# PROTECTING OT SYSTEMS

A MarketPulse Survey for Connection

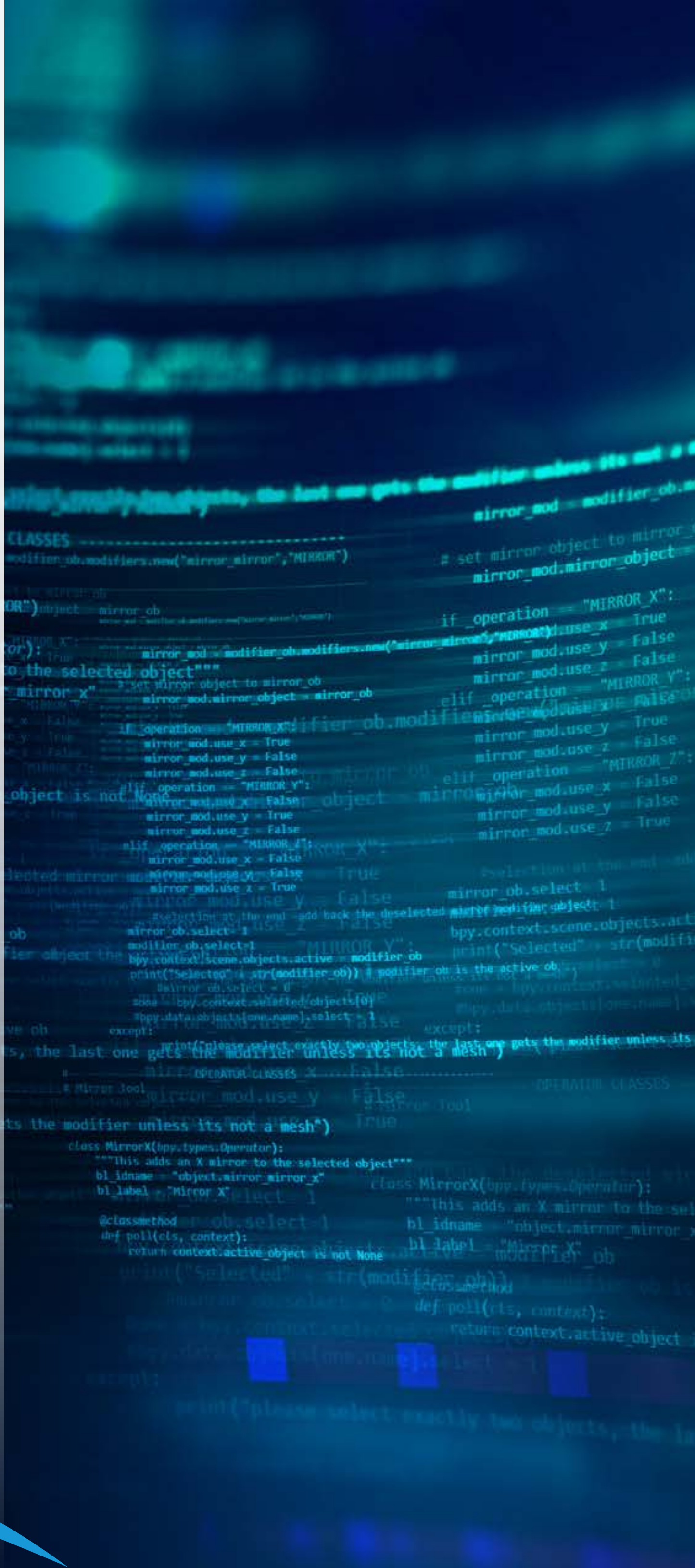
DECEMBER 2022

Connection®
we solve IT®

In Partnership With:

FOUNDRY® NETWORKS

# CONTENTS



# INTRODUCTION

Managing your operational technology (OT) ecosystem isn't always a simple task. From integration with new and upcoming trends to optimizing automation, there are several facets and nuances for any single organization to consider—regardless of vertical. Connection partnered with Foundry to deliver this peer-level review of the information you need to know when taking a fresh look at your environment.

# METHOD AND OBJECTIVES

## Survey Goals

This survey was conducted among U.S. manufacturing organizations to understand how they are protecting OT systems.

We evaluate the biggest cybersecurity risk factors within OT environments today—as well as technologies, tools, measures underway, and plans to mitigate security risk—and the most concerning potential impacts of a cybersecurity event on the business.

### Total Respondents:

100

### Collection Method:

Online questionnaire

### Geography:

U.S.

### Field Dates:

November 22–December 5, 2022

### Number of Questions:

8 (Excluding profiling questions)

### Average Company Size:

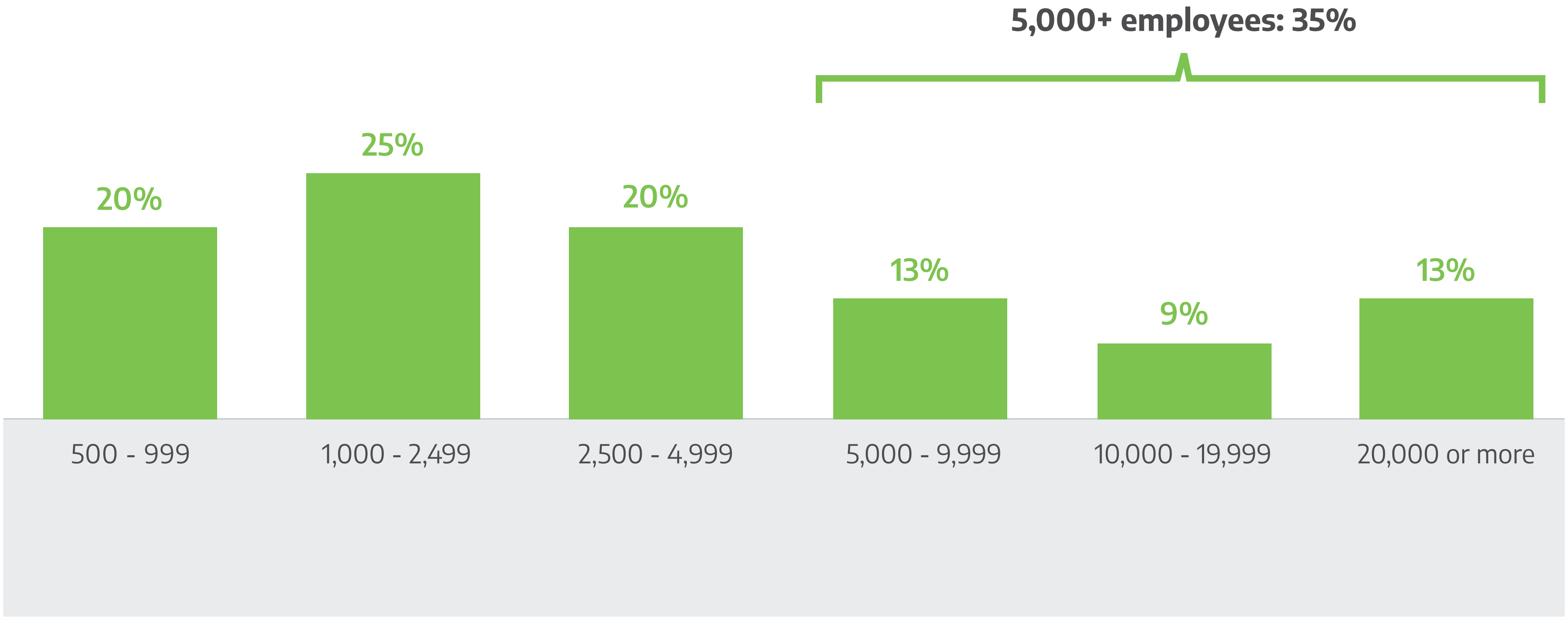
6262 employees

### Senior Decision-makers:

Respondents are senior decision makers employed in I.T., Operations, Production, Cybersecurity, and Executive management roles (Director and above titles and Engineers).

# RESPONDENT PROFILE

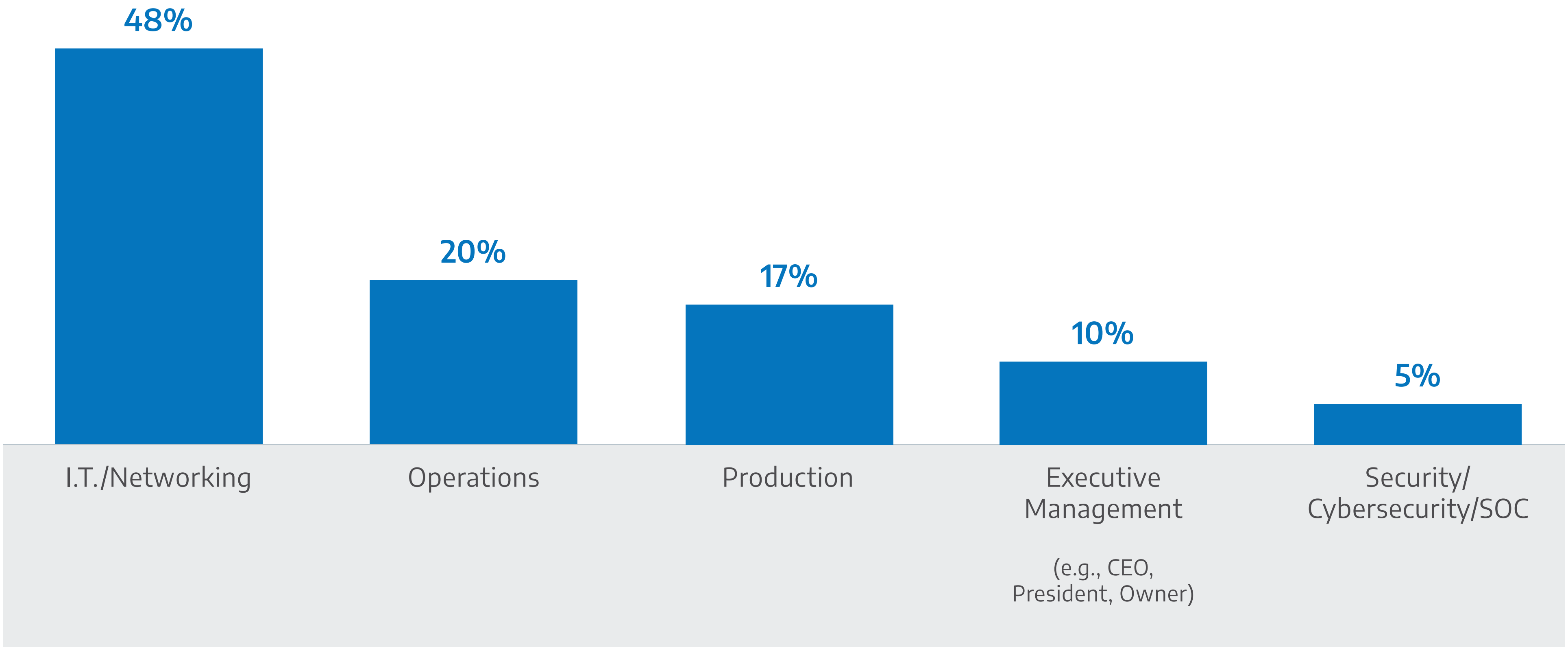
# COMPANY SIZE BY NUMBER OF EMPLOYEES



Question S3: Approximately how many people are employed in your entire organization or enterprise?
(Please include all plants, divisions, branches, parents, and subsidiaries worldwide.)

Base 100

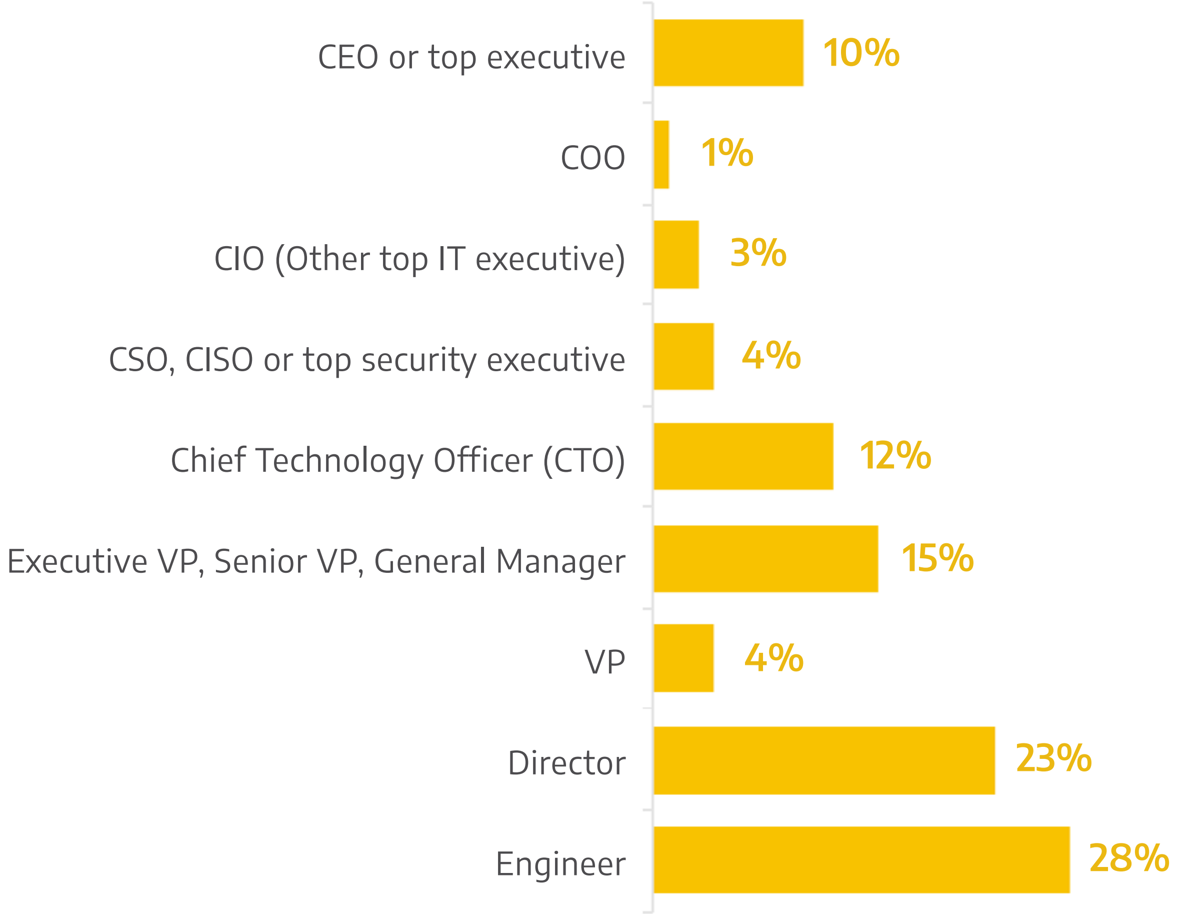
# PRIMARY ROLE



Question S4: With what functional area is your role most closely aligned?

Base 100

# JOB TITLES



Question S5. What is your primary job title?

Base 100

# EXECUTIVE SUMMARY

# HIGHLIGHTED FINDINGS

- **I.T. and operations teams typically hold primary responsibility for technology purchases to protect the OT environment** (51% report the I.T. team is primarily responsible, while 29% name the operations team, 10% indicate the production team and 9% cite the SOC/SIEM/security team).
- **I.T. is primarily responsible for day-to-day security in the OT environment** (60% indicate I.T. is responsible, vs. 19% indicating the SOC/SIEM/security team, 14% citing the operations team and 7% indicating the production team).
- **Lack of security awareness or training among users (44%) is considered the biggest cybersecurity risk factor within the OT environment.** More than one-third are concerned about technology that doesn't meet security requirements (37%), personal devices connecting to factory resources (36%), and/or users bypassing security controls (34%).
- **Six in ten (60%) report their organizations have experienced one or more successful cybersecurity attacks in the past 12 months** (13% indicate experience with multiple attacks).
- **Least privilege access (31% considering), virtual patching (29%), and industrial deep packet inspection (29%) are the top tools under consideration over the next 12 months to minimize OT security risk.** More than two-thirds indicate their organizations are already leveraging integrated threat monitoring (76%), endpoint firewalls (72%), and/or protocol management (69%).
- **As key measures to mitigate security risk, organizations are likely to be automating OT security functions** (35% underway, 13% planning), **seeking outside security assessments** (32% underway, 9% planning), **and/or deploying backup plans for OT systems** (29% underway, 12% planning) **over the next 12 months.**

# HIGHLIGHTED FINDINGS (CONTINUED)

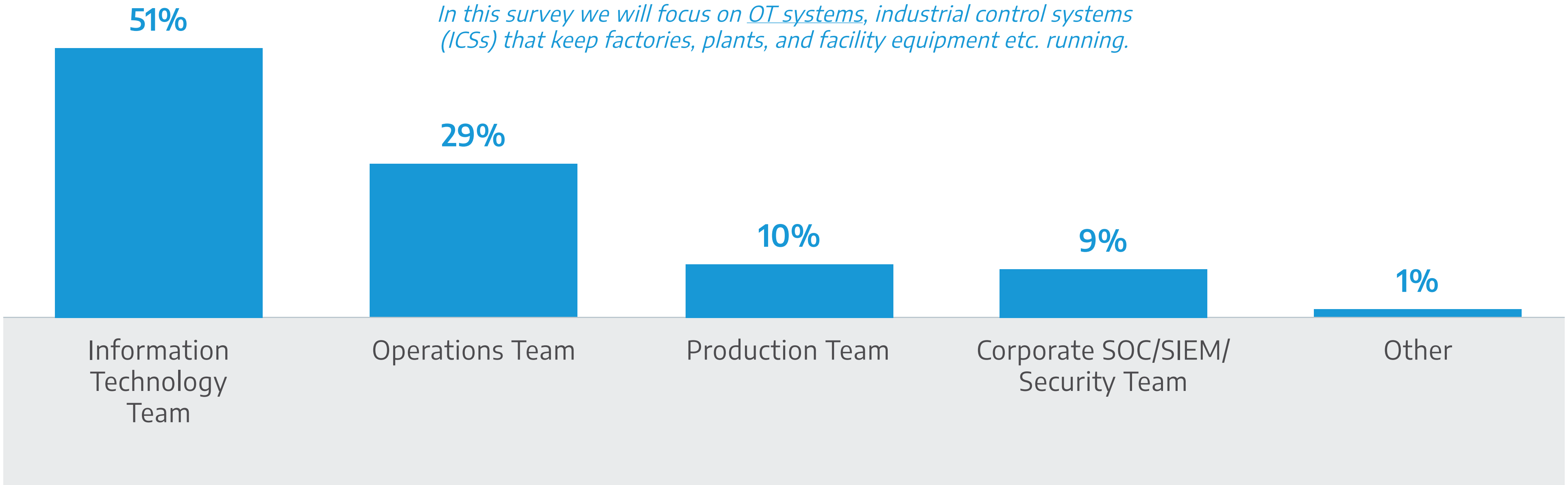
- **Nearly two-thirds (65%) report their organizations have experienced challenges with cybersecurity insurance.** Top challenges include increasing premiums (41%) and/or limited availability of cybersecurity insurance (30%) due to cybersecurity posture.
- **More than three quarters (77%) perceive the degree of cybersecurity risk posed by OT systems and infrastructure to be moderate to severe** (42% "moderate", 30% "significant", and 5% "severe").
- **Nearly half (49%) consider it likely that a cybersecurity event will impact OT systems and infrastructure over the next 12 months, and another 30% consider it to be a possibility.** Seventy percent (70%) of those in an I.T. role consider a future cybersecurity attack to be likely (compared to 40% of those in other roles).
- **Respondents are most concerned about the potential for financial loss** (27% rank this as their top concern and 71% among their top three) **and/or downtime** (23% rank as number one, and 65% in the top three) **resulting from cybersecurity events.**

# SURVEY RESULTS

# I.T. AND OPERATIONS TEAMS TYPICALLY HOLD PRIMARY RESPONSIBILITY FOR TECHNOLOGY PURCHASES TO PROTECT THE OT ENVIRONMENT

**Primary responsibility for making technology purchase decisions to protect OT systems and infrastructure:**

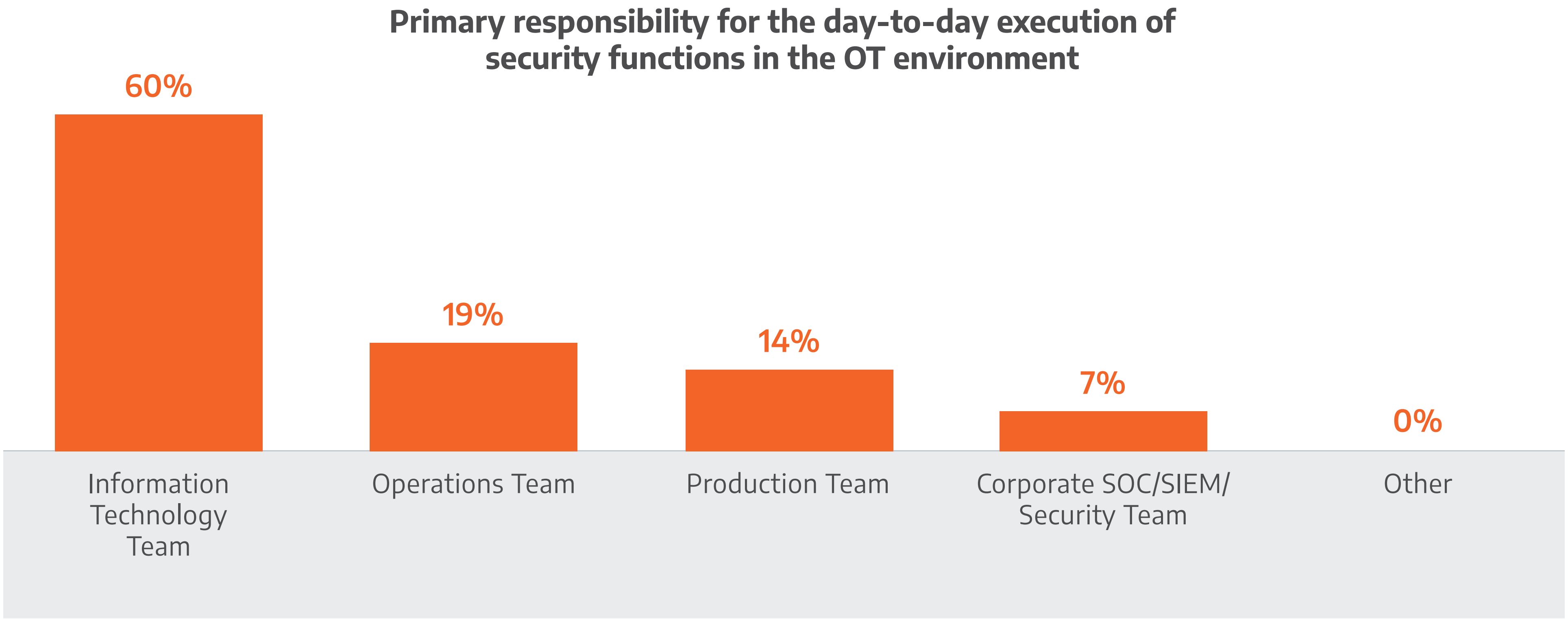
*In this survey we will focus on OT systems, industrial control systems (ICSs) that keep factories, plants, and facility equipment etc. running.*



Question 1A: Who is primarily responsible for making technology purchase decisions to protect OT systems and infrastructure at your organization?

Base 100

# I.T. IS PRIMARILY RESPONSIBLE FOR DAY-TO-DAY SECURITY IN THE OT ENVIRONMENT

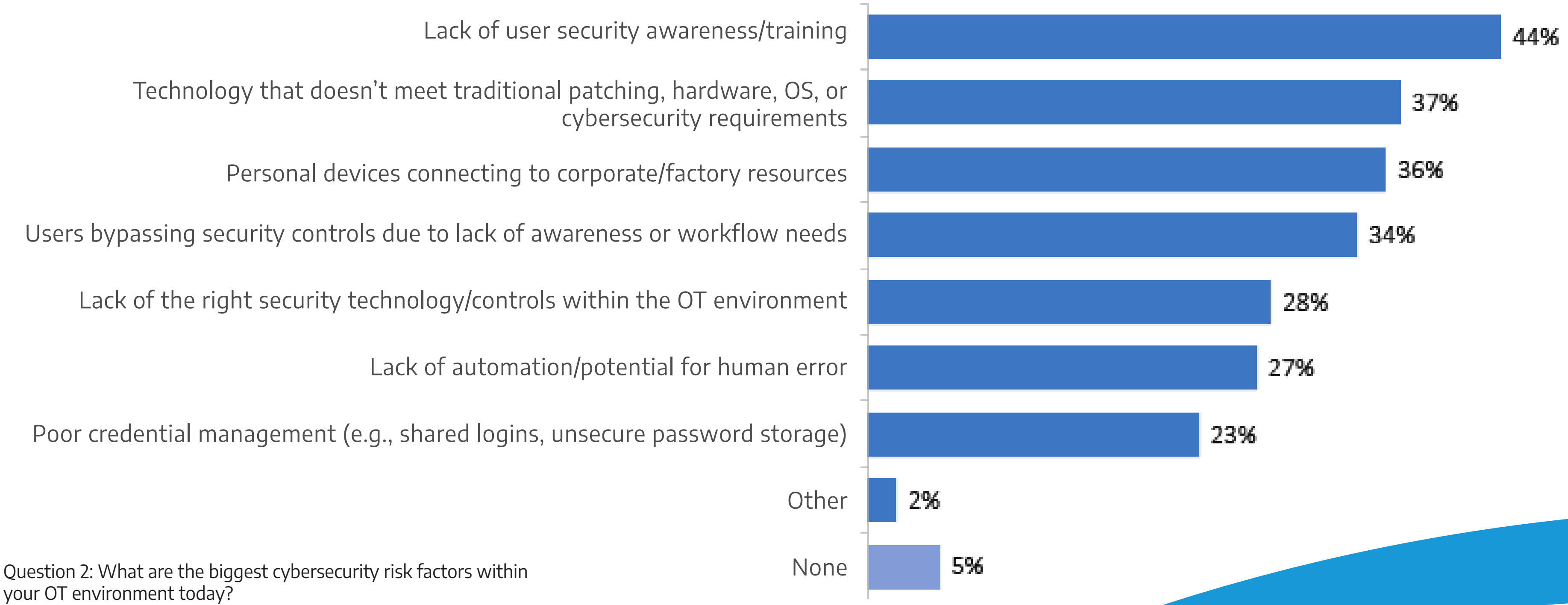


Question 1B: Who is primarily responsible for the day-to-day execution of security functions (e.g., end point protection, patching, network security, etc.) within the OT environment?

Base 100

# LACK OF SECURITY AWARENESS OR TRAINING AMONG USERS IS CONSIDERED THE BIGGEST CYBERSECURITY RISK FACTOR WITHIN THE OT ENVIRONMENT

## Biggest cybersecurity risk factors within OT environment (select 3)



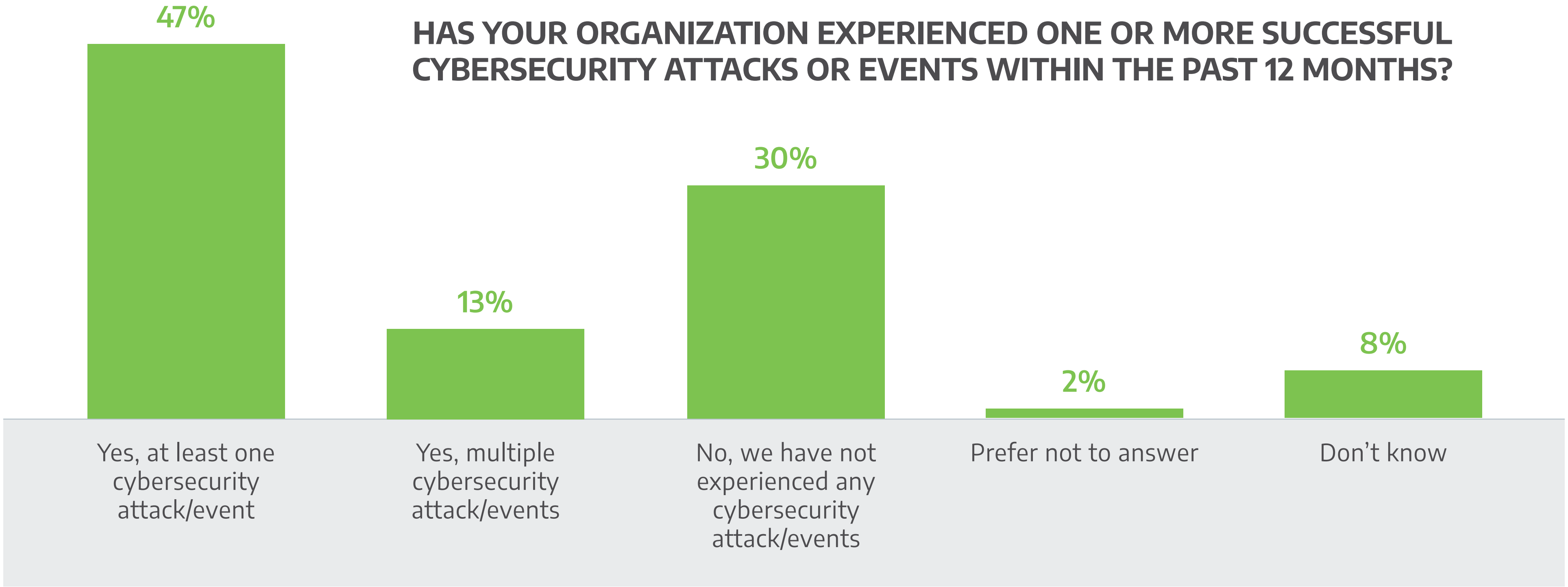
Question 2: What are the biggest cybersecurity risk factors within your OT environment today?

Base 100

# 60%

report their organizations have experienced one or more successful cybersecurity attacks in the past 12 months

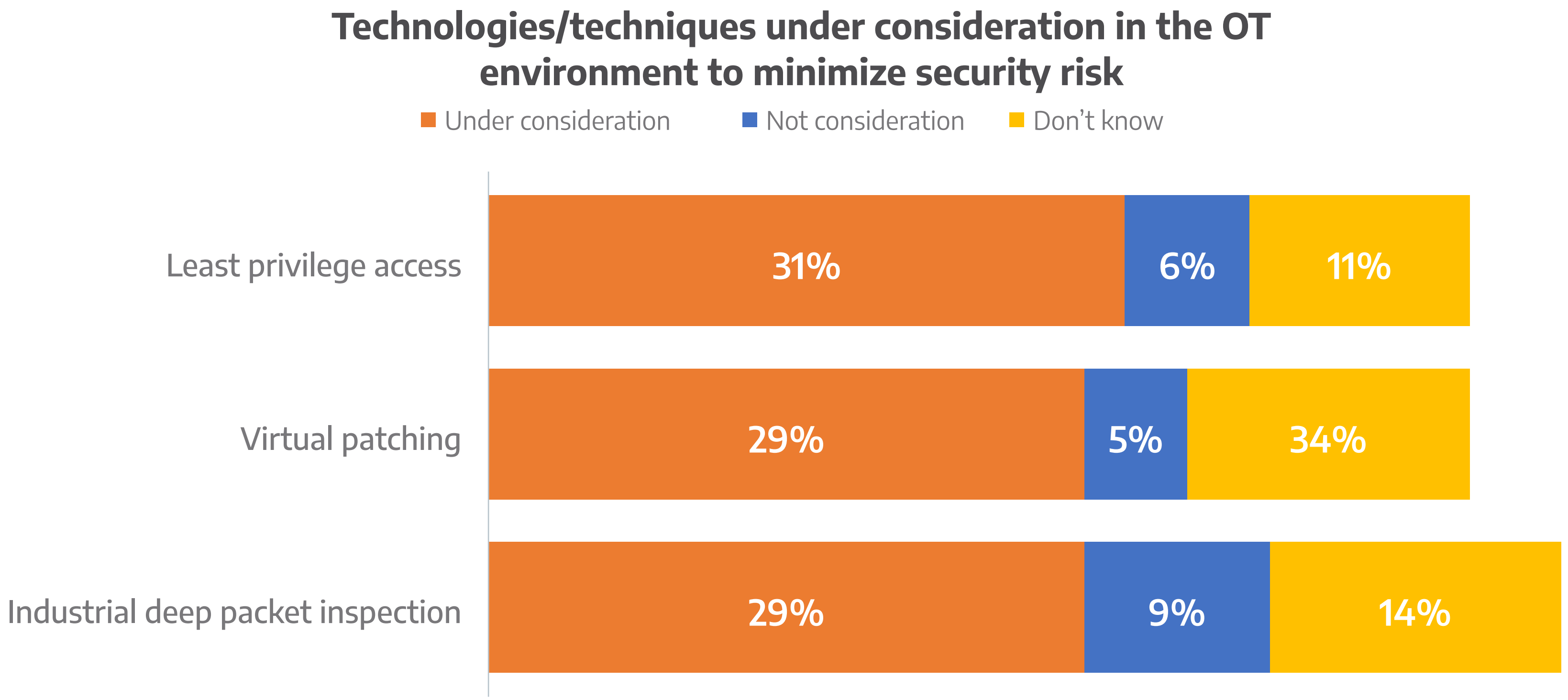
## HAS YOUR ORGANIZATION EXPERIENCED ONE OR MORE SUCCESSFUL CYBERSECURITY ATTACKS OR EVENTS WITHIN THE PAST 12 MONTHS?



Question 1B: Who is primarily responsible for the day-to-day execution of security functions (e.g., end point protection, patching, network security, etc.) within the OT environment?

Base 100

# LEAST PRIVILEGE ACCESS, VIRTUAL PATCHING, AND INDUSTRIAL DEEP PACKET INSPECTION ARE THE TOP TOOLS UNDER CONSIDERATION TO MINIMIZE OT SECURITY RISK



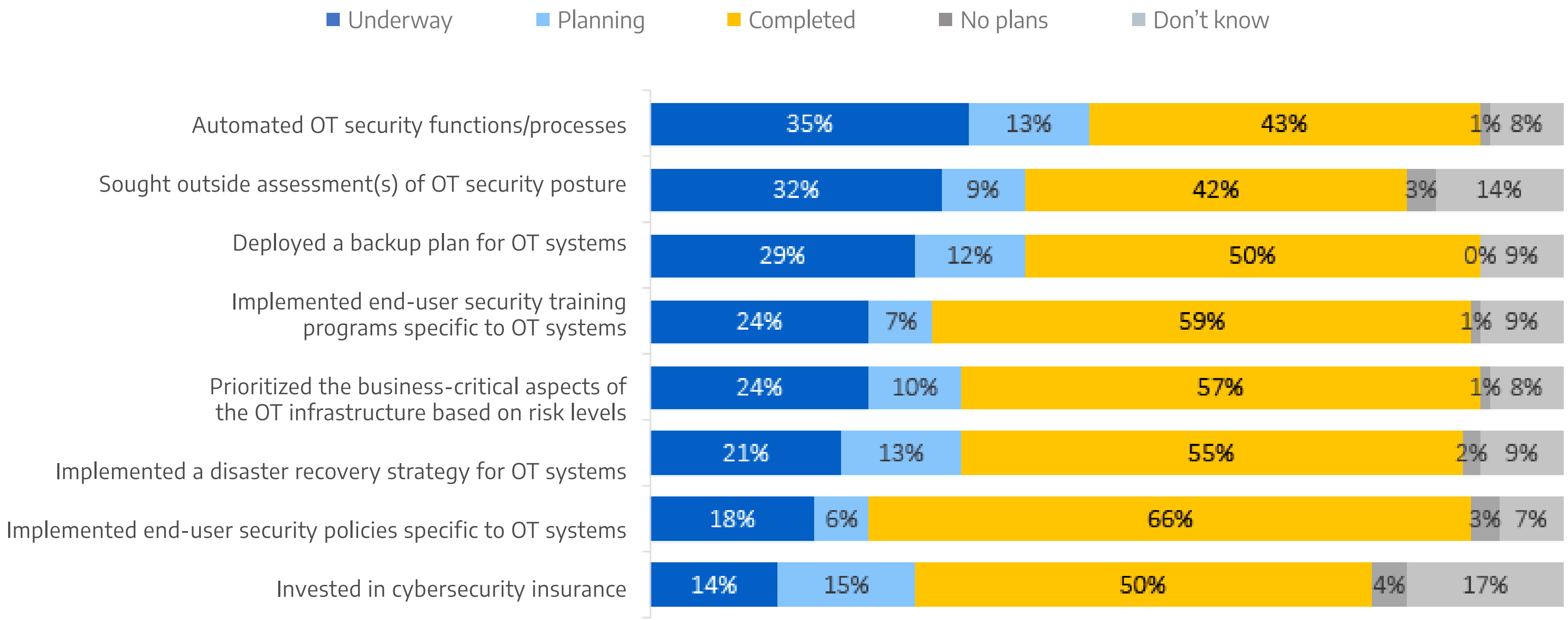
Question 4: What technologies/techniques are in place or under consideration within your OT environment over the next 12 months to minimize the likelihood of a cybersecurity event?

Base 100

# OT SECURITY RISKS

## AS KEY MEASURES TO MITIGATE SECURITY RISK, ORGANIZATIONS ARE LIKELY TO BE AUTOMATING OT SECURITY FUNCTIONS, SEEKING OUTSIDE SECURITY ASSESSMENTS, AND/OR DEPLOYING BACKUP PLANS FOR OT SYSTEMS

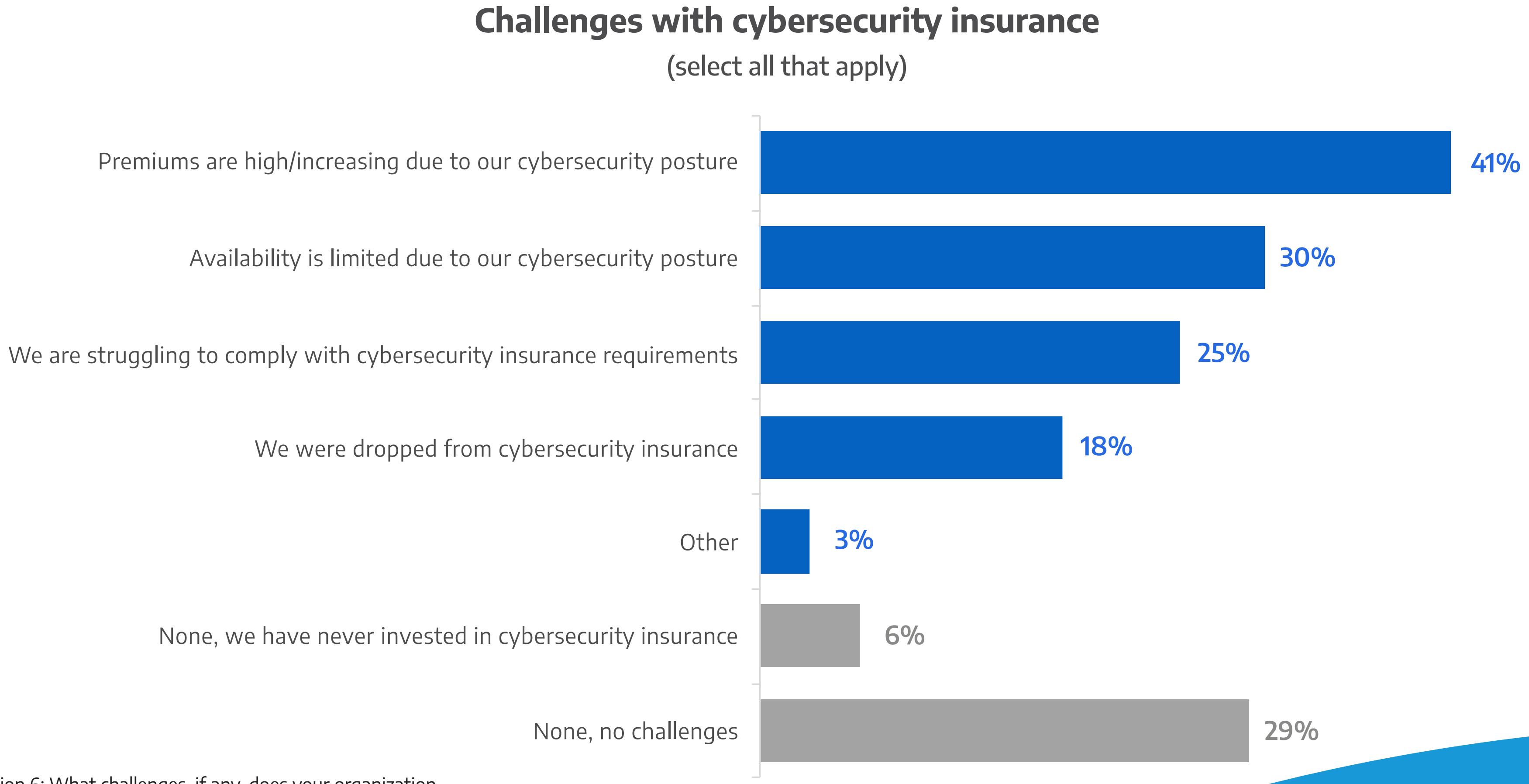
### Measures underway or planned to identify and mitigate OT security risk



Question 5: Which of the following measures has your company taken or are you planning over the next 12 months to identify and mitigate security risk within your OT environment?

Base 100

# NEARLY TWO-THIRDS (65%) REPORT THEIR ORGANIZATIONS HAVE EXPERIENCED CHALLENGES WITH CYBERSECURITY INSURANCE



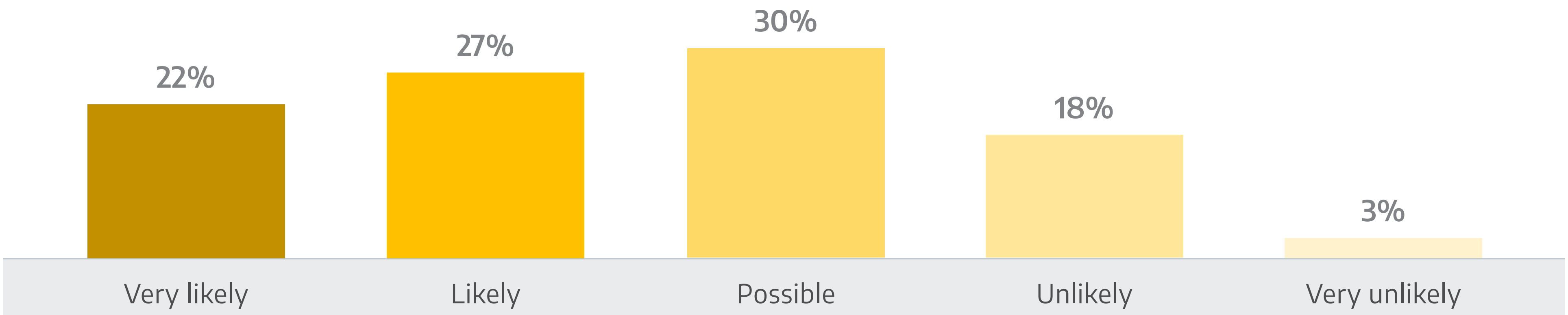
Question 6: What challenges, if any, does your organization face with respect to cybersecurity insurance?

Base 100

# 49%

consider it likely that a cybersecurity event will impact OT systems and infrastructure over the next 12 months.

## Likelihood Of A Cybersecurity Event Impacting The OT Environment Over The Next 12 Months



*70% of those in an I.T. role consider a future cybersecurity attack to be likely (compared to 40% of those in other roles).*

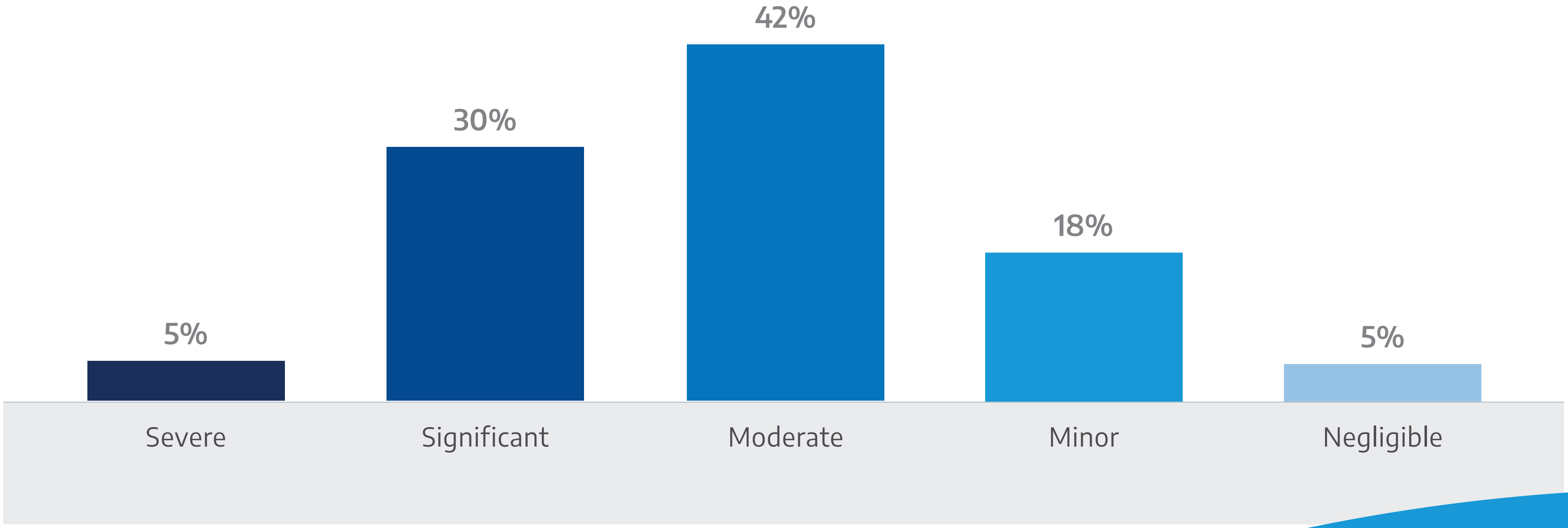
Question 7: How valuable would the following third-party services be for your organization in helping to support your application environment?

Base 100

# 77%

perceive the degree of cybersecurity risk posed by OT systems and infrastructure to be moderate to severe

## IN YOUR OPINION, WHAT IS THE DEGREE OF CYBERSECURITY RISK PRESENTED BY OT SYSTEMS AND INFRASTRUCTURE AT YOUR ORGANIZATION?

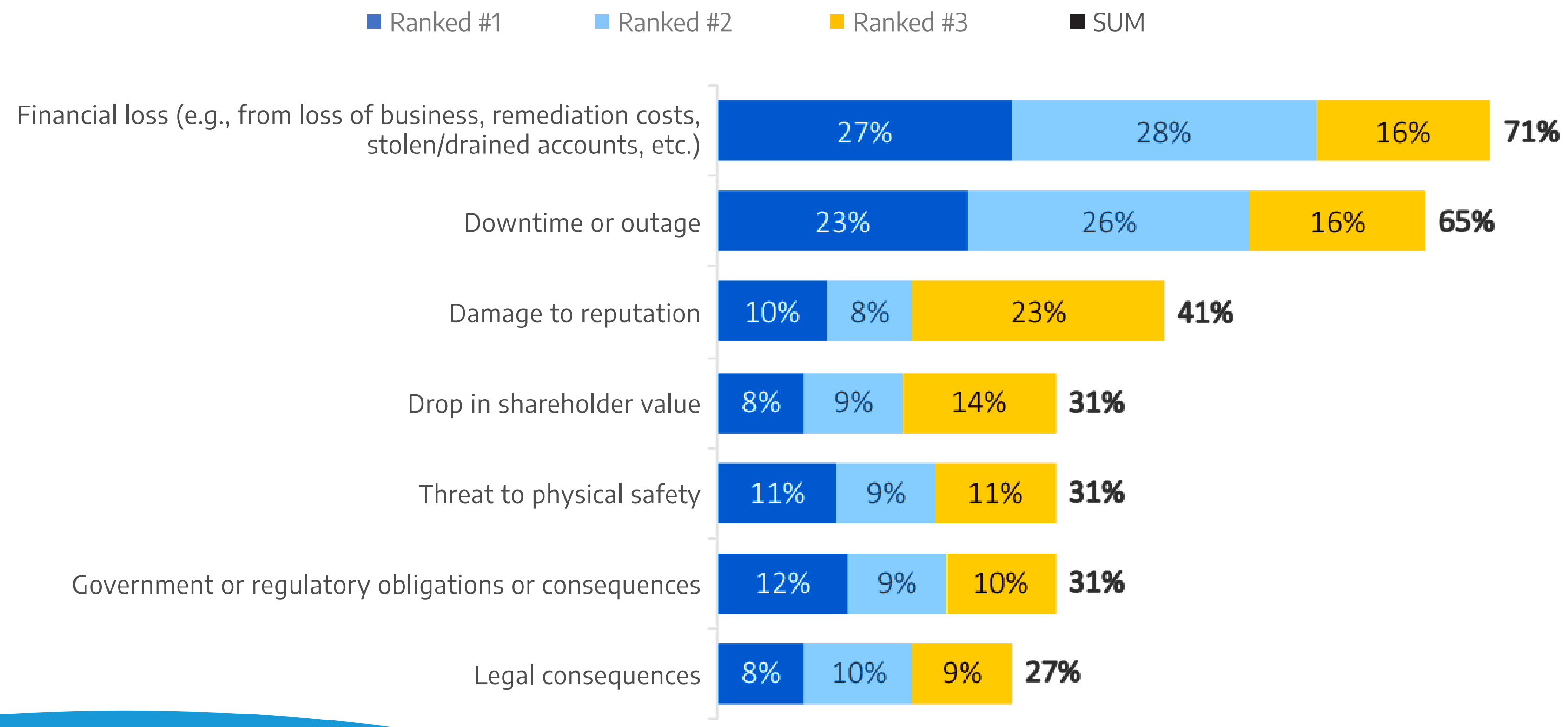


Question 7B: In your opinion, what is the degree of cybersecurity risk presented by OT systems and infrastructure at your organization? Please consider the potential business impact of a cybersecurity event within your OT environment.

Base 100

# PERCEIVED ADVANTAGES OF THIRD-PARTY APPLICATION SUPPORT SERVICES VARY BY TYPE OF APPLICATION ENVIRONMENT

## Top concerns regarding the potential business impact of a cybersecurity event



Question 8: What are your top concerns regarding the potential impact of a cybersecurity event on your business? Select the top three and rank in order from highest (1) to lowest (3) concern.

Base 100

# AMONG COMPANIES WITH 2,500 EMPLOYEES OR MORE:

- There is a **higher likelihood** compared to those at smaller enterprises (1,000-2,499 employees) that they are in the aerospace and defense (15% vs. 2%) or medical devices (11% vs. 0%) subsectors.
- Respondents at large organizations are **more likely to report they don't know if their organization has experienced one or more successful cybersecurity events** in the past 12 months (15% vs. 0% of other respondents).
- Respondents are **less likely to have the following technologies in place:** proximity-based authentication (47% vs. 67% of smaller enterprises), and least privilege access (44% vs. 62% of others).

# CYBERSECURITY INSURANCE CHALLENGES

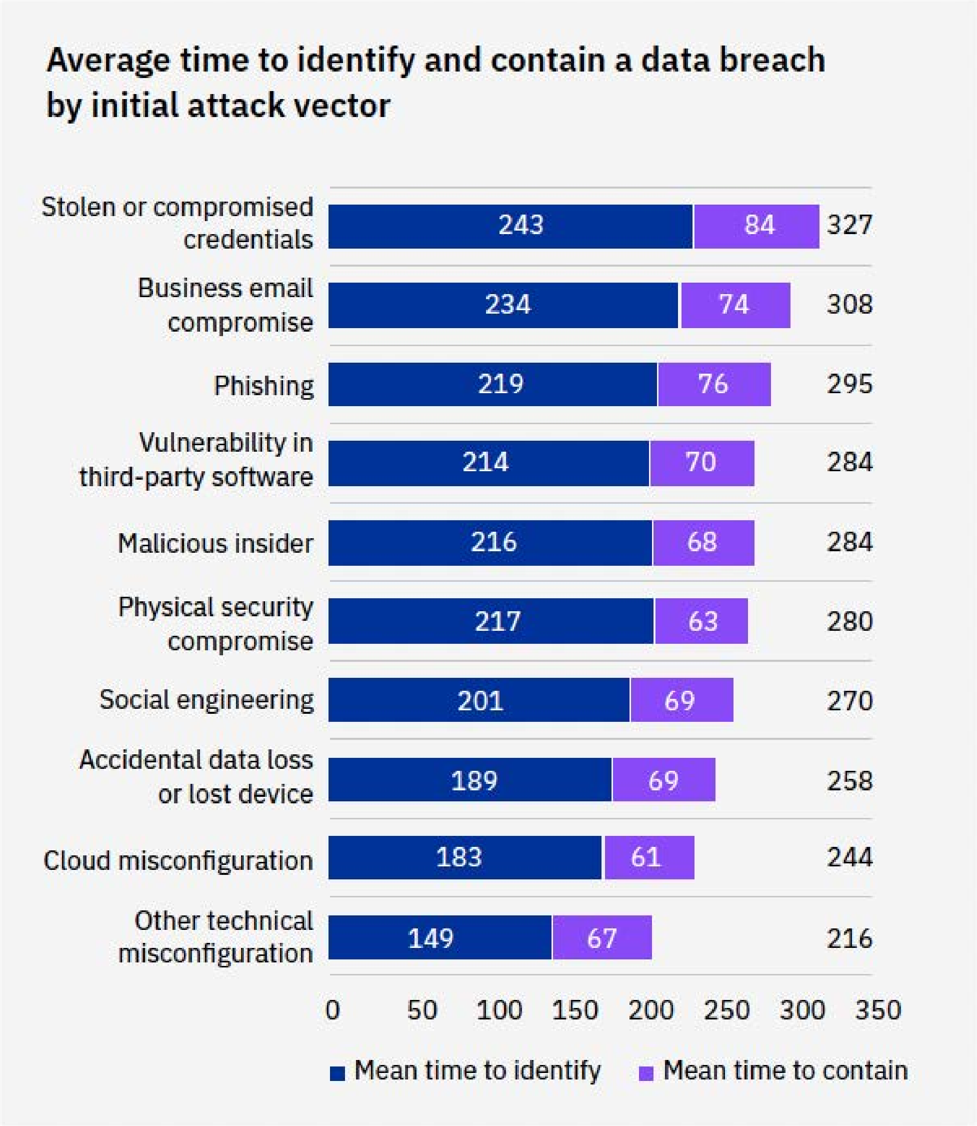
## FIND MORE THAN HALF (57%) REPORT EXPERIENCING HIGH CYBERSECURITY INSURANCE PREMIUMS, LIMITED AVAILABILITY AND/OR DENIAL OF INSURANCE DUE TO SECURITY POSTURE.

### AMONG THOSE EXPERIENCING THESE CHALLENGES:

- There is a **higher likelihood** they are in the automotive/transportation sector (18% compared to 5% of other respondents)
- Respondents are more likely to cite the following as OT cybersecurity risk factors: Lack of user security awareness/training (53% vs. 33% of others), personal devices connecting to corporate/factory resources (44% compared to 26%), lack of the right security technology/controls within the OT environment (37% vs. 16%), poor credential management (32% vs. 12%).
- They are much more likely to report their organization has experienced one or more successful cybersecurity events in the past 12 months (87% vs. 24% of other respondents).
- Respondents are more likely to be considering the following technologies over the next 12 months (not yet in place): industrial deep packet inspection (37% vs. 19%), virtual patching (39% vs. 16%), and proximity-based authentication (37% vs. 14%).
- Respondents are **more likely than others to report their organizations are underway** (not yet completed) with implementing end-user security policies specific to OT systems (28% vs. 5%) and with prioritizing the business-critical aspects of the OT infrastructure based on risk levels (32% vs. 14%).
- Sixty-nine percent (69%) **consider it likely or very likely that their OT systems and infrastructure will be impacted by a future cybersecurity event** in the next 12 months, compared to 23%
  of others.
- Nearly half (49%) **consider the degree of cybersecurity risk presented by OT infrastructure to be significant or severe**, compared to 17% of others.
- Respondents are more **likely to count "government or regulatory obligations or consequences"** among their top concerns regarding the impact of a cybersecurity event on their business (23% vs. 8%).

# FURTHER READING

# TOP BREACH VECTORS

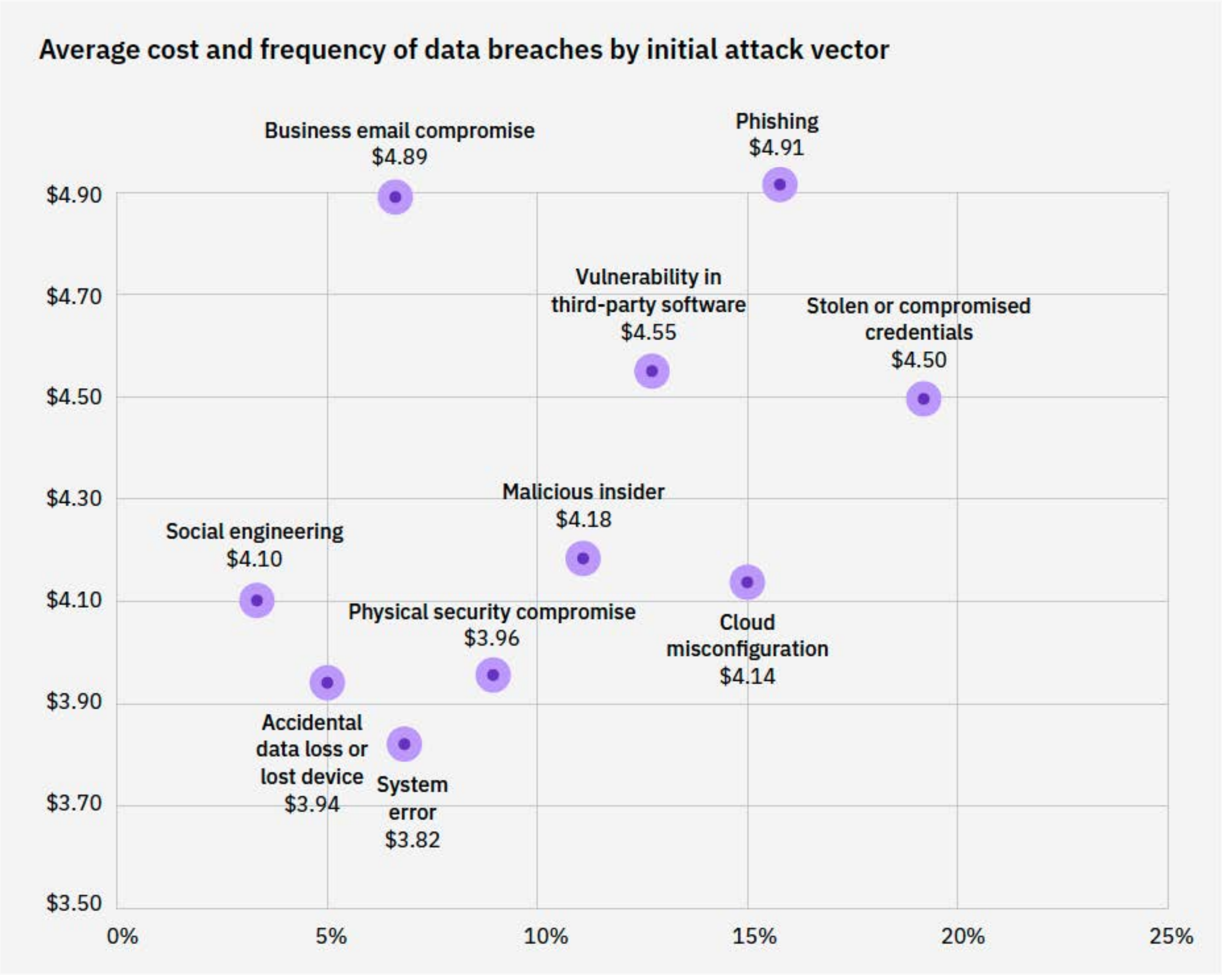


Measured in days

- Use of stolen or compromised credentials remains the most common cause of a data breach.
- These breaches had the longest lifecycle: 243 days to identify and 84 more days to contain.
- Multifactor solutions (including in OT) reduced total breach incident cost by $187k.
- Identity and access management (including in OT) reduced total breach incidents by $225k.

Source: IBM, 2022, Cost of a Data Breach Report 2022

# TOP BREACH VECTORS (CONTINUED)



Measured in USD millions

Source: IBM, 2022, Cost of a Data Breach Report 2022

# CONTACT A CONNECTION ACCOUNT MANAGER TODAY FOR MORE INSIGHT INTO THESE RESULTS.

Connection®
we solve IT

1.800.800.0014
www.connection.com/manufacturing

Connection®

we solve IT®

1.800.800.0014 ■ www.connection.com