

# Challenges in Meeting a High Bar for Cyber Recovery in Financial Services

**Dave Gruber** | Principal Analyst  
ENTERPRISE STRATEGY GROUP

JUNE 2025

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



## Introduction

Financial services (FinServ) organizations of all sizes and types 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.

While traditional disaster recovery planning and preparation is well established for many, modern cyberattacks often result in more intense levels and complexity of disruption. Therefore, a new level of cyber recovery planning, preparation, and operations is needed, one that prepares for the unknown in terms of scope, impact, and scale while enabling rapid operational resilience.

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

To gain further insight into these trends, Enterprise Strategy Group surveyed 500 IT and security professionals employed at various organizations across the world involved with or responsible for business continuity and disaster recovery (BC/DR) technologies and posture at their organizations. Responses by those at FinServ companies (N=76) were then compared to those in other sectors (N=424) to uncover ways in which FinServ companies differ from their peers in statistically significant ways.

## Research Objectives

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

### CONTENTS:

<b>Executive Summary</b>	<b>Unique Cyber Recovery Issues for FinServ</b>	<b>FinServ Organizations’ Cyber Recovery Outcomes Appear Stronger Than Other Sectors’</b>	<b>How FinServ Organizations Achieve Superior Outcomes Despite Their Unique and Acute Challenges</b>	<b>Conclusion</b>	<b>About Commvault</b>
<b>PAGE 3</b>	<b>PAGE 4</b>	<b>PAGE 8</b>	<b>PAGE 12</b>	<b>PAGE 19</b>	<b>PAGE 20</b>





## Executive Summary

1. The FinServ industry continues to be a massive target for cyber criminal activity. Purveyors of large volumes of money and sensitive data, modern FinServ operations involve diverse and complex IT infrastructure, often changing at an accelerated pace and requiring more dynamic and resilient cybersecurity strategies. Under the constant watch of regulators, FinServ organizations need extreme diligence to comply with policies. In response, they often operate with a higher bar than other industries, requiring more advanced preparation and testing and more aggressive service-level agreements (SLAs).
2. Despite this more intense environment, our research showed that FinServ organizations often achieve higher results when it comes to overall cyber recovery. But it's important to recognize that for FinServ organizations, the bar is higher, and while, comparatively, these results might appear as if FinServ orgs are markedly achieving more success, more is expected, which is reflected in the research where FinServ respondents felt 13% less prepared when it came to skills, technology, and experience to recover from a successful cyberattack. We see further challenges reported in the ability to test recovery activities with the level of complexity, interdependencies, and potential failure points involved. Producing a clean, hardware test environment suitable for formally testing a full recovery further increases this complexity.
3. This higher level of need in the FinServ industry requires more vigilance, discipline, and thoroughness, putting a strain on existing IT and security teams to deliver and achieve adequate levels of cyber resilience. Emerging cyber recovery solutions show promise for providing relief in this already-strained environment.

*Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.*





# **Unique Cyber Recovery Issues for FinServ**

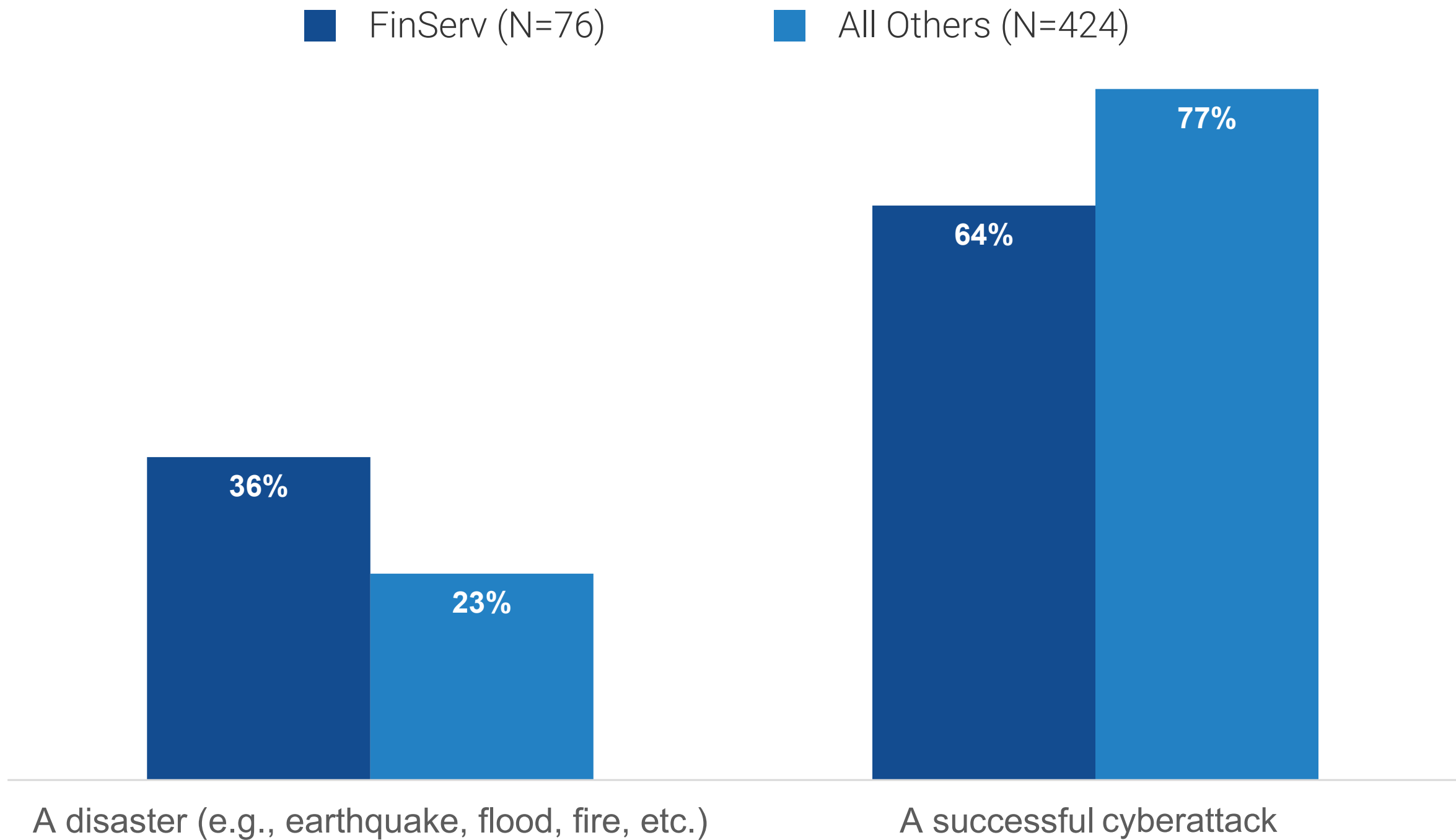
# FinServ Organizations Feel Less Prepared to Recover From Cyberincidents Than Their Peers

In the aggregate, organizations’ confidence in dealing with cyberincidents has eclipsed disasters.

While the concept of cyber recovery is more nascent, the volume of cyberattacks and the damage they can do have pushed organizations to rapidly build up their defenses and processes for response.

This dynamic holds true in the FinServ sector, but it is less pronounced than in other industries, indicating that FinServ organizations have lagged in pivoting their focus from natural disasters toward cyberattacks: 64% of those in the FinServ industry said they are more prepared to recover from a cyberattack than a disaster (vs. 77% in other verticals).

The Type of Incident Organizations Feel More Prepared to Recover From



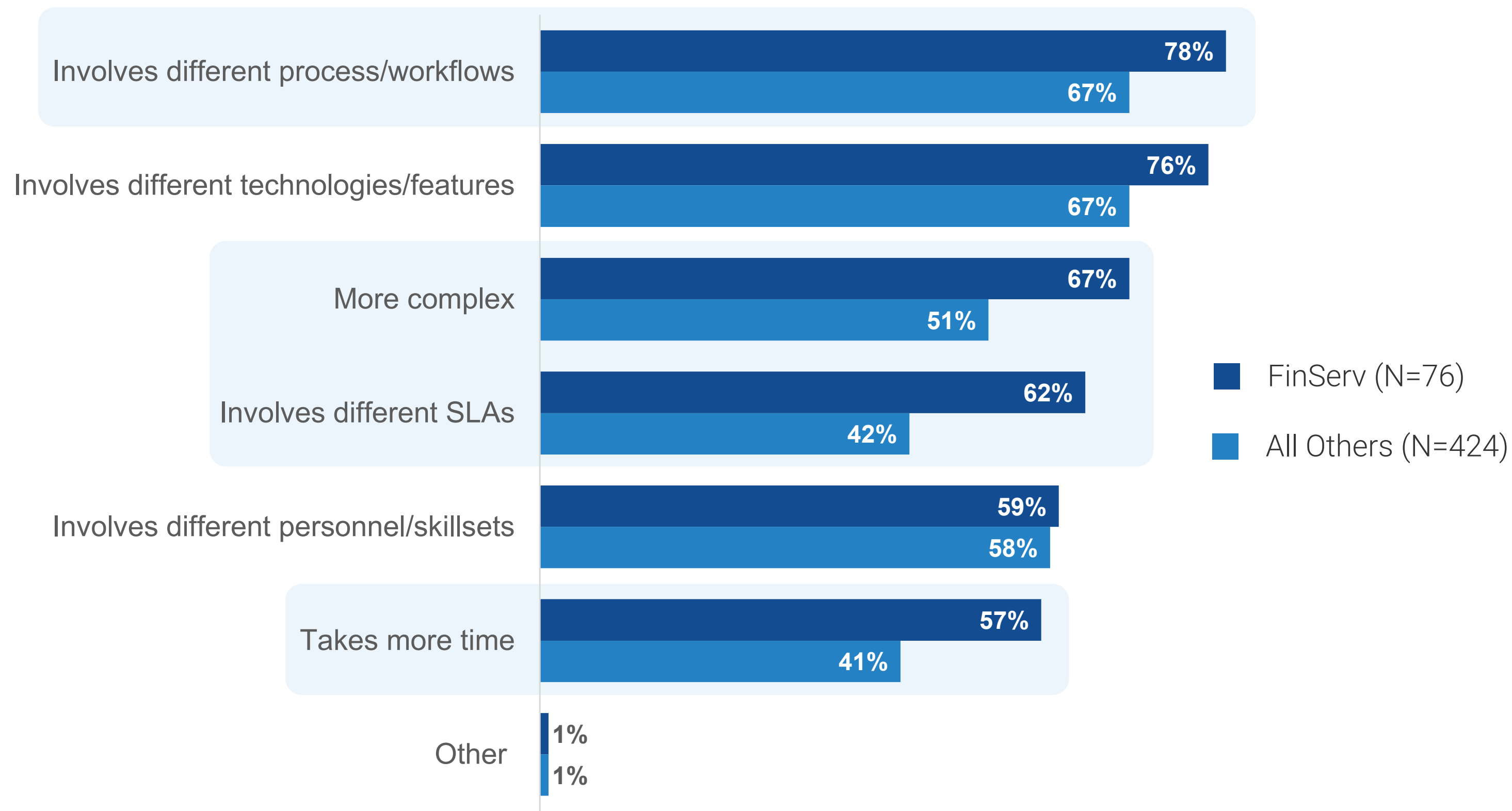
## FinServ Organizations See Cyber Recovery as More Complex and Time-consuming

Given the prior data, it is not surprising to observe that, relative to those in other verticals, respondents at FinServ organizations more often reported that cyber recoveries involve different processes, are more complex, more time-consuming, and subject to different SLAs than disaster recoveries.

We believe the reasons are multifaceted:

- Regulatory requirements likely play a factor, as many regulations that FinServ organizations are subject to mandate specific cyber response procedures that might not apply in disaster recoveries.
- Their propensity to see these processes as more complex and time-consuming might stem from the sophisticated attacks they tend to face and the complex integrations common in the industry in areas like payment networks.
- Their focus on customer trust might be a driver for faster cyber recovery SLAs, as a loss in trust can lead to liquidity issues and depositor erosion.

### Differences Between Cyber and Traditional Recoveries

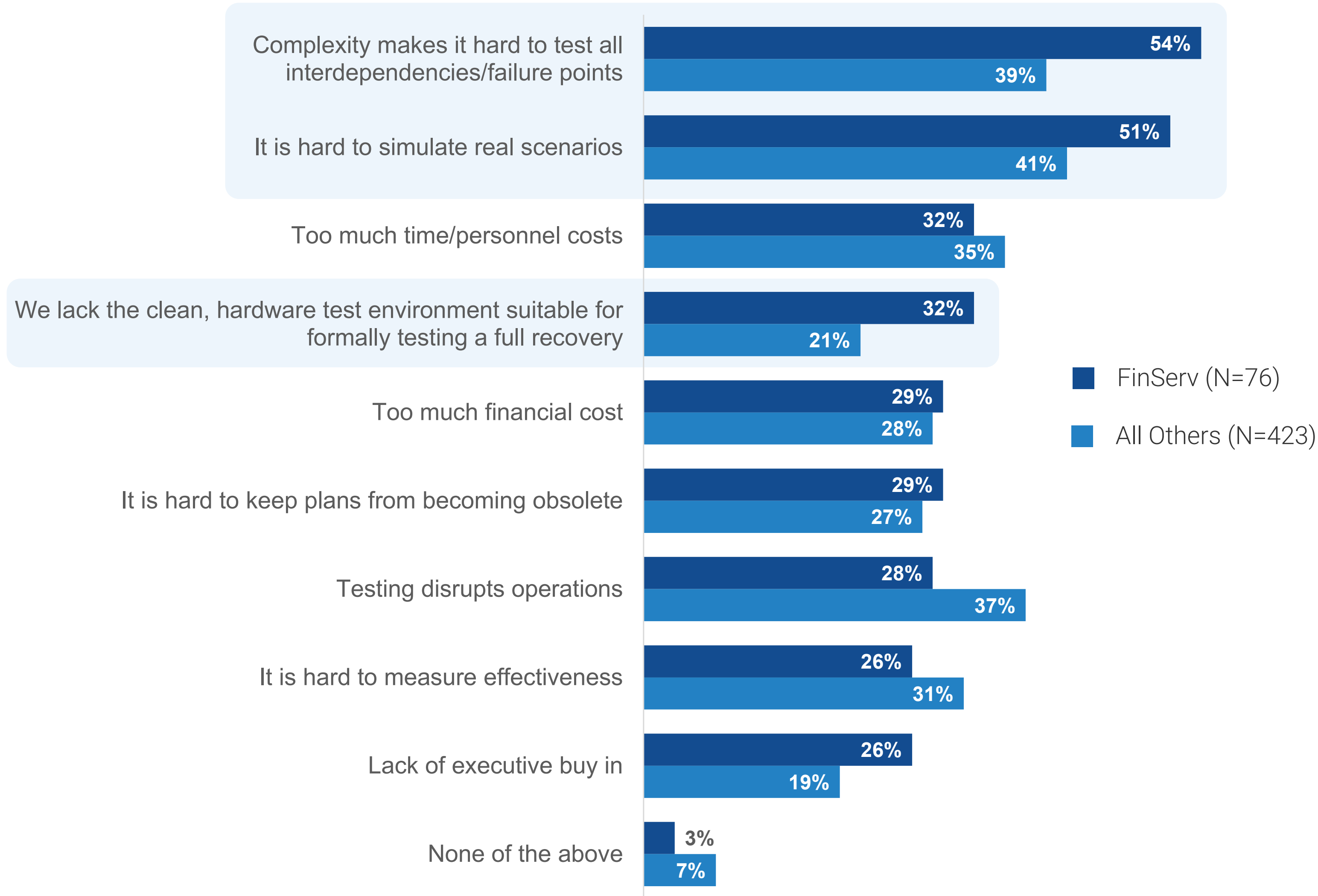





# Challenges Associated With Testing Cyber Recovery Processes

Testing cyber recovery activities is also more challenging within the FinServ industry, with these organizations being more apt to say environmental complexity, difficulty in simulating real scenarios, and a lack of a clean, hardware test environment are challenges they encounter when thinking about testing cyber recovery plans.

## Challenges Related to Testing Cyber Recovery Plans







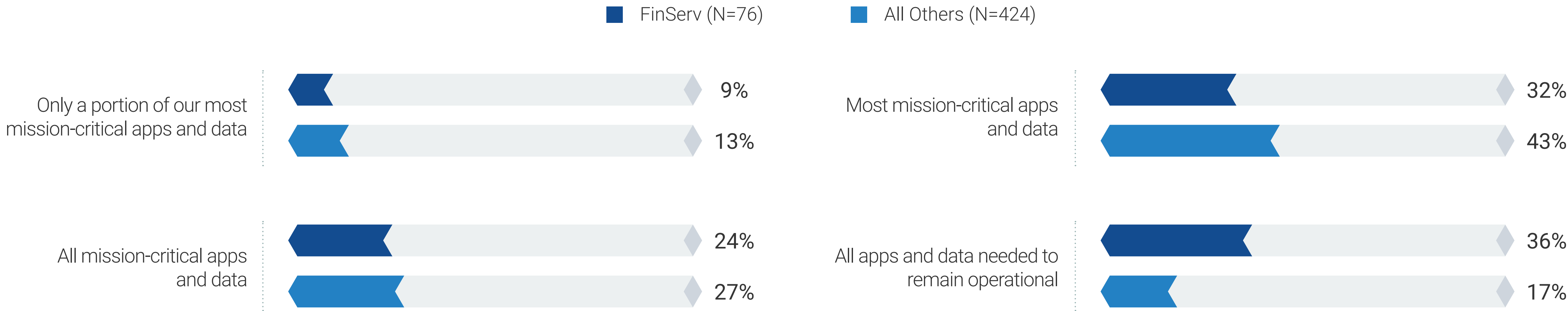
**FinServ Organizations' Cyber  
Recovery Outcomes Appear  
Stronger Than Other Sectors'**



## FinServ Organizations Feel Less Prepared to Recover From Cyberincidents Than Their Peers

FinServ organizations were more than twice as likely to report they are confident their cyber recovery plans are protecting all the apps and data the organization needs to remain operational (36% vs. 17%). Conversely, respondents in other industries were more apt to say their plans only protect a subset of mission-critical apps and data (56% vs. 41%). This level of preparedness sets the stage for achieving more positive outcomes in actual recovery activities.

I am confident in our cyber recovery plans’ ability to protect...



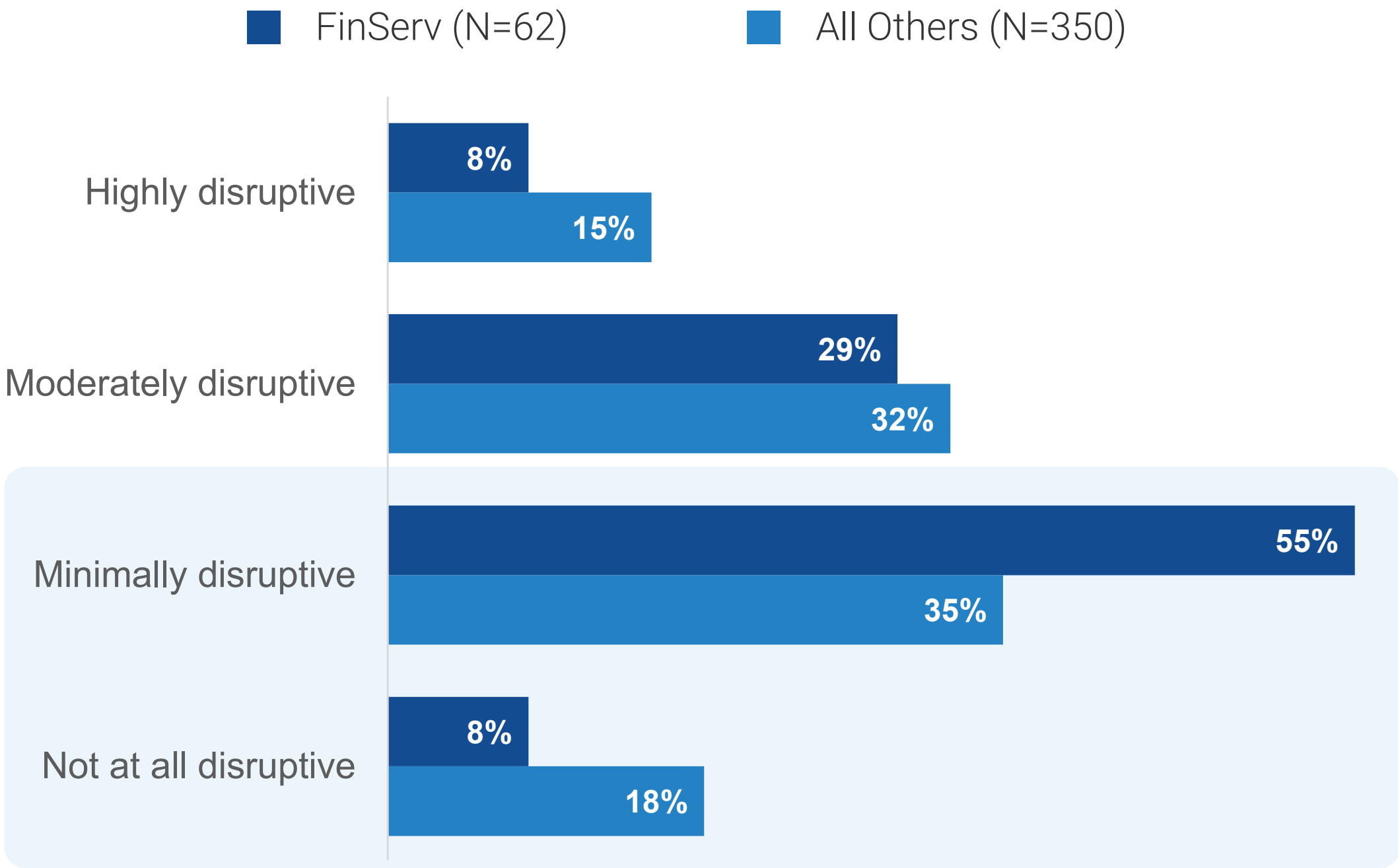


## Quantitative and Qualitative Measures of Cyber-resilient Success

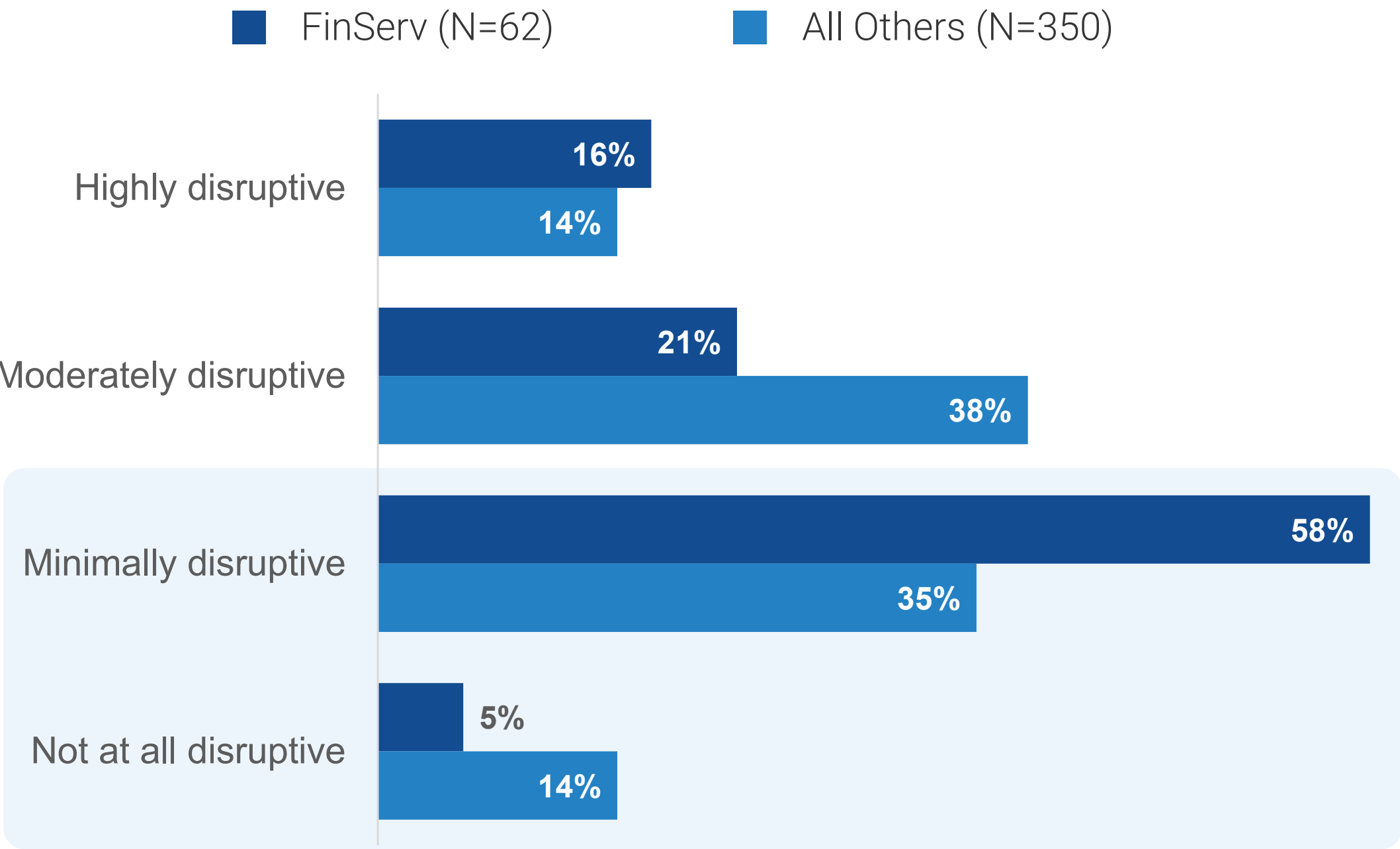
While most cyber recoveries are deemed successful in terms of meeting SLAs (75% on average across all respondents, and 77% among FinServ specifically), many said either downtime or data loss associated with recent attacks has been at least moderately disruptive. Notably, additional levels of preparedness resulted in FinServ organizations reporting less disruption to business operations:

- 63% of FinServ organizations said data loss experienced due to cyberattacks over the last 12 months has been minimally/not at all disruptive vs. 53% of respondents in other sectors.
- 63% also said downtime experienced due to attacks has been minimally/not at all disruptive vs. 49% of respondents in other sectors.

Data loss experienced has been...



Downtime experienced has been...

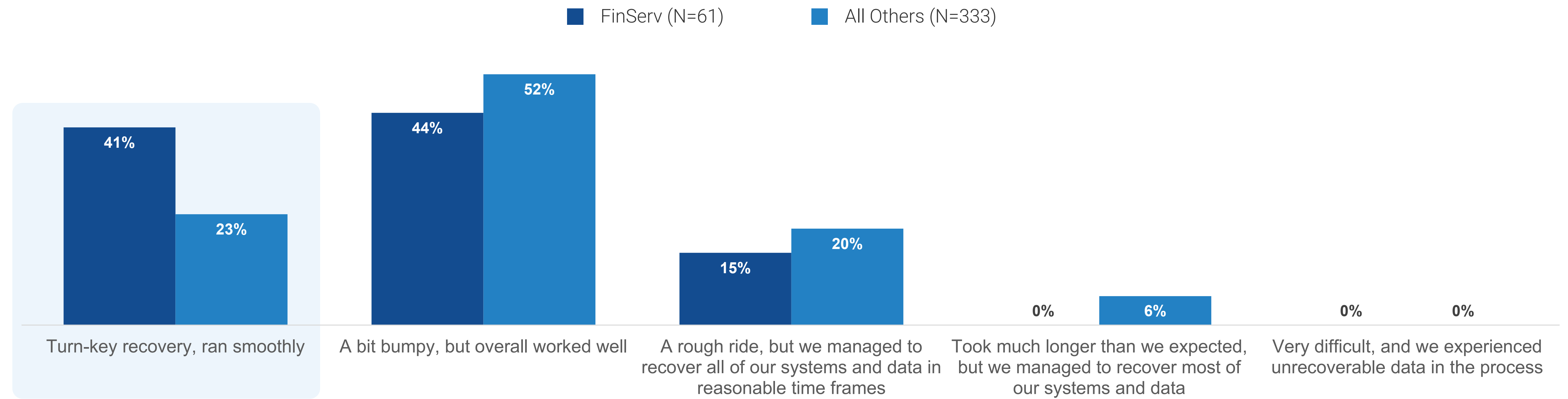




## FinServ Organizations Report Smoother Cyber Recoveries

In addition to reporting less disruption tied to data loss and downtime caused by cyberattacks, FinServ organizations also reported smoother cyber recoveries: 41% said their processes have led to turnkey, smooth recoveries (23% for all other industries).

Respondents’ Description of Recent Cyber Recoveries







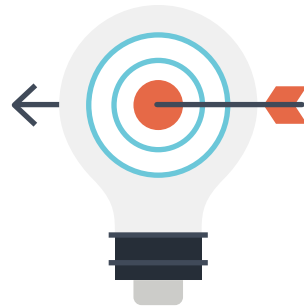
# **How FinServ Organizations Achieve Superior Outcomes Despite Their Unique and Acute Challenges**



# Five Keys to Cyber-recovery Success at FinServ Organizations

While it is somewhat paradoxical that FinServ organizations are both experiencing elevated cyber recovery challenges and delivering market-leading cyber recovery outcomes, that is exactly what the data shows.

However, the data also gives us clues as to how FinServ organizations deliver this performance. We believe this data can be used as a guide for the behaviors all organizations should follow to prepare them to quickly and effectively recover from cyberattacks.



## 1. Set Aspirational SLAs

Ambitious recovery time objectives (RTOs) and recovery point objectives (RPOs) can help push organizations to create a culture that prioritizes operational discipline and justify the technical infrastructure investments needed to respond to cyberattacks with speed and effectiveness. The data shows FinServ organizations lead their peers in setting aggressive targets.



## 2. Test Attack Readiness Frequently

Regularly testing cyber recovery plans is essential to exposing technical gaps, staffing shortfalls, and process inefficiencies before they are encountered in a crisis situation. By committing to frequent and rigorous testing, organizations are better able to continuously improve their recovery strategies and capabilities. The data shows FinServ companies lead their peers in embracing more regular testing.



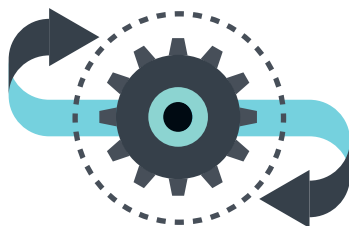
## 3. Empower the CISO to Set the Strategy

No executive at an organization is better prepared to lead the charge on cyber recovery strategies more than the CISO. Selecting solutions, establishing playbooks, and developing effective test plans for cyber recoveries demand a command of the threat landscape, an understanding of enterprise risk, and intimate familiarity with the compliance requirements the organization is subject to. More than other verticals, FinServ firms have identified that empowering CISOs to make cyber recovery strategy decisions will lead to superior performance.



## 4. Identify Key Areas of Investment for the Organization

Managing enterprise risk in any area, including cyber recovery, is a balancing act between determining acceptable risk thresholds and the investment levels needed to achieve them. FinServ organizations differ from their peers in that they are making investments in high availability infrastructure (e.g., parallel systems) much more often. This is a good insight for FinServ decision-makers to keep in mind, as even a few minutes of downtime can be extremely expensive.



## 5. Leverage AI as a Force Multiplier for Cyber Recovery Personnel

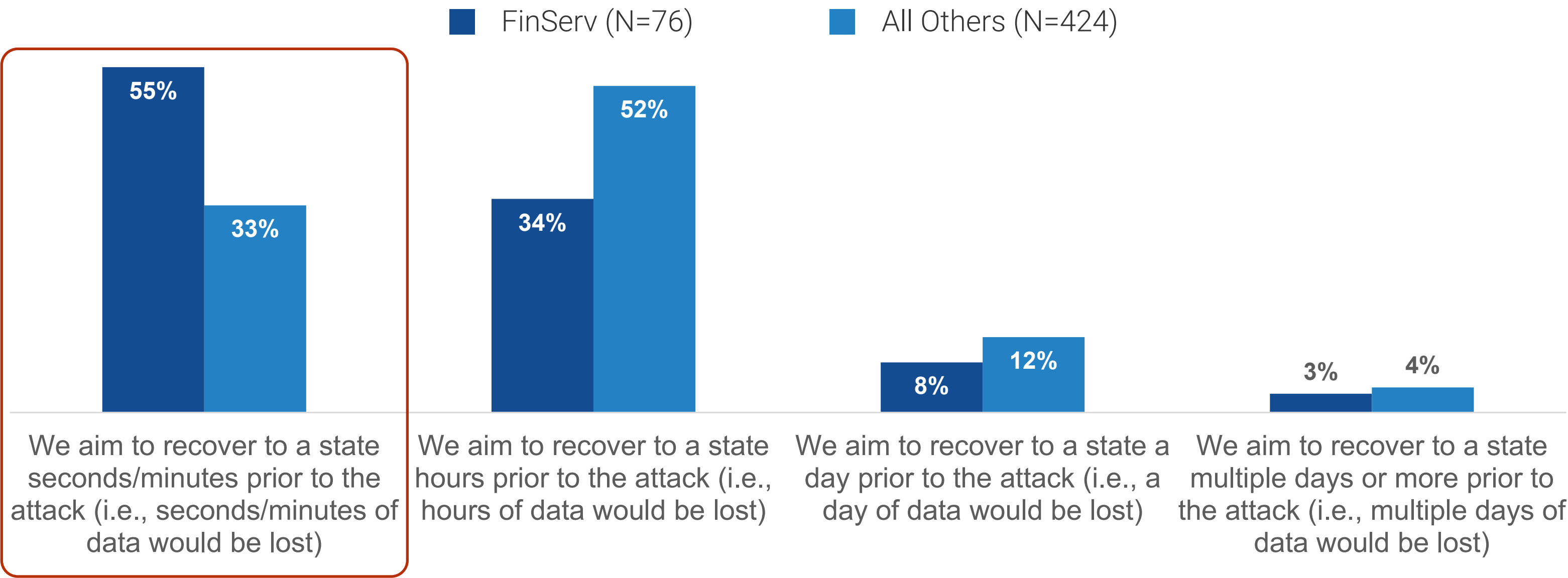
Cyber recovery processes are rife with opportunities for automation. From isolating compromised systems, dynamic failover to backup systems, executing incident response playbooks, and more, automation can help shrink recovery times. Advanced AI/ML capabilities can enhance these automations by enabling adaptive response that learns from previous incidents. FinServ organizations are well ahead of their peers in terms of adoption in this area.



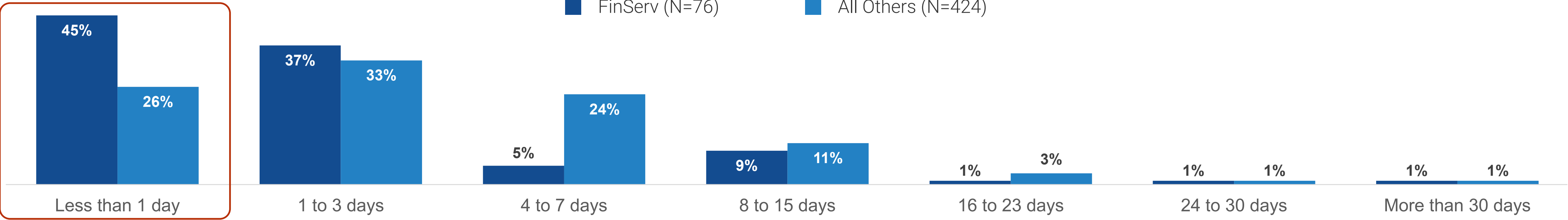
## FinServ Organizations Set Aspirational SLAs

In the aggregate, only 36% of organizations targeted seconds/minutes of lost data. And in terms of outages, only 29% of organizations in the aggregate maintained an RTO associated with cyberattacks of less than a day. However, in both regards, FinServ firms targeted shorter SLAs much more often. We believe this is driven by the fact that the loss of financial transactions can result in widespread effects to both firms’ operating objectives and customer financials. In turn, these more aggressive SLAs likely drive greater investments and a culture that prioritizes rapid recoveries, which both likely help FinServ firms’ performance.

Organizations’ RPO for Cyberattacks



Organizations’ RTO for Cyberattacks

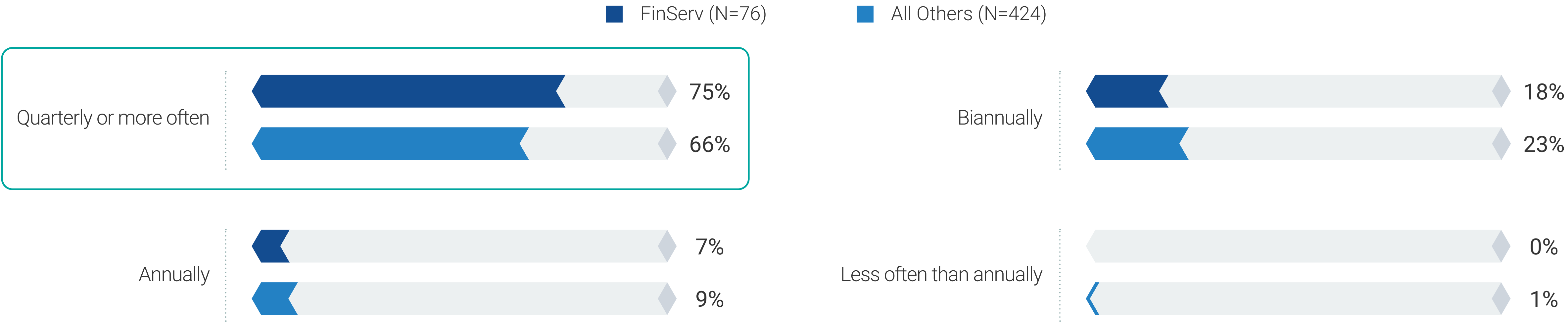




## FinServ Firms More Frequently Test Their Cyber Recovery Plans

More stringent resilience requirements in the FinServ sector appear to be driving more aggressive testing of cyber recovery plans. Specifically, 75% of FinServ respondents reported they perform quarterly (or more frequent) cyber recovery tests (vs. 66% among respondents in other verticals). Indeed, this behavior of more frequently testing cyber recoveries might be one of the reasons FinServ orgs grapple with issues related to environmental complexity and a lack of a clean, hardware test environment more often than their counterparts in other industries. However, more frequent testing also logically improves outcomes when real recoveries are required by identifying gaps in process and technology and verifying teams are comfortable with their roles and responsibilities.

### Frequency of Cyber Recovery Plan Testing







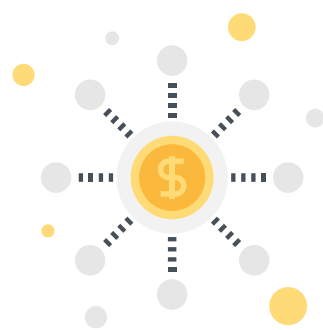
## Greater CISO Involvement in Cyber Recovery Planning

CISOs in FinServ organizations are more apt to be the owners of cyber recovery planning activities in areas like assessments and impact analyses, determining the need for new investment and test plan creation. These differences highlight a more active engagement in risk mitigation ownership for FinServ CISOs.

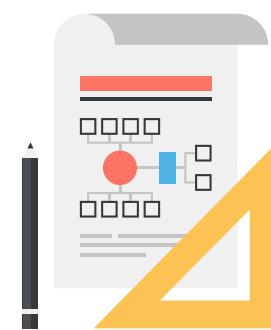
When asked who had the most ownership over specific areas of their organizations’ cyber recovery plan, respondents from FinServ organizations responded that it was their CISO for the following components:



**Risk assessments and business impact analysis:**  
CISO/CSO – 29% for FinServ vs. 17% for all other industries



**Determining the need for new investment:**  
CISO/CSO – 34% for FinServ vs. 21% for all other industries



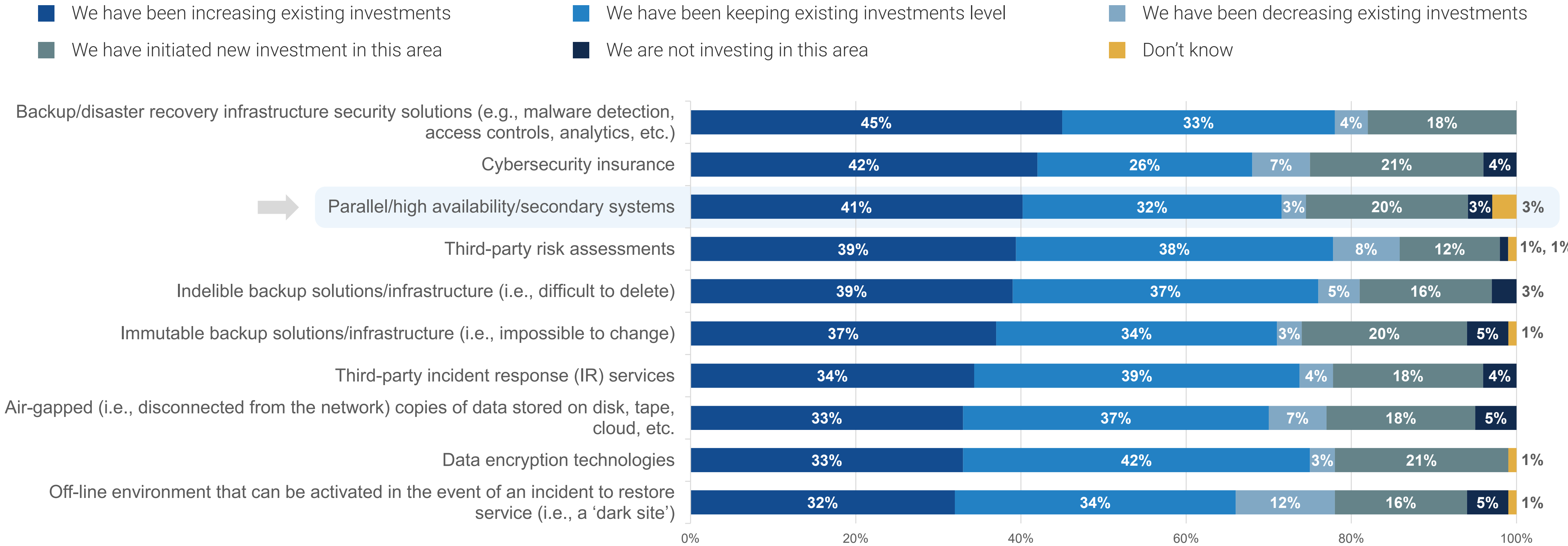
**Creation of the testing plan:** CISO – 24% for FinServ vs. 14% for all other industries



# FinServ Firms Are Investing to Increase Their Cyber Resilience

The average FinServ respondent participating in the survey reported their organization is increasing its existing investments in approximately 4 discrete technology areas, with the expressed purpose of increasing cyber resilience. This aggressive level of investment shows how FinServ organizations are making cyber resilience a business priority. While, statistically speaking, there were few differences between FinServ organizations and other verticals, one area of divergence emerged: the propensity to be increasing existing investments in parallel/HA systems (41% vs. 26% in other verticals). We believe these investments are driven, at least in part, by a need to minimize downtime and hit the ambitious RTOs discussed previously.

## Recent Investment Trends in Resilience Technologies in the FinServ Sector



## AI/ML-powered Security Technologies Have Passed the Tipping Point

Seventy-eight percent of organizations reported using AI/ML-powered security technologies extensively or selectively. Respondents in cybersecurity (i.e., those organizations closer to the tools) more often reported extensive adoption (40% vs. 26%). FinServ organizations are also more extensively embracing AI/ML-powered security solutions (43% for FinServ vs. 29% for all other industries), reflecting a push toward automation and faster threat detection and response, which, in turn, bolster cyber recovery capabilities and outcomes.

### Has Your Organization Deployed Security Solutions That Include AI/ML Capabilities?

■ FinServ (N=76)      ■ All Others (N=424)

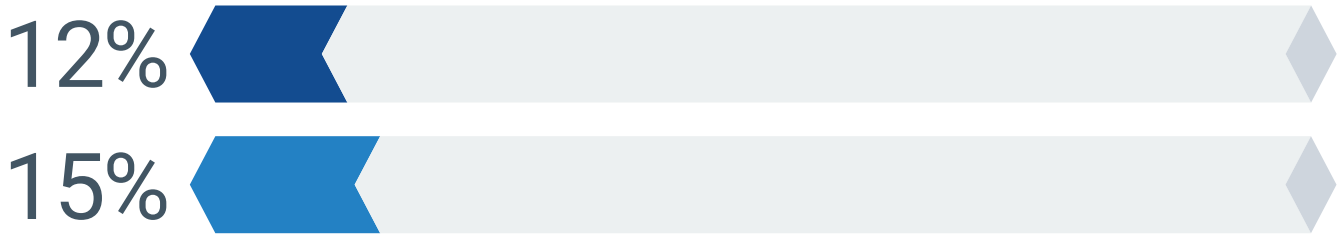
Yes, extensively



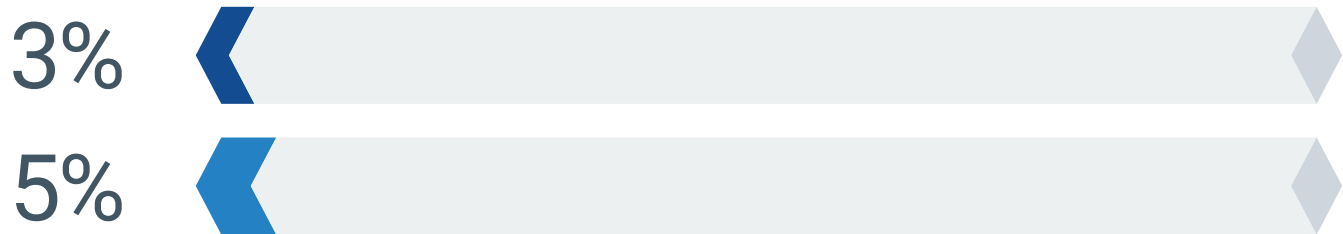
Yes, selectively



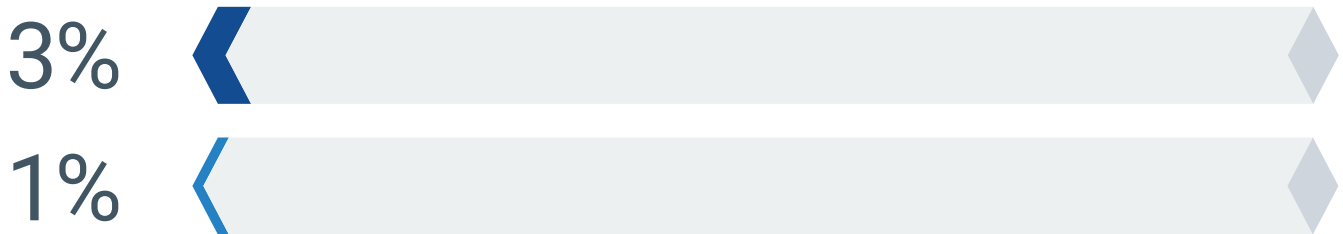
No, but we are in the process of deploying security technologies that include AI/ML



No, but we are interested in deploying security technologies that include AI/ML



No, and we have no plans for or interest in doing so







## Conclusion

Beyond downtime and data loss, cyberattacks can cause far-reaching business impacts. Reputational damage, customer loss, hard-money financial penalties from compliance violations, third-party liability and damages, and other financial losses are all possible. In response, cyber resilience has become a mainstream objective for IT and security leaders alike.

In examining the data from the FinServ sector specifically, these dynamics appear to be amplified. FinServ organizations' propensity to be subject to more stringent regulations, be more sensitive to outages and data loss, and operate extremely complex environments have all combined to create high levels of anxiety in the sector.

However, even as organizations in the FinServ sector "feel" less prepared than their peers, they comparatively enjoy better outcomes in practice. The bar is high, and the complexity continues, requiring FinServ organizations to continue investment in strengthening skills, discipline, and technologies that can support more aggressive SLAs, recovery testing, and overall operational cyber resilience.



ABOUT

Commvault is the gold standard in cyber resilience, helping more than 100,000 organizations keep data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere – at the lowest TCO.

Safeguarding and governing financial data isn't a necessity – it's a competitive edge. Learn how Commvault's cyber resilience solutions help you protect, recover, and maintain continuous business operations.

LEARN MORE





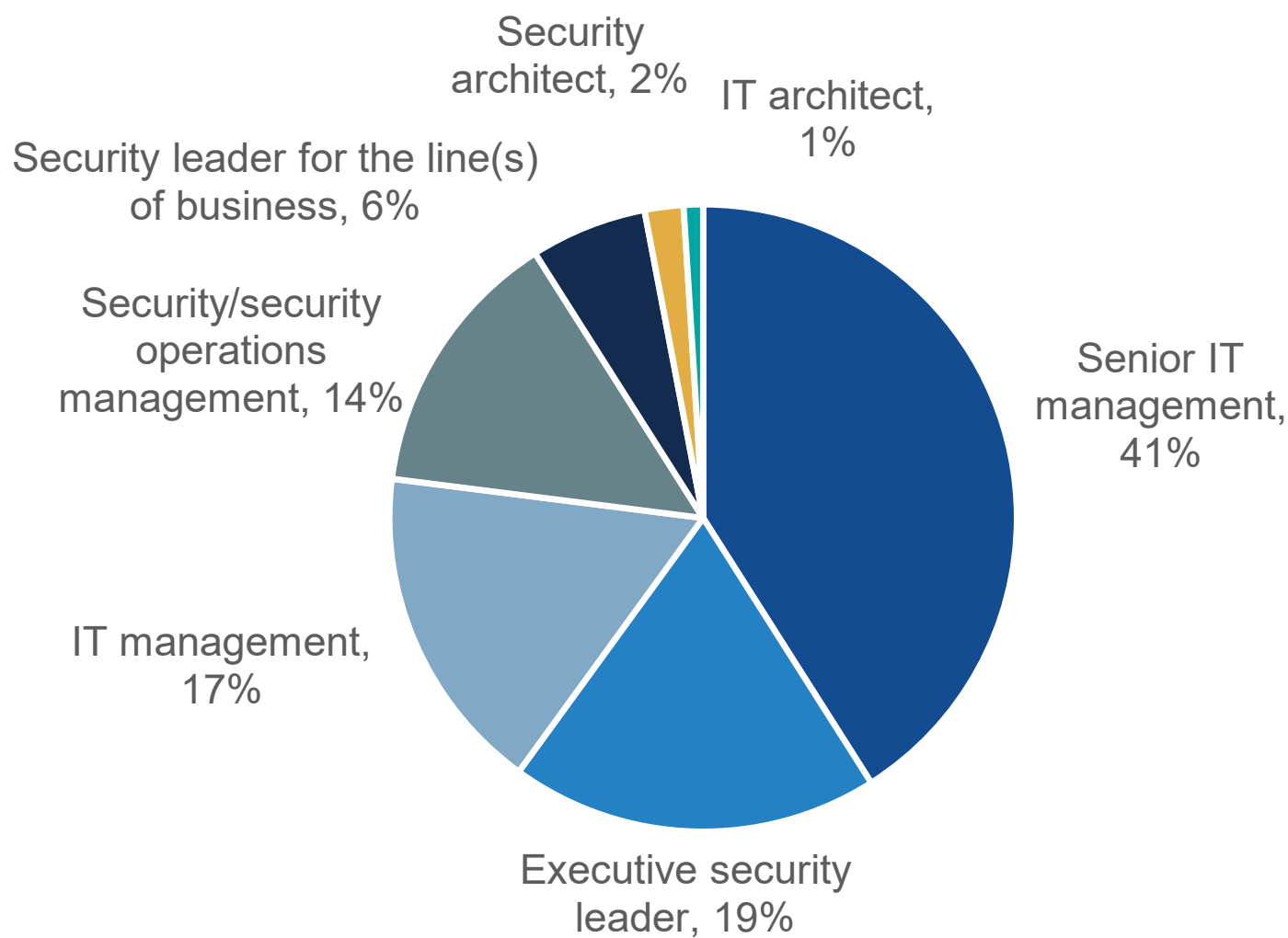
RESEARCH METHODOLOGY  
AND DEMOGRAPHICS

To gather data for this report, Commvault commissioned Enterprise Strategy Group to conduct a comprehensive online survey of IT and cybersecurity professionals knowledgeable about their organization’s BCDR technologies and posture. Respondents represent a variety of private- and public-sector organizations in North America (U.S., Canada, 35%), Western Europe (France, Germany, U.K., 35%), and the Asia-Pacific region (ANZ, Singapore, 30%) between August 27, 2024, and September 14, 2024. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

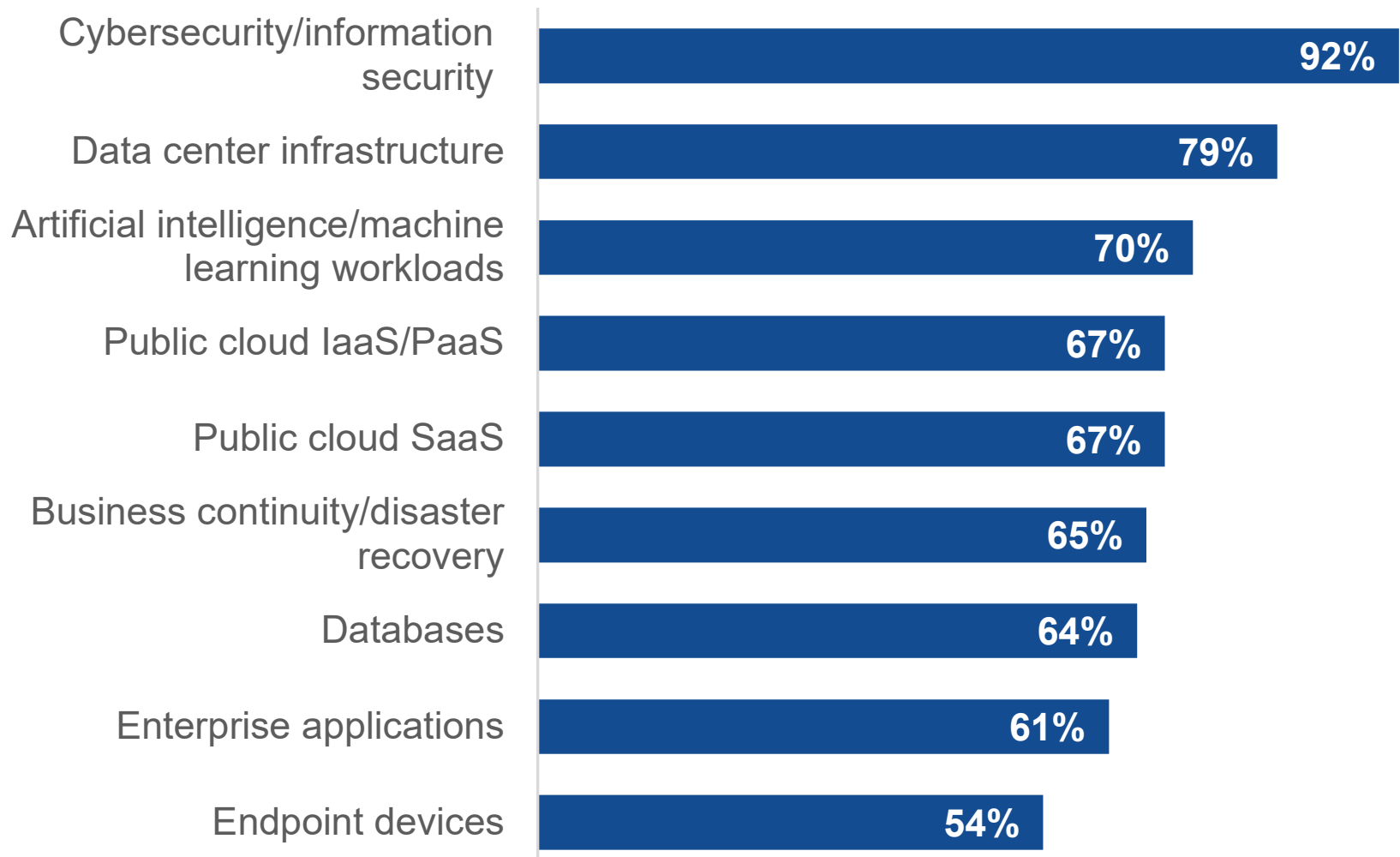
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 500 IT and cybersecurity professionals. The margin of error at the 95% confidence level for this sample size is + or - 4 percentage points.

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

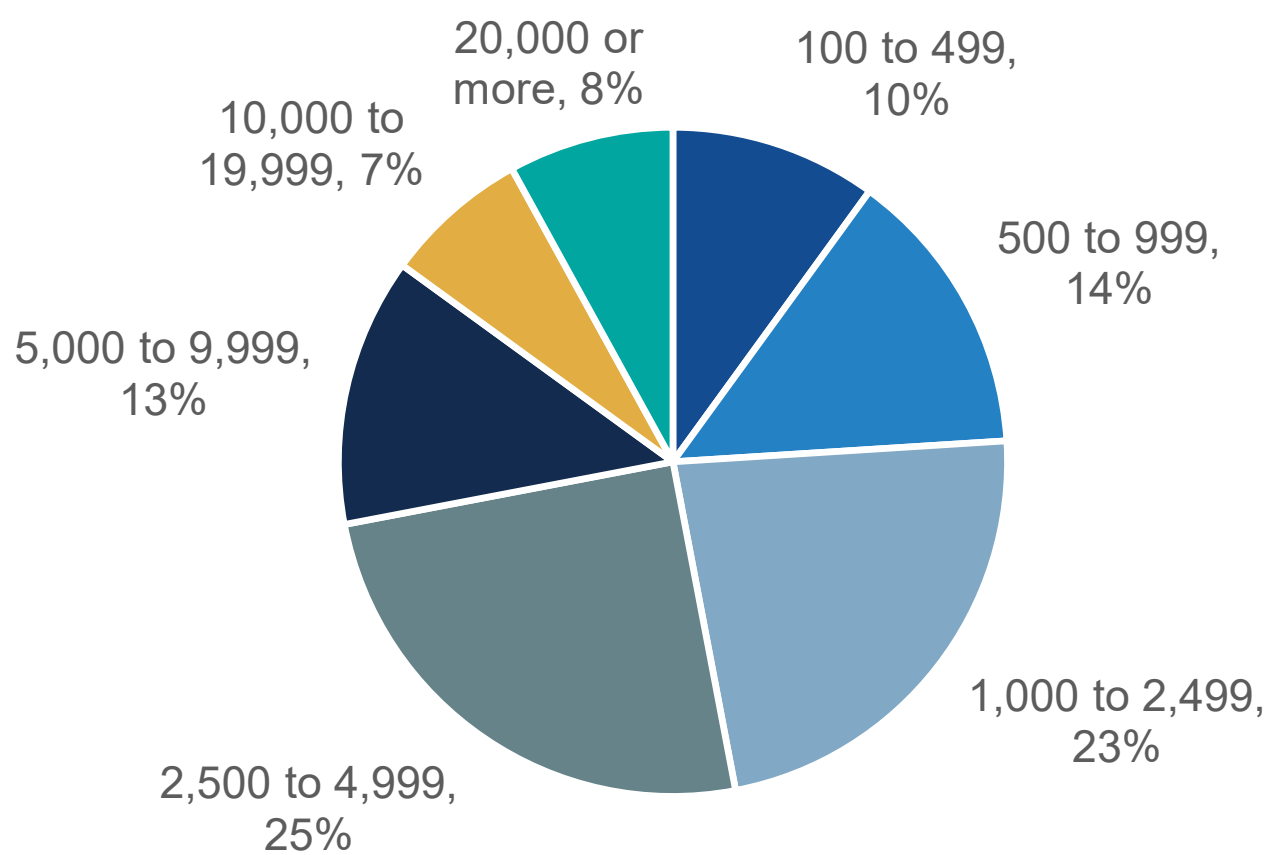
Respondents by role.



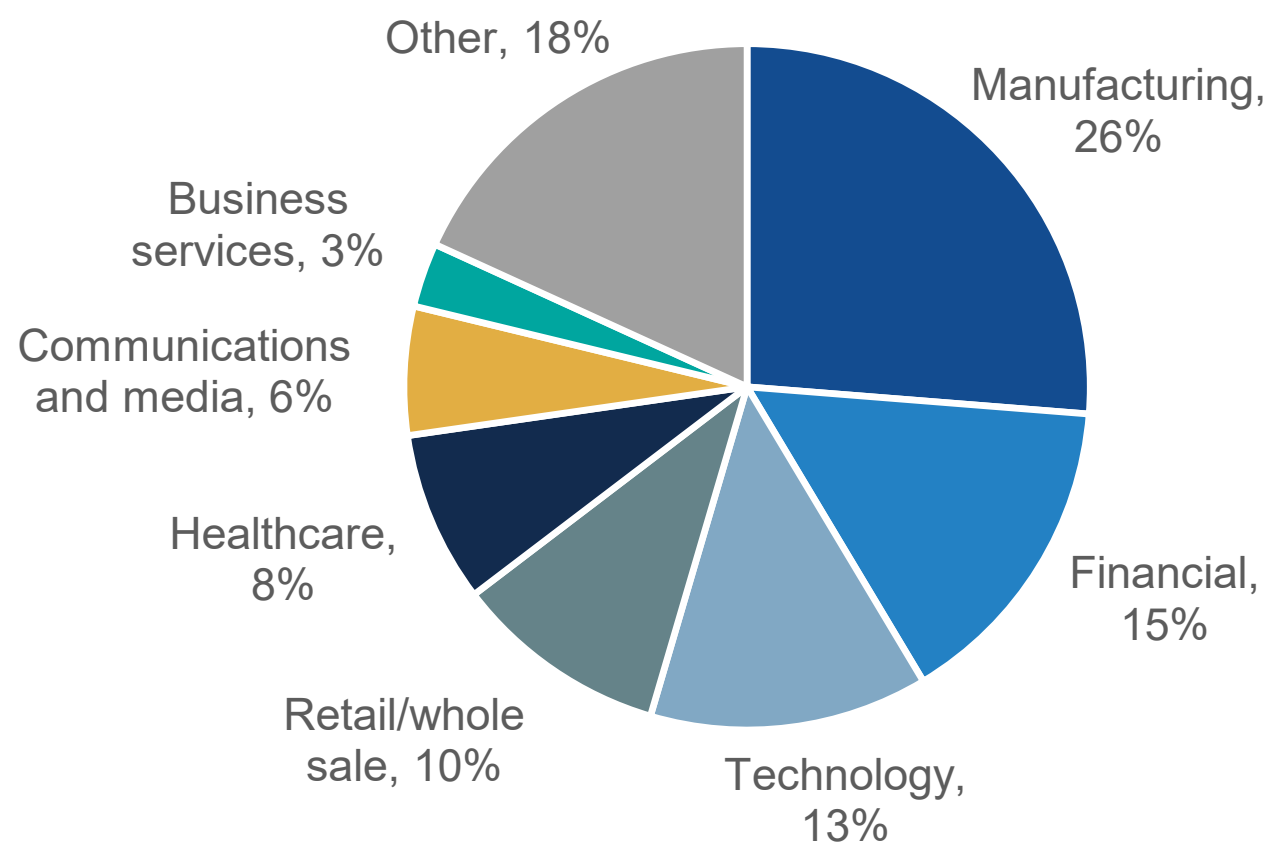
Respondents’ areas of purchase influence.



Respondents by company size (number of FTEs)?



Respondents by industry.



©2025 TechTarget, Inc. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of Informa TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).



Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

© 2025 TechTarget, Inc. All Rights Reserved.