environment—including systems, infrastructure, and data—is necessary. Without tangible metrics that show how and where investments make a difference, establishing a case for specific investments can be challenging. Focusing on the most critical components of the operating infrastructure often gets the most support, but secondary components within the operating environment are often linked to more visible infrastructure. Careful understanding and planning is, therefore, needed to prioritize a path to resilience.

More Work Is Needed to Strengthen CR

Only 26% are confident in their ability to protect all mission-critical applications and data. This alarming statistic demonstrates how much work is needed to achieve effective levels of cyber resilience.

How Much of the Environment Can Be Confidently Recovered?

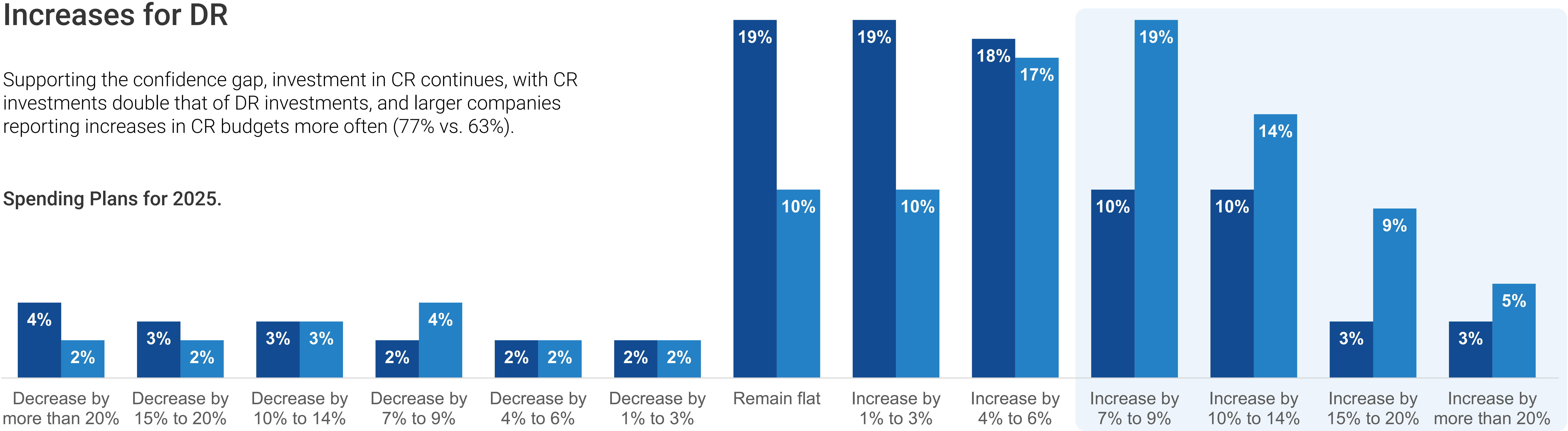


> "Only 26% are confident in their ability to protect **all mission-critical applications and data.**"

Budget Increases for CR Will Far Outstrip Increases for DR

Supporting the confidence gap, investment in CR continues, with CR investments double that of DR investments, and larger companies reporting increases in CR budgets more often (77% vs. 63%).

Spending Plans for 2025.

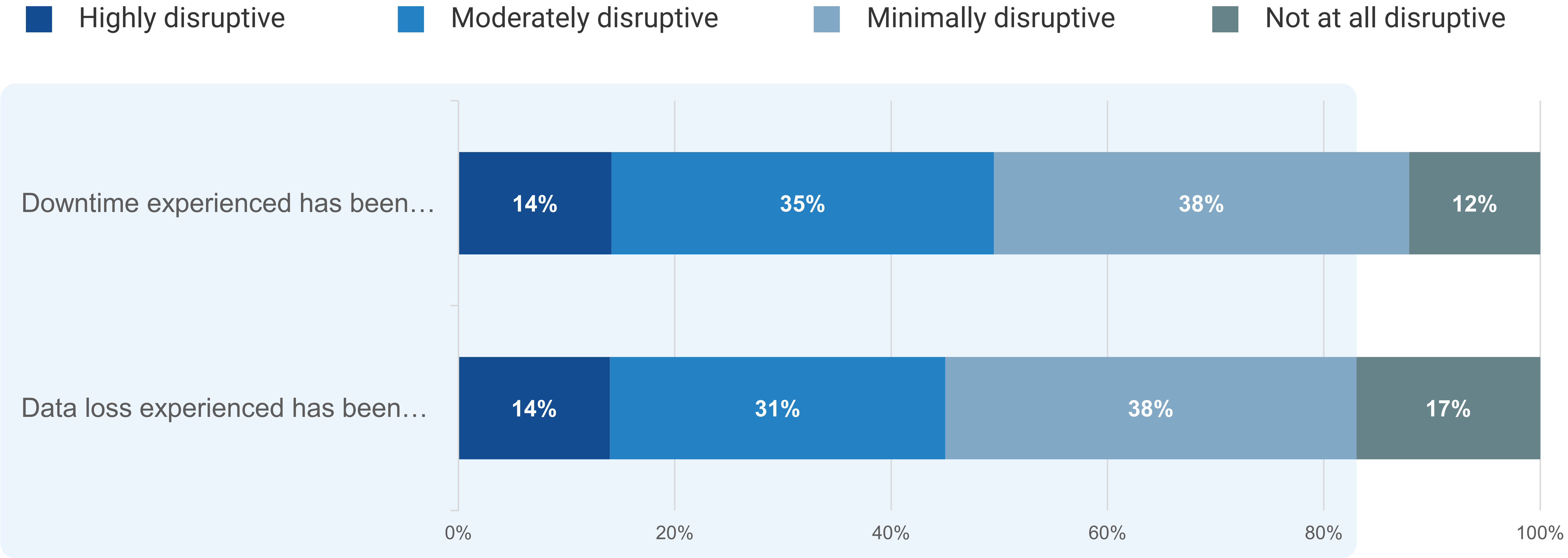


BACK TO CONTENTS

How Successful Are CR Actions? Quantitative and Qualitative Measures of CR Success

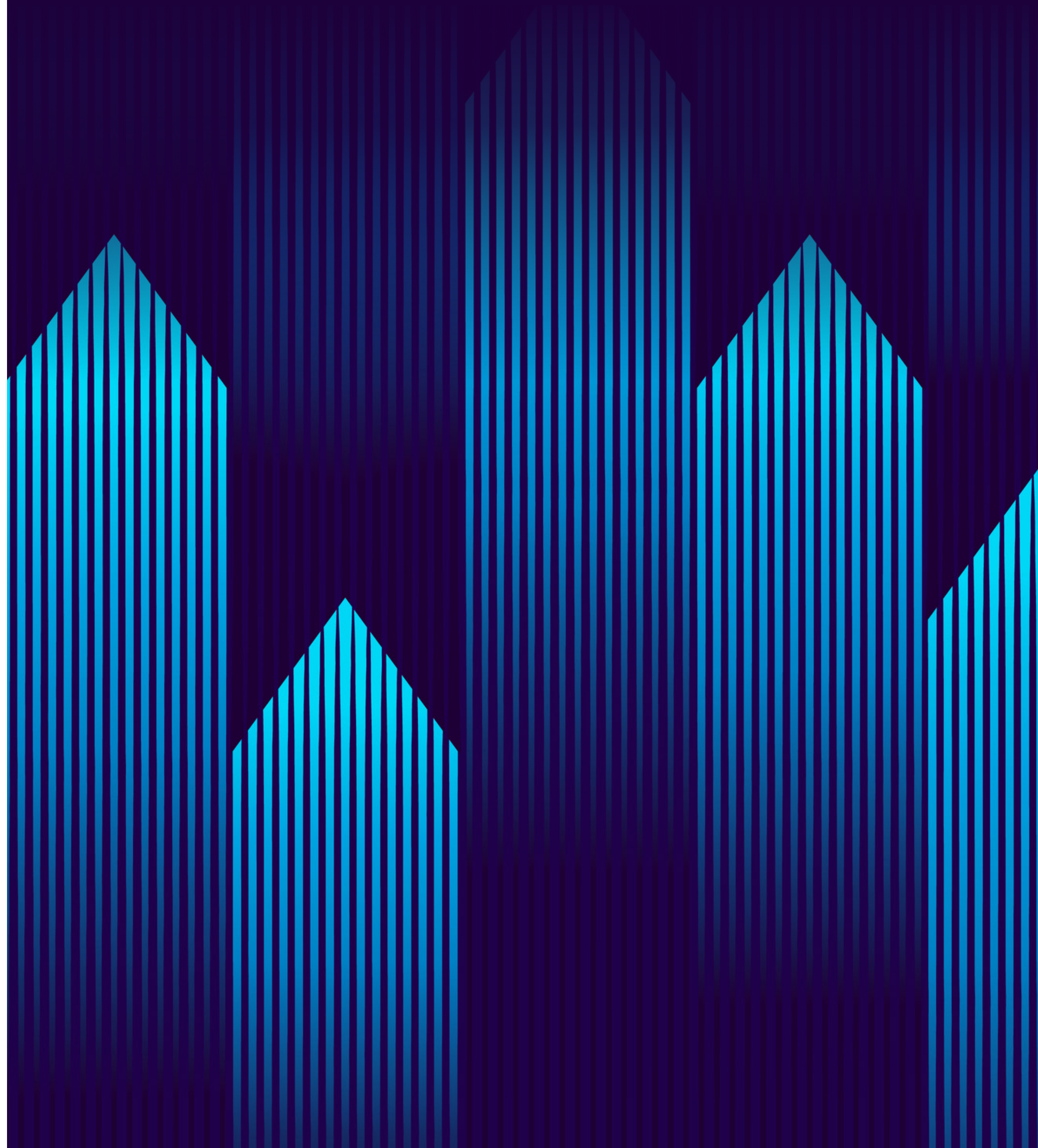
While most CR efforts are deemed successful in terms of meeting SLAs, almost half say either downtime (49%) or data loss (45%) associated with attacks has been disruptive. This begs the question: How are organizations measuring the concept of "successful CR"? Risk-tolerance levels vary, so while one organization's success might mean 100% data recovery within a short timeframe, another organization might measure success based on lower targets for both recovery and timeframe.

Business Disruption Ratings for Cyberattacks Within the Last 12 Months.



75%

Percentage of **fully successful** CR in the past 12 months.

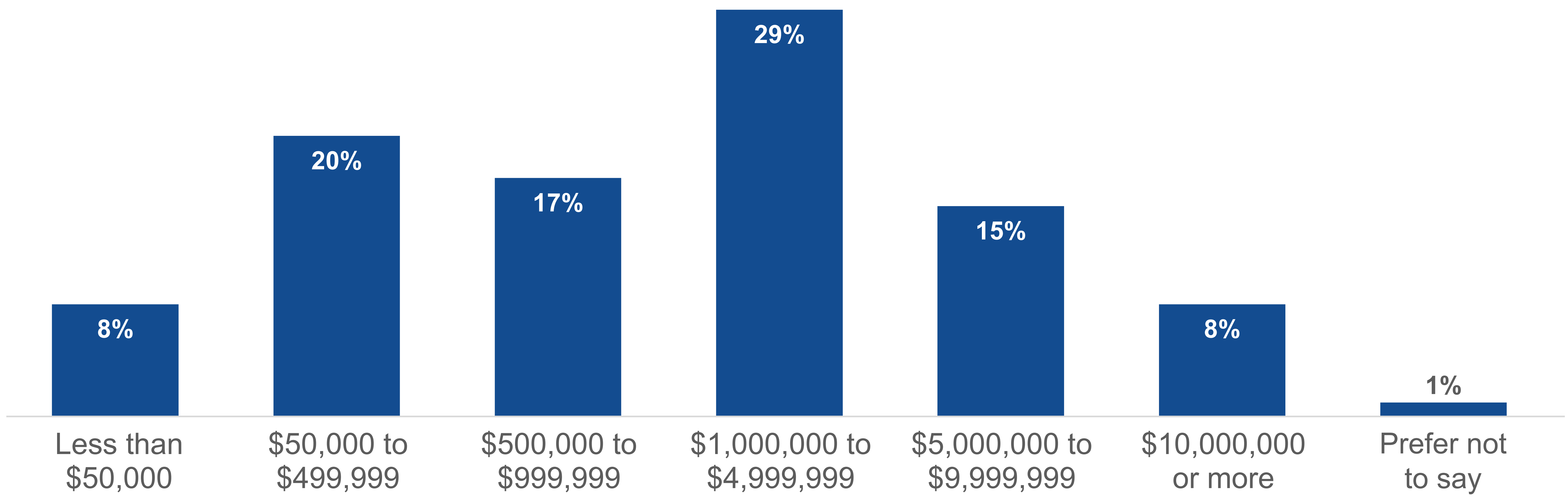


More Is At Stake

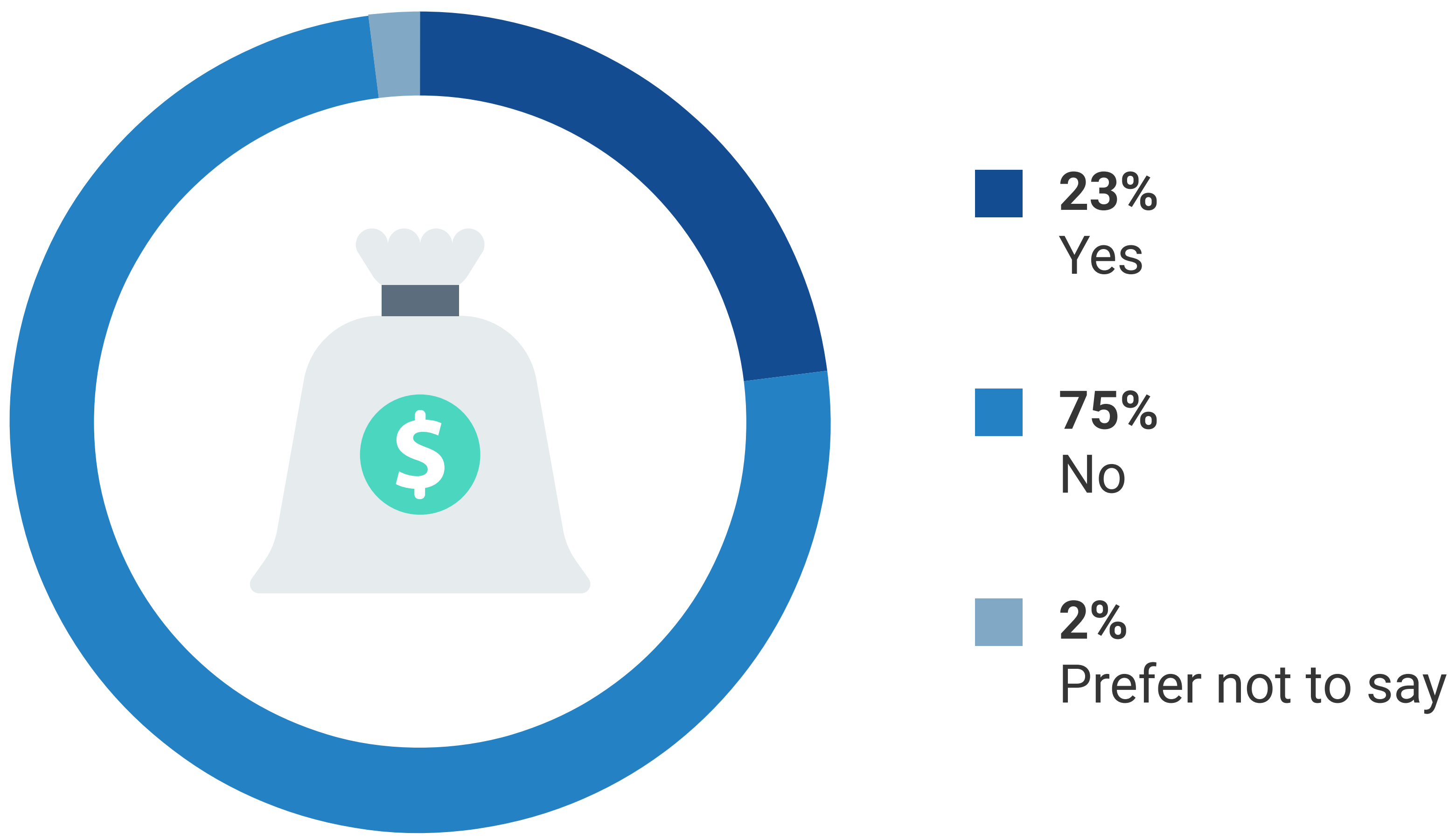
Beyond downtime and data loss, cyberattacks cause far-reaching additional impacts. Reputational damage, customer loss, hard-money financial penalties from compliance violations, third-party liability and damages, and other financial losses occur for many. According to our research, almost one-fourth (23%) of organizations made a ransomware payment to bad actors in the past year. The largest ransom payment organizations reported making is approximately $3 million.

Only one in five organizations escaped attacks unscathed… or so they think.

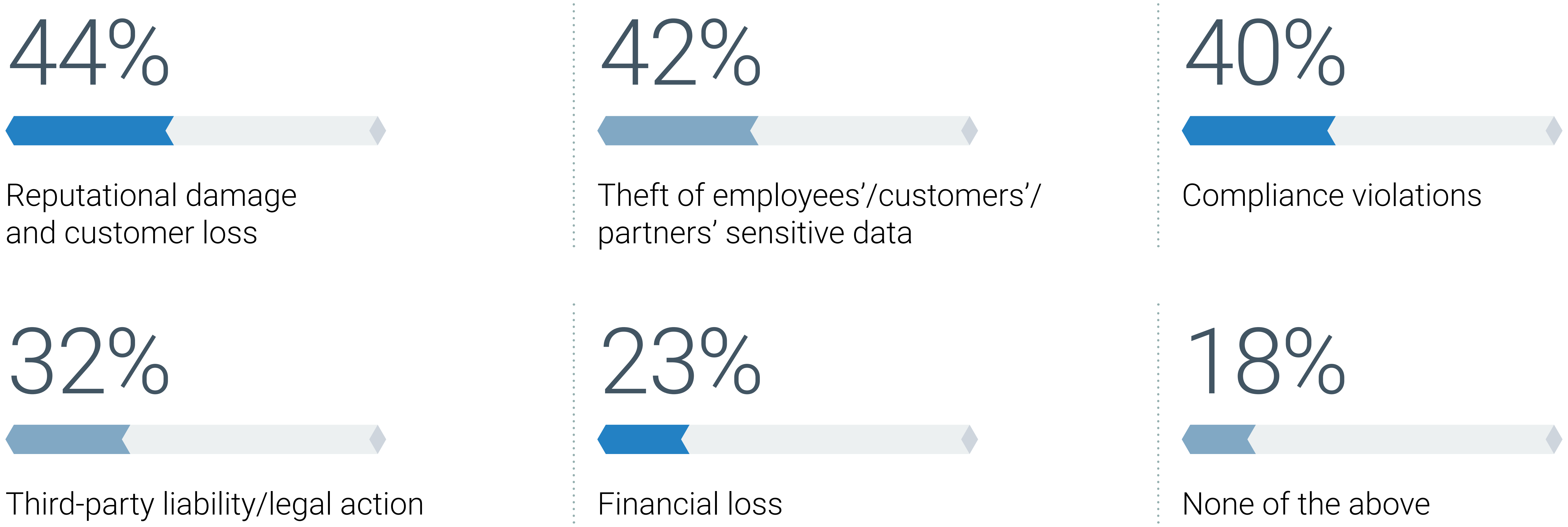
The Largest Ransom Paid in the Past Year.



Propensity to Have Paid a Ransom in the Past Year.



Types of Business Impact, Aside From Data Loss and Downtime, Caused by Cyberattacks.



Conclusion

Cyber resilience has become a mainstream objective for IT and security leaders alike. As strategies mature, aligning to core business resilience objectives requires collaboration and alignment between line-of-business leaders and technology leaders. While disaster and recovery strategies are well understood and reasonably well implemented for most, CR strategies continue to be a work in progress, with different and often more-expansive requirements across people, process, and technology.

All facets of the operating infrastructure must be considered, prioritized, and protected to enable continual business and financial risk mitigation. Data resilience is core to achieving these objectives. Data protection vendors such as Commvault can help provide strategy and solutions needed to meet CR requirements.

For more information on how Commvault can help strengthen your disaster and cyber recovery strategy and execution, click the link below.

LEARN MORE

Commvault®

RESEARCH OBJECTIVES

Commvault and TechTarget's Enterprise Strategy Group set out to understand the strategies that organizations are using for cyber-resilience planning and operations and to understand and compare where and how CR strategies differ from traditional DR strategies. This research intends to further identify overlaps and identify opportunities to integrate and refine both.

SURVEY DETAILS

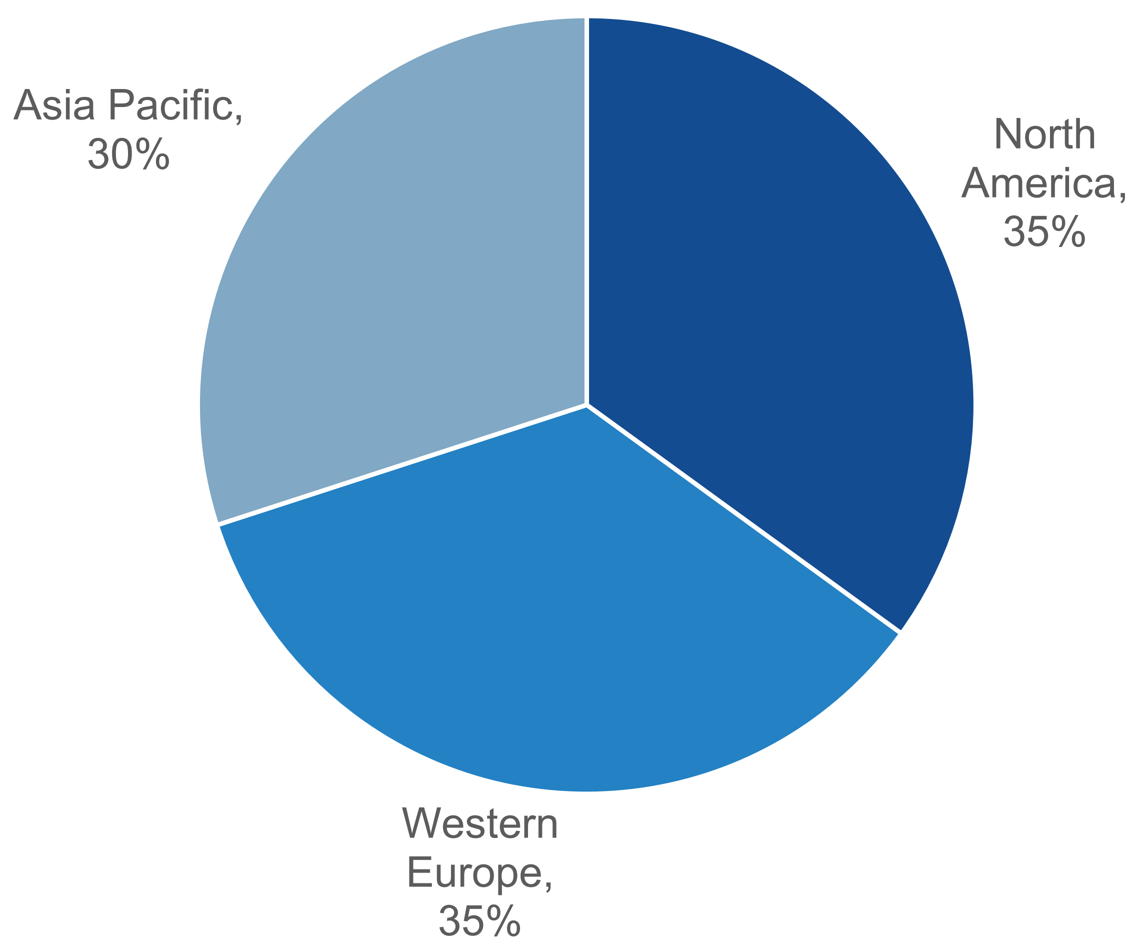
Quantitative web-based survey

- N=500 qualified completes.
- North America (U.S., Canada, 35%); Western Europe (France, Germany, U.K., 35%); Asia Pacific (ANZ, Singapore, 30%).
- Field dates: 8/27/2024-9/14/2024.

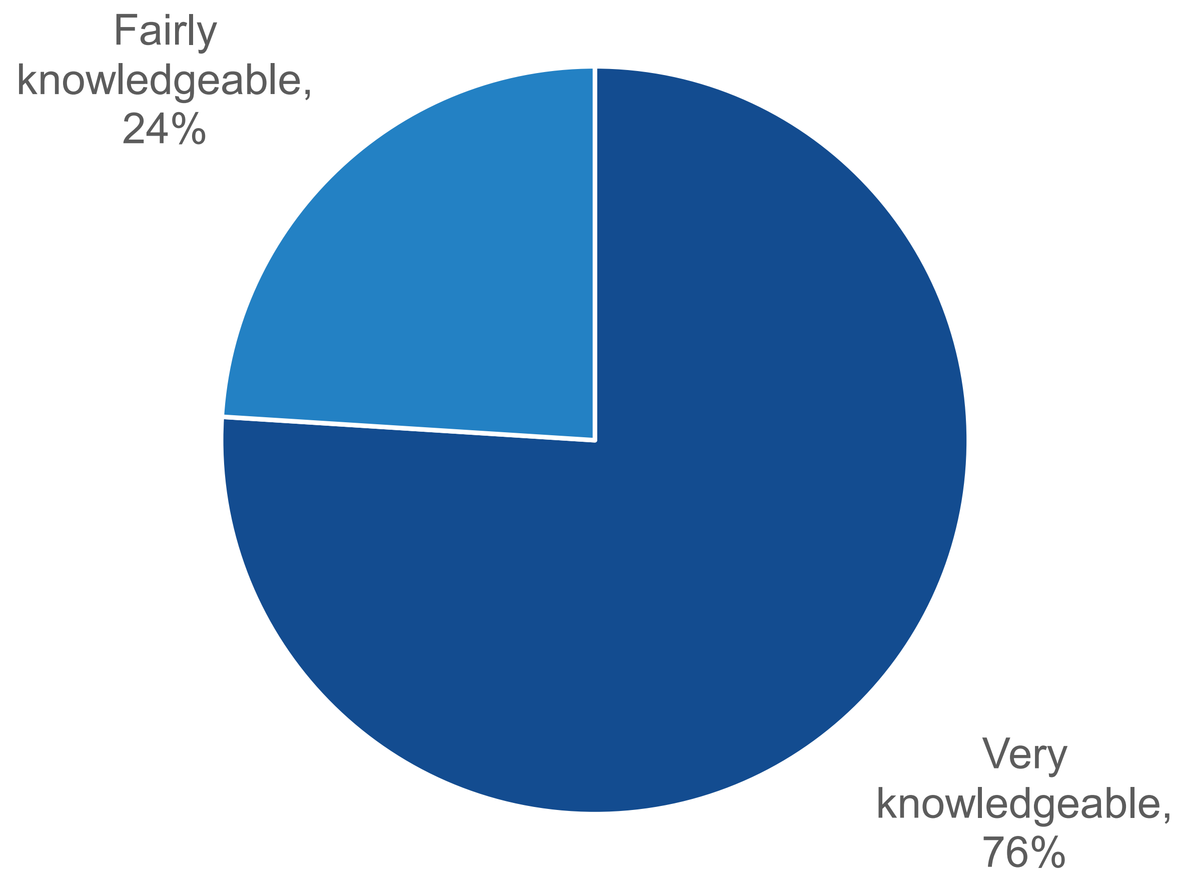
Survey respondents

- IT and cybersecurity professionals knowledgeable about their organization's BC/DR technologies and posture.
- Midmarket (100 to 999 employees, 24%) and enterprise (1,000+ employees, 76%) with $100M+ in annual revenue.

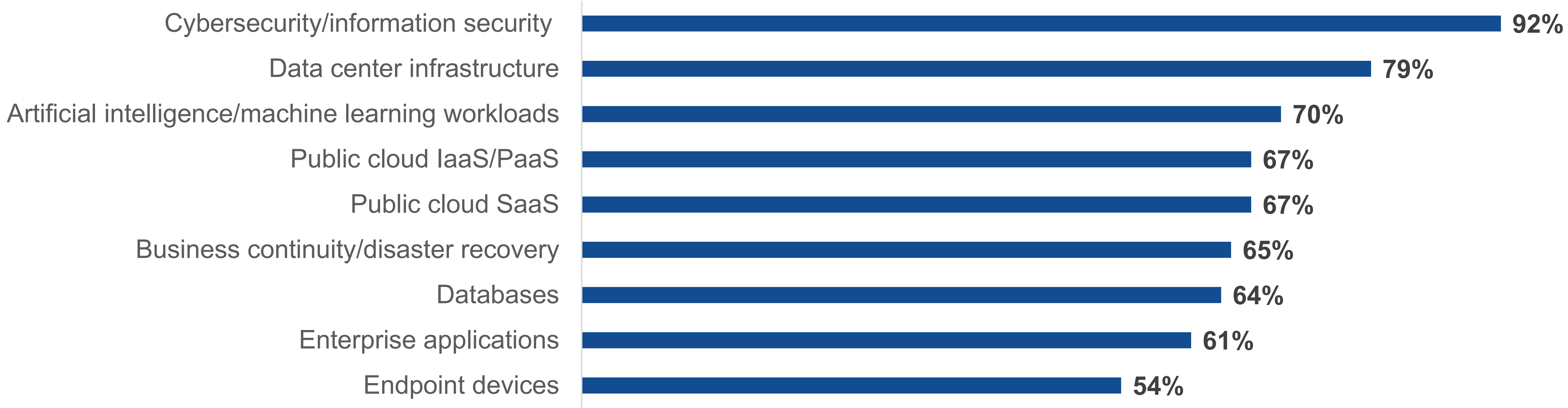
Respondents by Region.



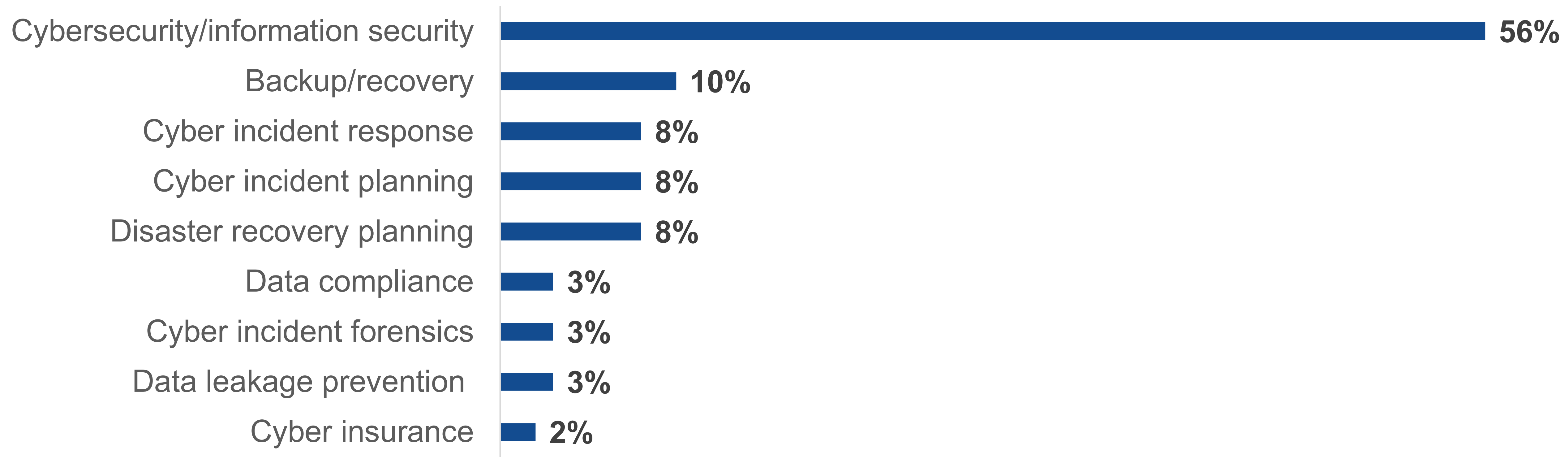
Respondents by Level of Knowledge of Executing a CR.



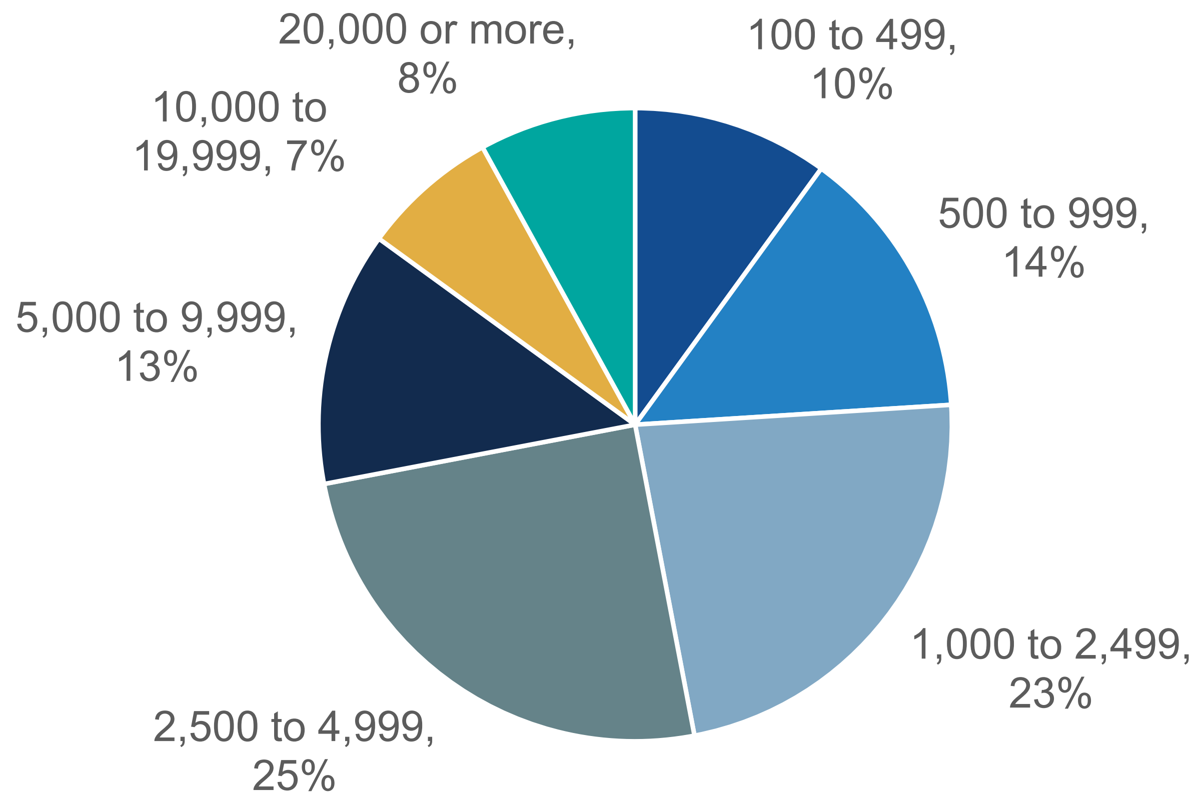
Respondents by Areas of IT Involvement.



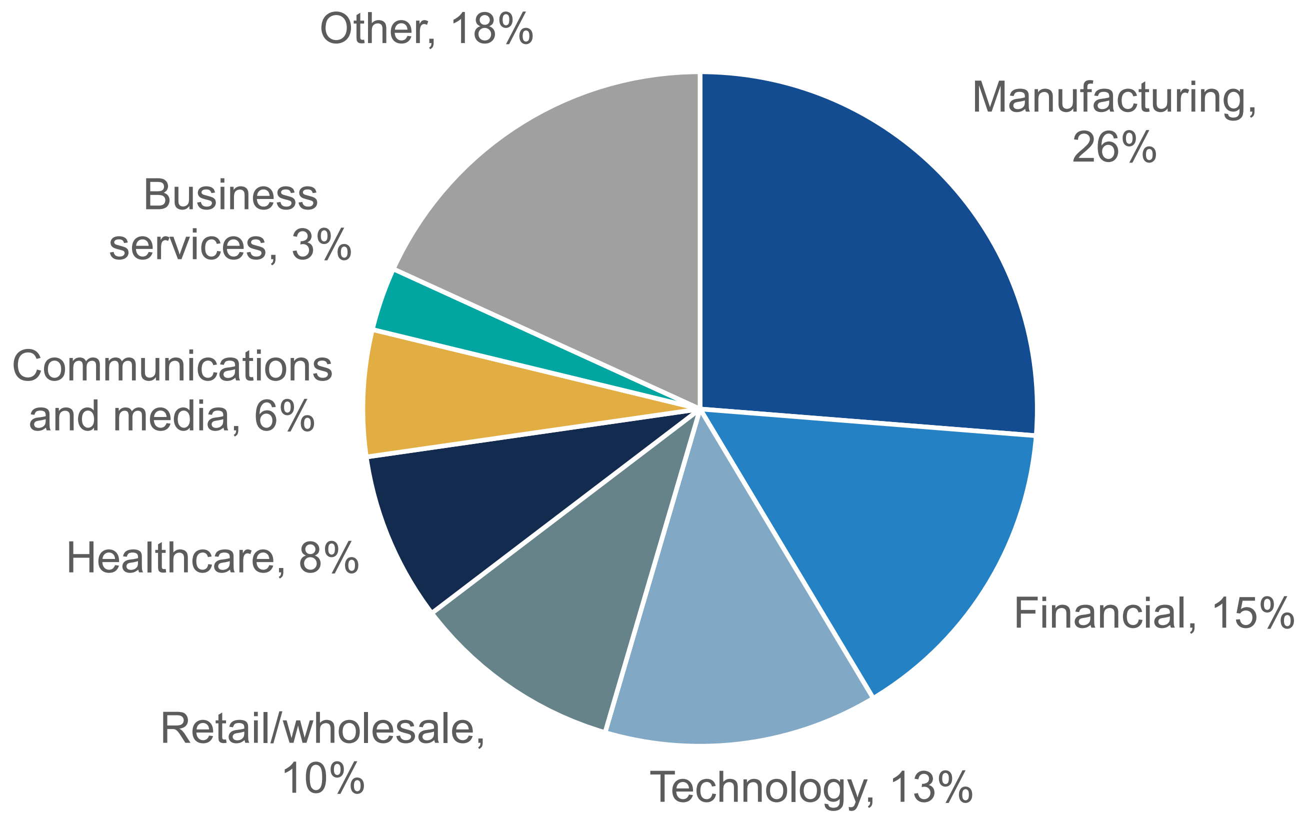
Respondents by Primary Area of CR Involvement.



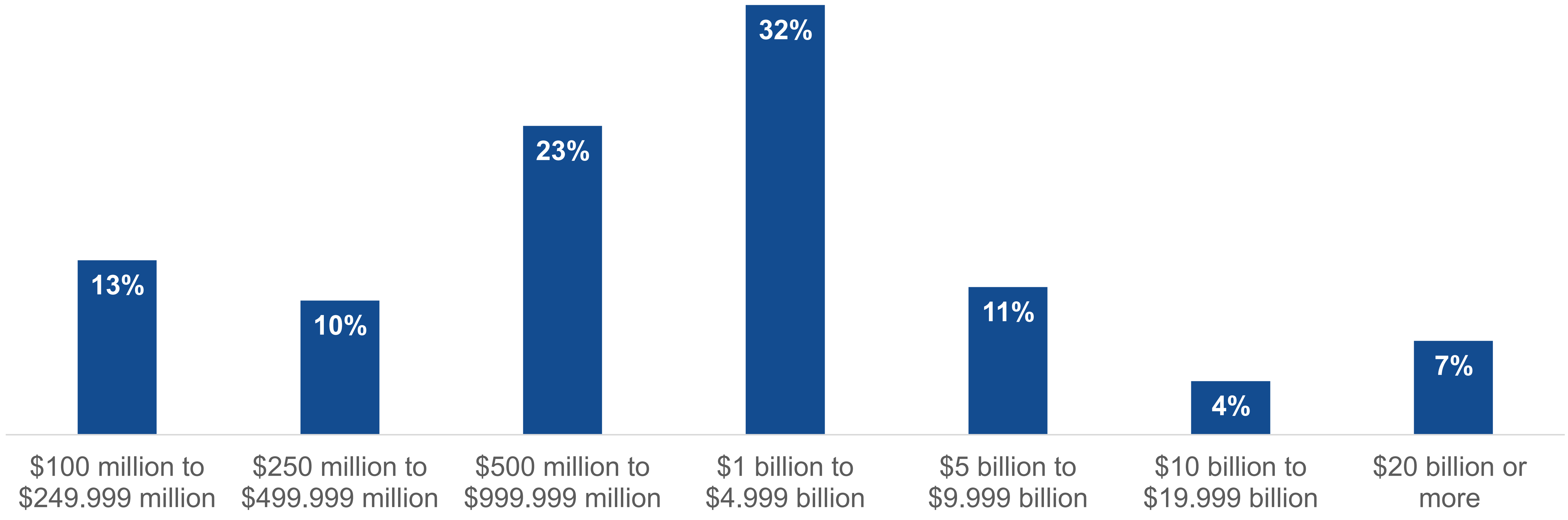
Respondents by Number of Employees.



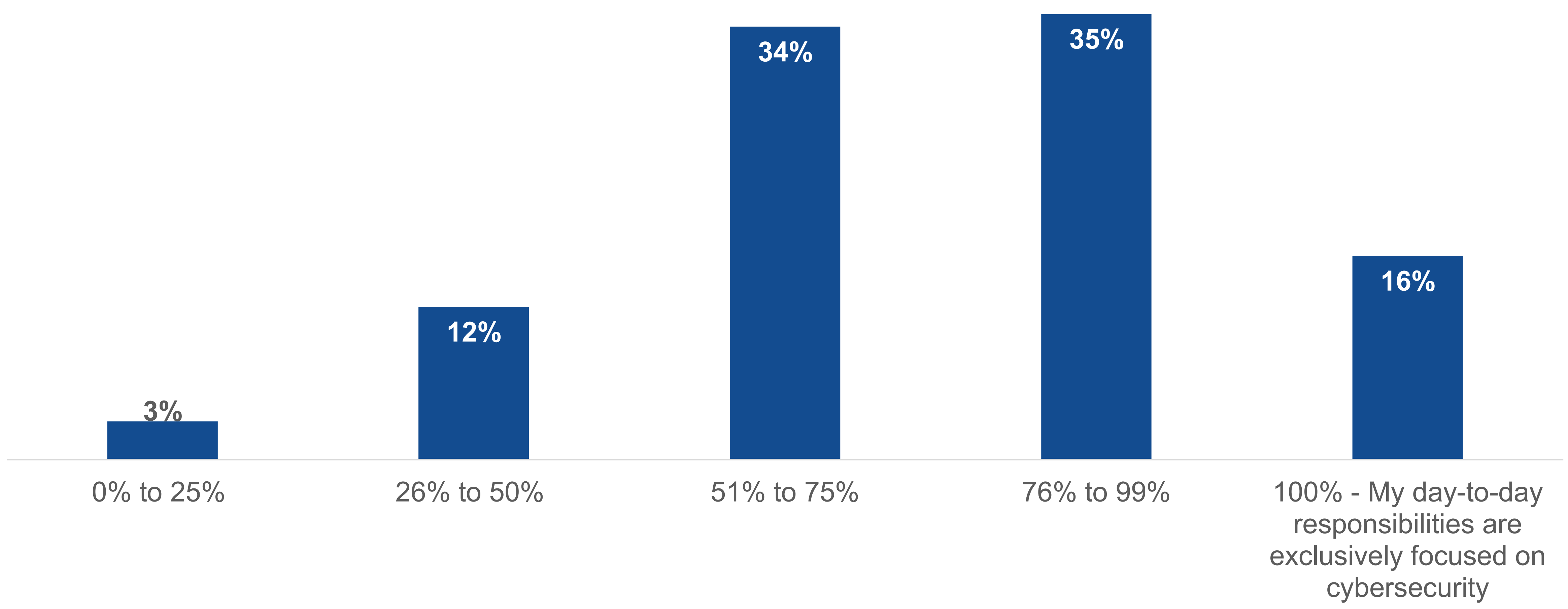
Respondents by Industry.



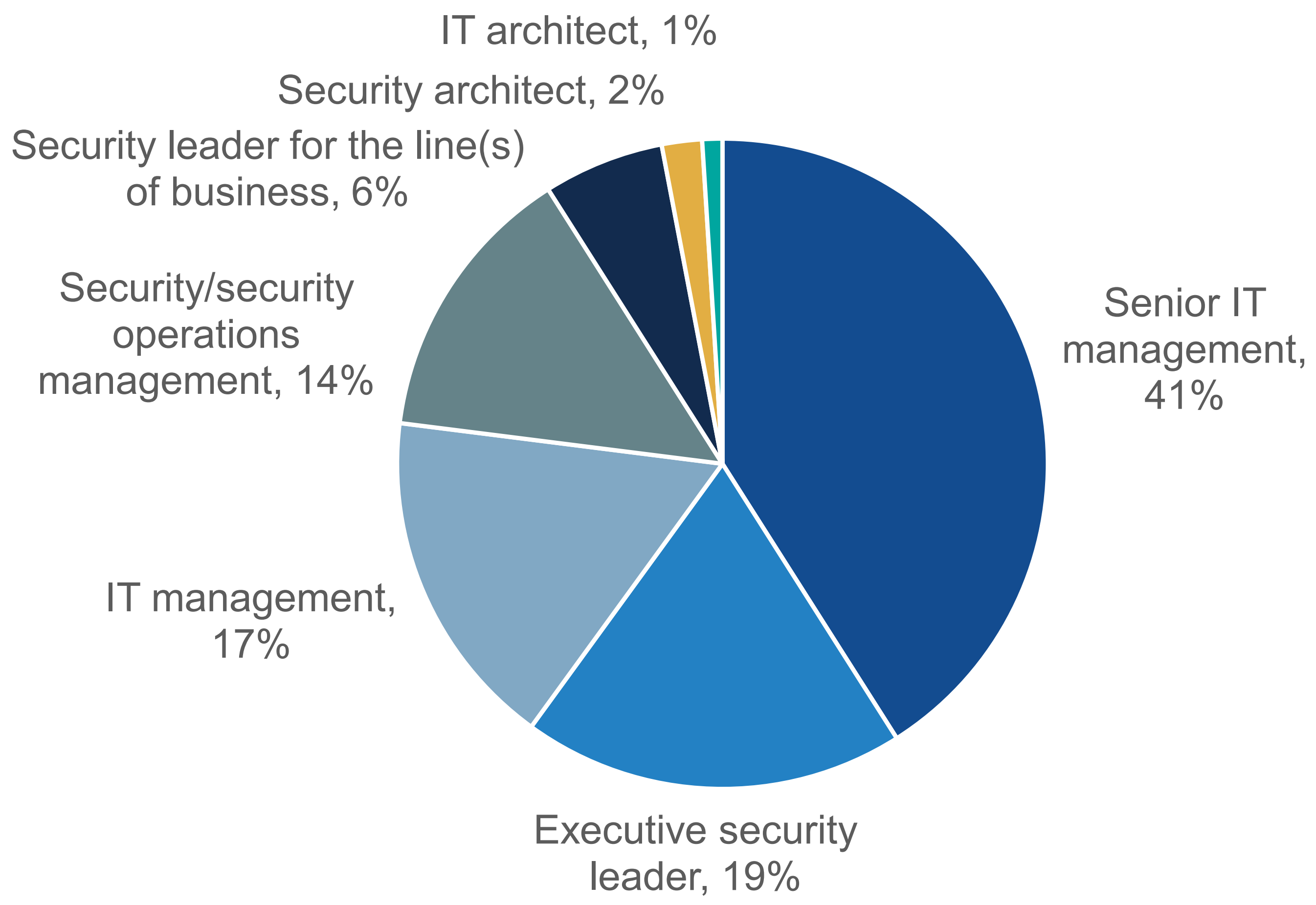
Respondents by Annual Revenue.



Respondents Responsible for Cybersecurity by Percent of Day-to-day Responsibilities Dedicated to Cybersecurity.



Respondents by Job Title/Level.



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.

Enterprise
Strategy Group™
by 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.