# BACKUP AND RECOVERY

A MarketPulse Survey for Connection

OCTOBER 2023

Connection®
we solve IT®

In Partnership With:

FOUNDRY

# TABLE OF CONTENTS

# INTRODUCTION

Managing your backup and recovery ecosystem can quickly become a make-or-break situation.

As cyberthreats become more invasive, the data you rely on to return to a working state needs to be protected in new ways. Connection partnered with Foundry to deliver this peer-level review of the information you need to know when taking a harder look at how you are saving and retrieving critical data.

# METHOD AND OBJECTIVES

## Survey Goals

In this survey we evaluate data backup and recovery strategies at enterprise organizations, including data storage methods and frequency of testing backup data integrity.

We also uncover the impact of data loss on enterprise organizations.

Lastly, we determine important factors when choosing backup service or software.

**Total Respondents:**

100

**Collection Method:**

Online questionnaire

**Geography:**

U.S.

**Field Dates:**

October 17–26, 2023

**Number of Questions:**

8

**Average Organization Size:**
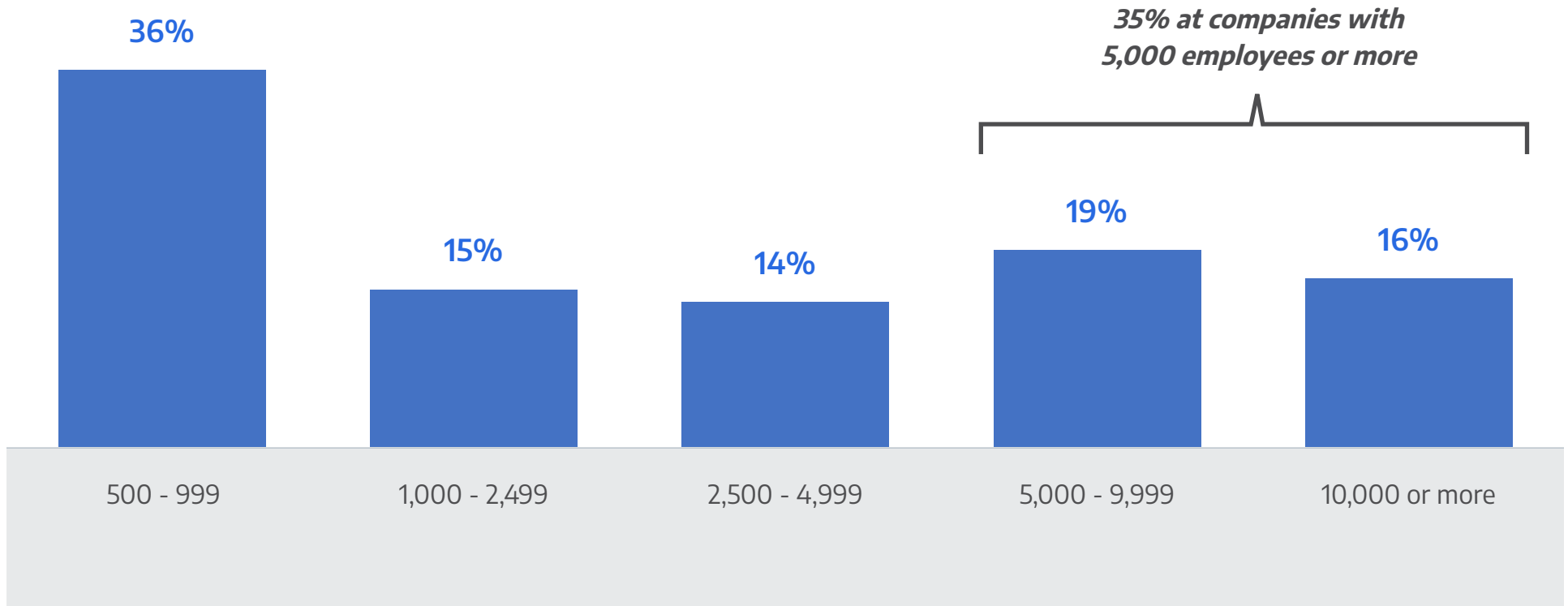
5,370 employees

**Senior Decision-makers:**

Respondents are employed in IT management roles or above

# RESPONDENT PROFILE

# COMPANY SIZE BY NUMBER OF EMPLOYEES



**36%**

**15%**

**14%**

**19%**

**16%**

*35% at companies with 5,000 employees or more*

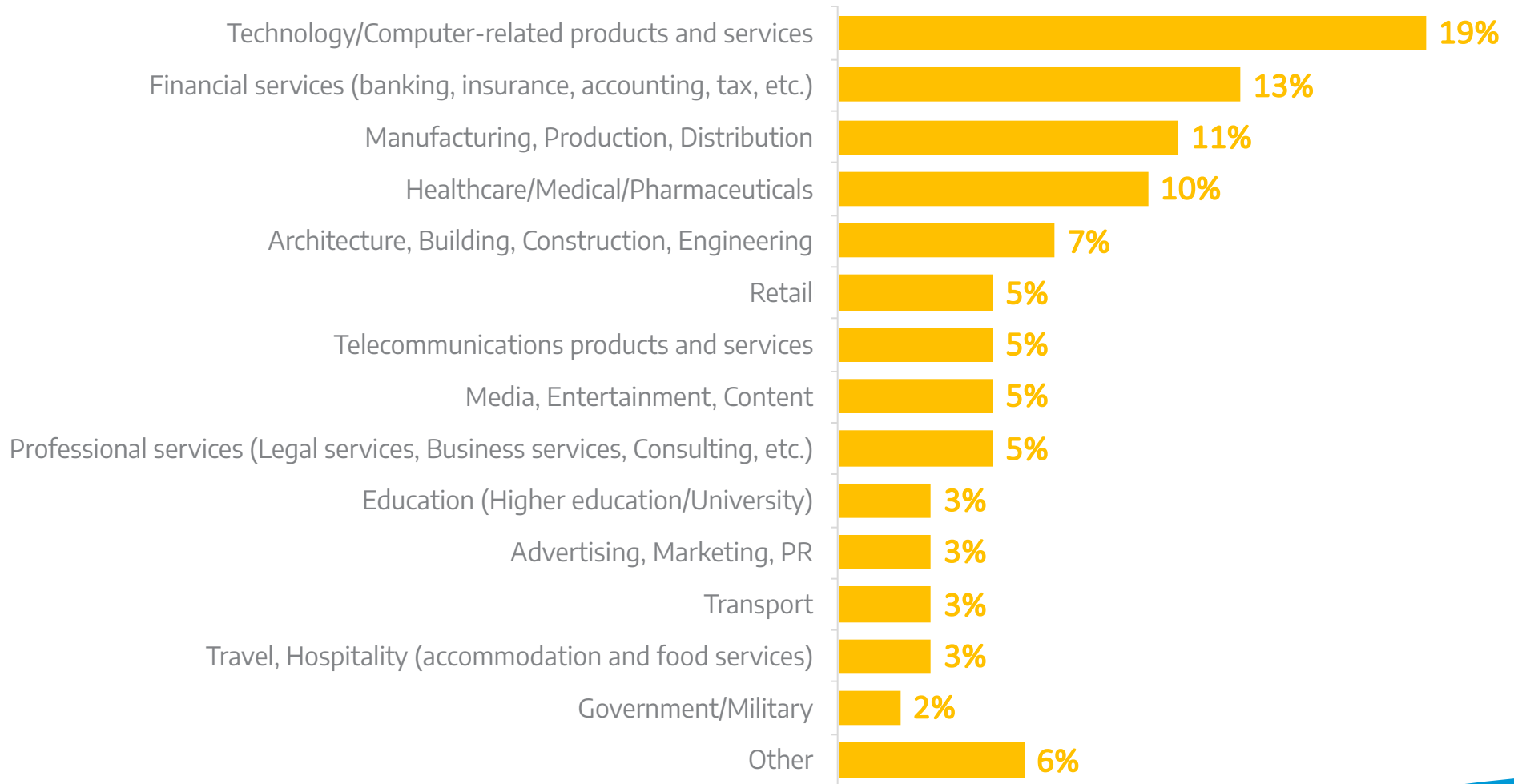| 500 - 999 | 1,000 - 2,499 | 2,500 - 4,999 | 5,000 - 9,999 | 10,000 or more |

Question S1: Approximately how many people are employed in your entire organization or enterprise? (Please include all plants, divisions, branches, parents, and subsidiaries worldwide.)
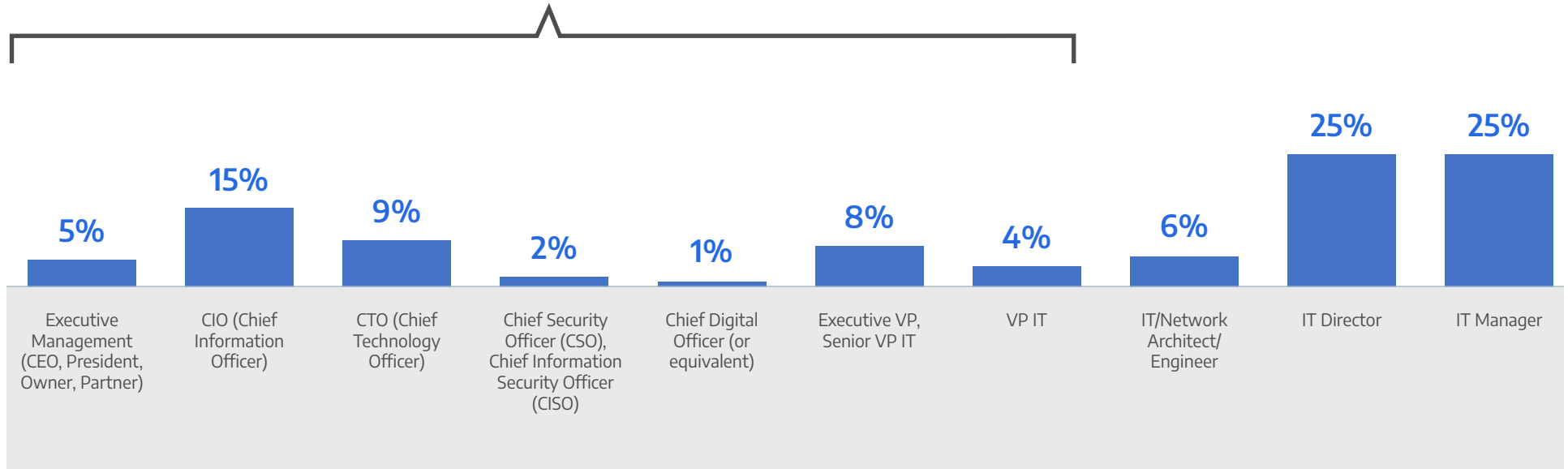
Base 100

# PRIMARY INDUSTRY

| Industry | Percentage |
|---|---|
| Technology/Computer-related products and services | 19% |
| Financial services (banking, insurance, accounting, tax, etc.) | 13% |
| Manufacturing, Production, Distribution | 11% |
| Healthcare/Medical/Pharmaceuticals | 10% |
| Architecture, Building, Construction, Engineering | 7% |
| Retail | 5% |
| Telecommunications products and services | 5% |
| Media, Entertainment, Content | 5% |
| Professional services (Legal services, Business services, Consulting, etc.) | 5% |
| Education (Higher education/University) | 3% |
| Advertising, Marketing, PR | 3% |
| Transport | 3% |
| Travel, Hospitality (accommodation and food services) | 3% |
| Government/Military | 2% |
| Other | 6% |

Question 9: Which of the following best describes your organization's industry or sector?

Base 100

# JOB TITLES

**44% hold VP or above titles**



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 5% | 15% | 9% | 2% | 1% | 8% | 4% | 6% | 25% | 25% |
| Executive Management (CEO, President, Owner, Partner) | CIO (Chief Information Officer) | CTO (Chief Technology Officer) | Chief Security Officer (CSO), Chief Information Security Officer (CISO) | Chief Digital Officer (or equivalent) | Executive VP, Senior VP IT | VP IT | IT/Network Architect/ Engineer | IT Director | IT Manager |

Question S3: What is your primary job title?
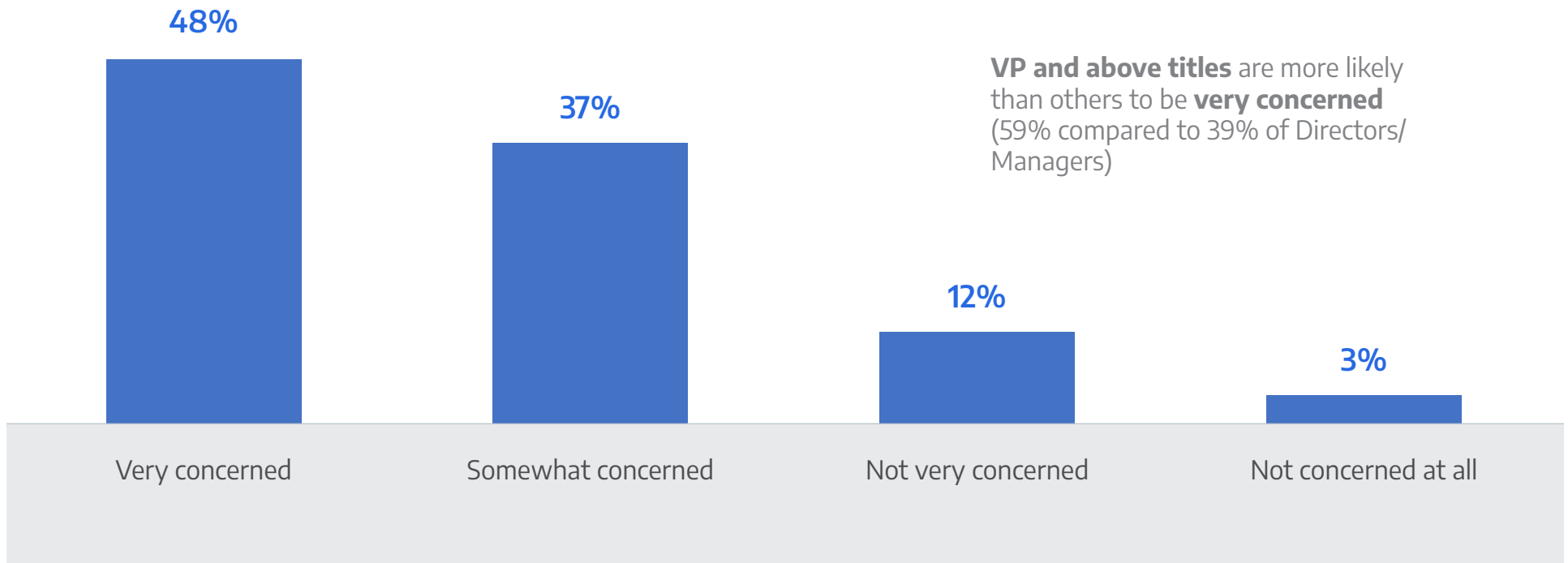
Base 100

# EXECUTIVE SUMMARY

# HIGHLIGHTED FINDINGS

- **Most IT decision-makers (85%) are concerned about the potential for data loss over the next 12 months.**
  48% are very concerned and 37% are somewhat concerned.

- **91% report their organizations have experienced data loss. 85% indicate this has occurred in the past 12 months.**
  59% have experienced a cyberattack, 57% have lost data due to human error, and 55% cite system failure as a contributor to data loss.

- **75% of those who have experienced data loss report a strong to severe impact on overall security posture.**
  66% report a similar impact on productivity. 55% indicate finances/expenses have been strongly or severely impacted by data loss.

- **55% report their organizations are backing up all organizational data.**
  18% are backing up mission-critical data only, 21% are only backing up data within specific areas, and 6% do not yet have a backup or recovery plan.

- **93% of organizations with a backup and recovery plan are using cloud or hybrid storage for backup data.**
  49% are leveraging hybrid storage, 44% are storing backup data in the cloud, and just 7% are using local storage for backup data.

- **55% of those with a backup and recovery plan are conducting routine and frequent data integrity checks.**
  20% are checking data integrity on a routine but limited basis, and 23% check data integrity only occasionally.

- **33% have not evaluated their backup and recovery strategy in the past 6 months.**
  26% evaluated their plan 6 months to 2 years ago, while 7% indicate their strategy was last evaluated more than 2 years ago. 66% have reviewed their plan in the past 6 months.

- **Security and encryption are rated as the most important factors when choosing a backup service or software.**
  52% rate this as the most important factors. Speed and performance are rated as the most important considerations among 22% of respondents. 14% rate ease of use and automation as the top factors. 12% rank cost of storage space as number one.

# SURVEY RESULTS

# 85% ARE CONCERNED ABOUT THE POTENTIAL FOR DATA LOSS OVER THE NEXT 12 MONTHS

**Concern about the potential for data loss over the next 12 months**



**48%** Very concerned

**37%** Somewhat concerned

**12%** Not very concerned

**3%** Not concerned at all

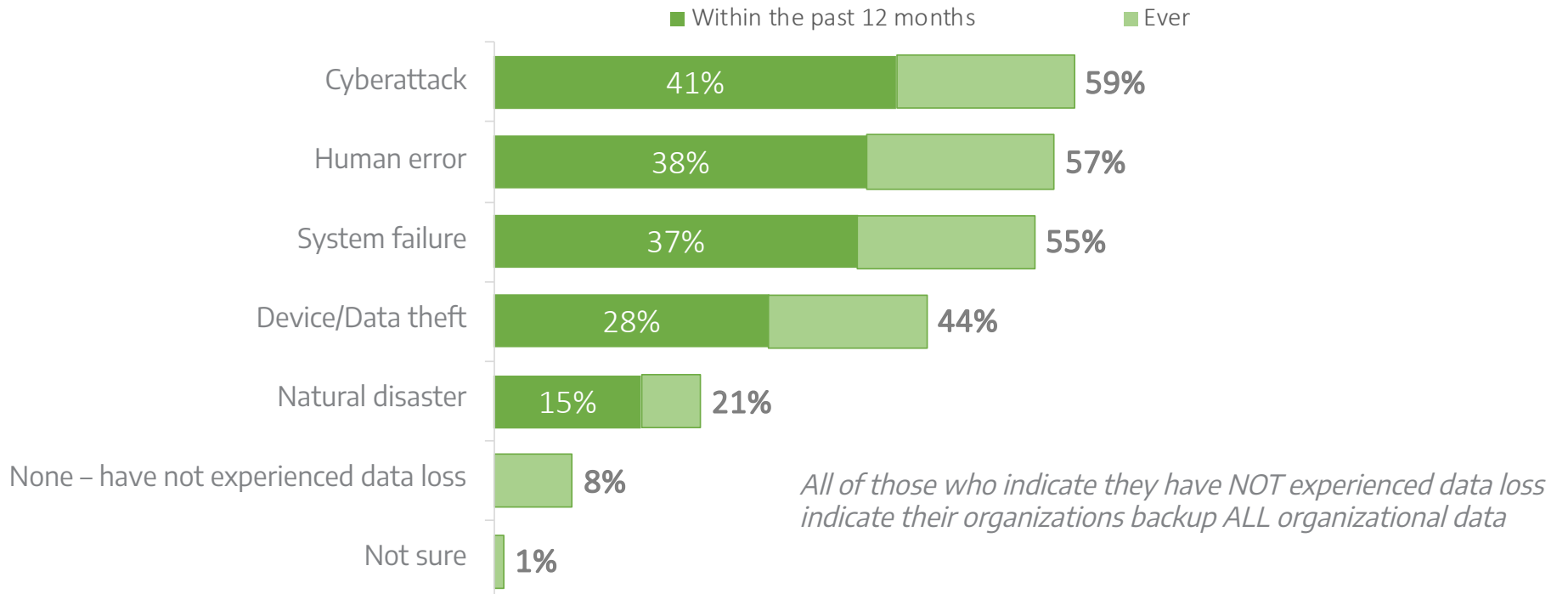**VP and above titles** are more likely than others to be **very concerned** (59% compared to 39% of Directors/ Managers)

Question 1: How concerned is your organization about the potential for data loss over the next 12 months?

Base 100

Connection
we solve IT®

FOUNDRY

BACKUP AND RECOVERY

# NINE IN TEN (91%) REPORT THEIR ORGANIZATIONS HAVE EXPERIENCED DATA LOSS; A MAJORITY (85%) HAVE LOST DATA IN THE PAST 12 MONTHS

**Has your organization ever experienced data loss attributed to any of the following?**



■ Within the past 12 months    ■ Ever

| | Within the past 12 months | Ever |
|---|---|---|
| Cyberattack | 41% | 59% |
| Human error | 38% | 57% |
| System failure | 37% | 55% |
| Device/Data theft | 28% | 44% |
| Natural disaster | 15% | 21% |
| None – have not experienced data loss | | 8% |
| Not sure | | 1% |

*All of those who indicate they have NOT experienced data loss indicate their organizations backup ALL organizational data*
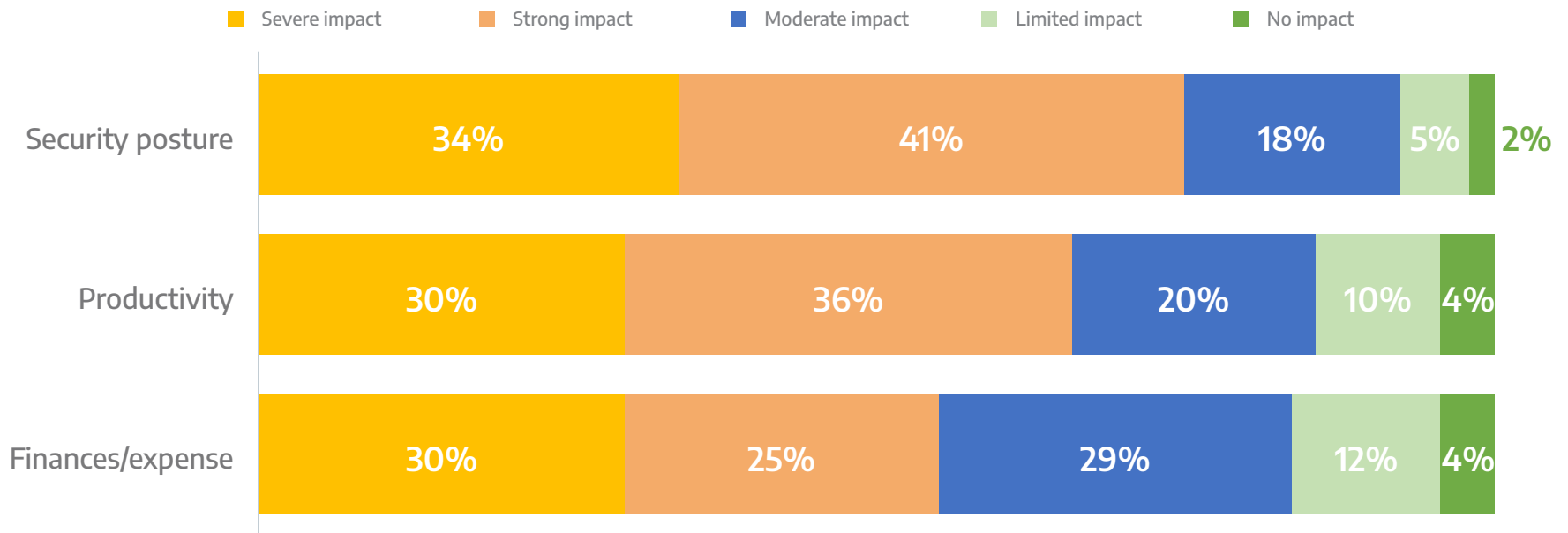
Question 2a: Has your organization ever experienced data loss attributed to any of the following?
Question 2b: Which of these data loss incidents occurred within the past 12 months?

Base 100

# THREE-QUARTERS (75%) OF THOSE WHO HAVE EXPERIENCED DATA LOSS REPORT A STRONG TO SEVERE IMPACT ON OVERALL SECURITY POSTURE

## Impact of data loss on organization
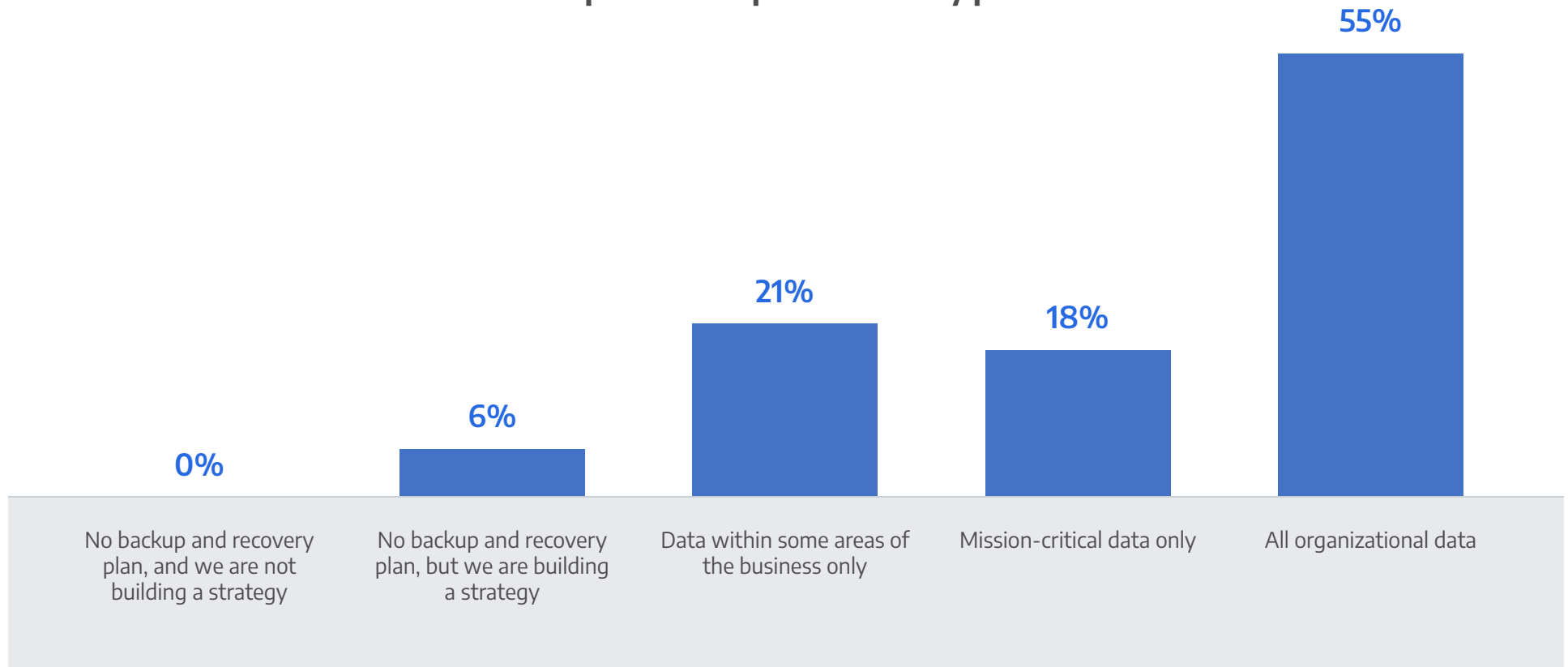*(Among those who have experienced data loss)*

■ Severe impact   ■ Strong impact   ■ Moderate impact   ■ Limited impact   ■ No impact

| | Severe impact | Strong impact | Moderate impact | Limited impact | No impact |
|---|---|---|---|---|---|
| Security posture | 34% | 41% | 18% | 5% | 2% |
| Productivity | 30% | 36% | 20% | 10% | 4% |
| Finances/expense | 30% | 25% | 29% | 12% | 4% |

Question 3: How has data loss impacted the following at your organization?

Base 91 Those who have experienced data loss.

Connection — we solve IT   FOUNDRY   |   BACKUP AND RECOVERY

# 55% ARE BACKING UP ALL ORGANIZATIONAL DATA

## Scope of backup and recovery plan



| No backup and recovery plan, and we are not building a strategy | No backup and recovery plan, but we are building a strategy | Data within some areas of the business only | Mission-critical data only | All organizational data |
|---|---|---|---|---|
| 0% | 6% | 21% | 18% | 55% |

Question 4: What is the scope of your organization's backup and recovery plan?

Base 100

Connection we solve IT® · FOUNDRY | BACKUP AND RECOVERY

# 93% OF THOSE WITH A BACKUP AND RECOVERY PLAN ARE USING CLOUD OR HYBRID STORAGE FOR BACKUP DATA

## How is your backup data stored?
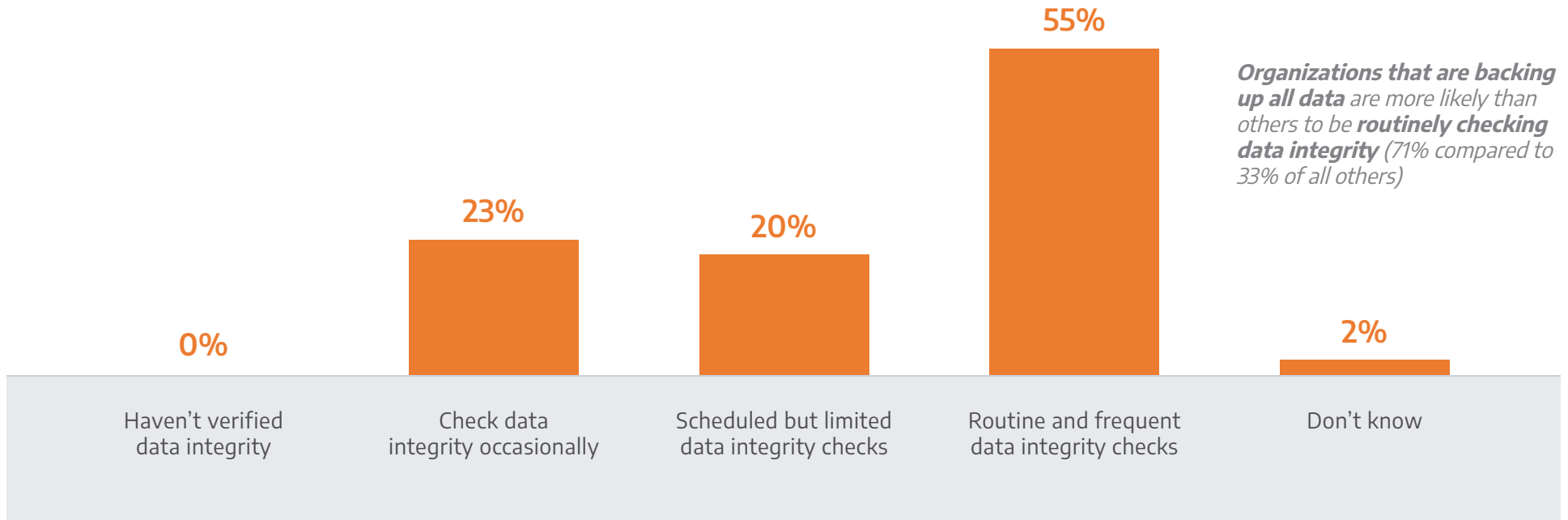### (Among those with a backup and recovery plan)



| Local backup data storage | Cloud (or other non-local) backup data storage | Hybrid backup data storage |
|---|---|---|
| 7% | 44% | 49% |
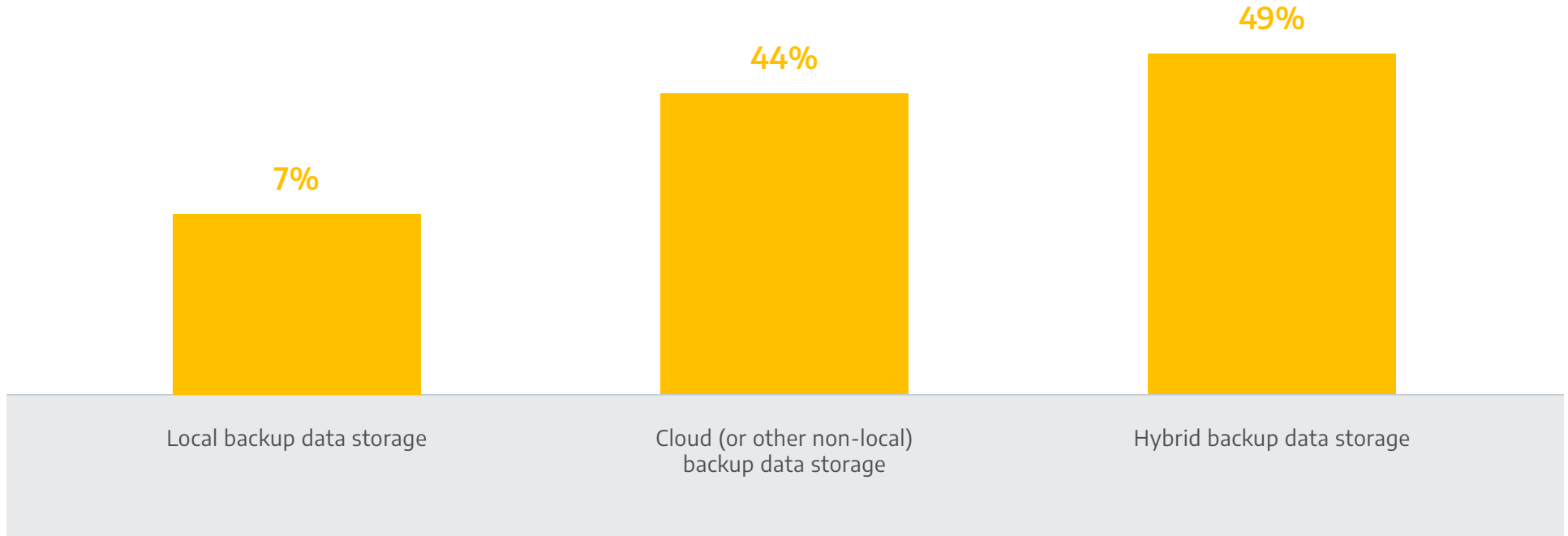
Question 5: How is your backup data stored?

Base 94 Those who have a backup and recovery plan.

Connection we solve IT® | FOUNDRY | BACKUP AND RECOVERY

# 55% OF THOSE WITH A BACKUP AND RECOVERY PLAN ARE CONDUCTING ROUTINE AND FREQUENT DATA INTEGRITY CHECKS

## How often do you test the integrity of your backup data?
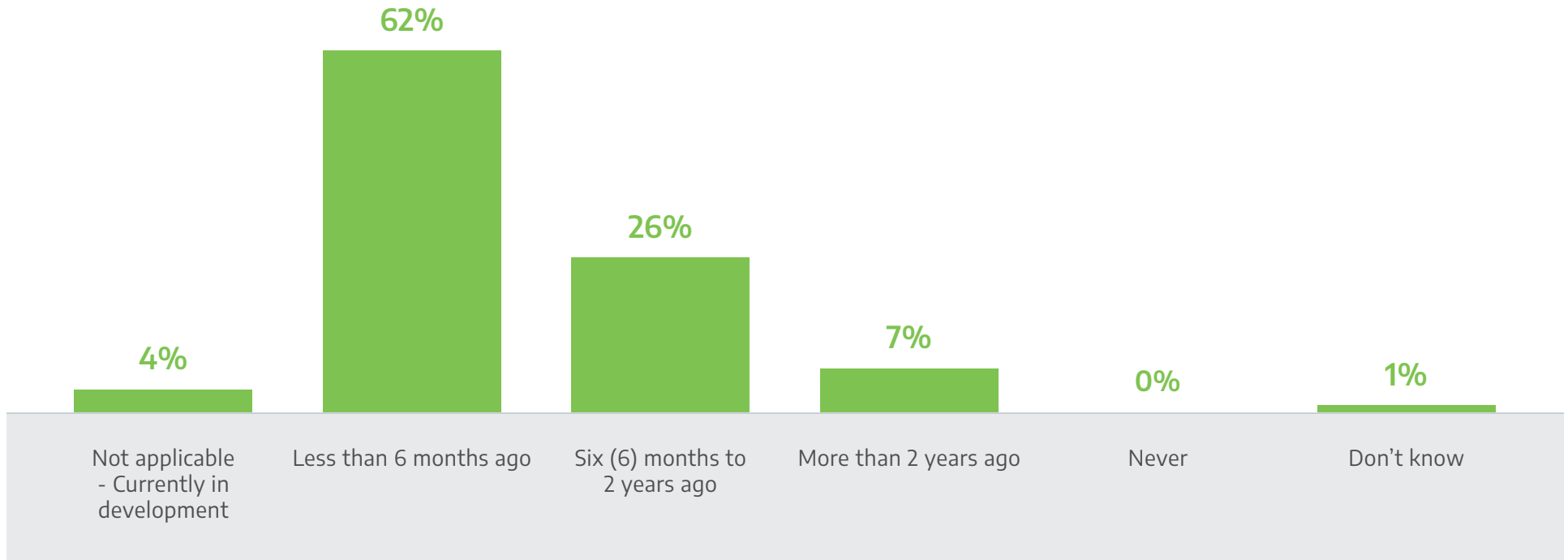### (Among those with a backup and recovery plan)



| Haven't verified data integrity | Check data integrity occasionally | Scheduled but limited data integrity checks | Routine and frequent data integrity checks | Don't know |
|---|---|---|---|---|
| 0% | 23% | 20% | 55% | 2% |

*Organizations that are backing up all data are more likely than others to be routinely checking data integrity (71% compared to 33% of all others)*

Question 6: How often do you test the integrity of your backup data?

Base 94 Those who have a backup and recovery plan.

Connection we solve IT  FOUNDRY

# 33% HAVE NOT EVALUATED THEIR BACKUP AND RECOVERY STRATEGY IN THE PAST 6 MONTHS

**When was your backup and recovery strategy last evaluated to ensure your business-critical data stays protected?**
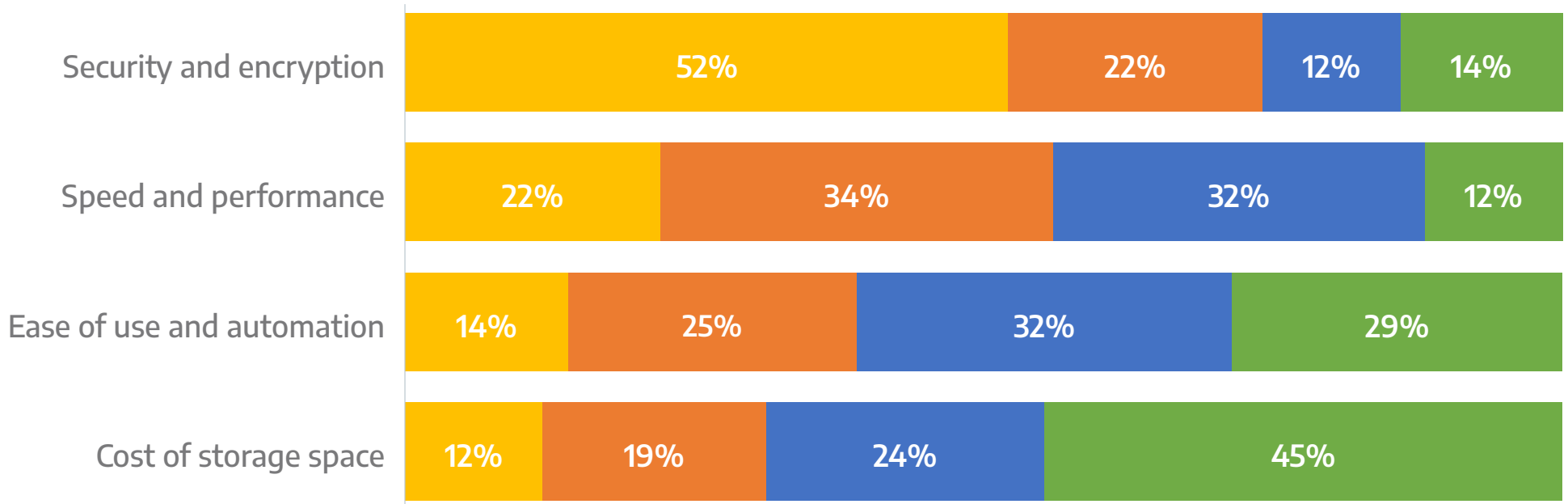


| Not applicable - Currently in development | Less than 6 months ago | Six (6) months to 2 years ago | More than 2 years ago | Never | Don't know |
|---|---|---|---|---|---|
| 4% | 62% | 26% | 7% | 0% | 1% |

Question 7: When was your backup and recovery strategy last evaluated to ensure your business-critical data stays protected?

Base 100

Connection
we solve IT

FOUNDRY

# SECURITY AND ENCRYPTION IS RATED AS THE MOST IMPORTANT FACTOR WHEN CHOOSING A BACKUP SERVICE OR SOFTWARE

**What are the most important factors for your organization when choosing a backup service or software?**

Legend: 1st Most Important | 2nd Most Important | 3rd Most Important | Least Important

| Factor | 1st Most Important | 2nd Most Important | 3rd Most Important | Least Important |
|---|---|---|---|---|
| Security and encryption | 52% | 22% | 12% | 14% |
| Speed and performance | 22% | 34% | 32% | 12% |
| Ease of use and automation | 14% | 25% | 32% | 29% |
| Cost of storage space | 12% | 19% | 24% | 45% |

Question 8: What are the most important factors for your organization when choosing a backup service or software? Rank the following choices from most important (1) to least important (4).

Base 100

# CONTACT YOUR CONNECTION ACCOUNT TEAM TODAY FOR MORE INSIGHTS INTO THESE RESULTS.

**Connection®**
we solve IT®

1.800.800.0014
www.connection.com

# Connection®

## we solve IT®

1.800.800.0014  ■  www.connection.com