INSIDER THREAT

2018 REPORT

Cybersecurity Insiders

Crowd Research Partners

PRESENTED BY: ca technologies

INSIDER THREAT 2018 REPORT

TABLE OF CONTENTS

INTRODUCTION

Today's most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. This survey is designed to uncover the latest trends and challenges regarding insider threats as well as solutions to prevent or mitigate insider attacks.

Our 400,000 member online community, Cybersecurity Insiders, in partnership with the Information Security Community on LinkedIn, asked Crowd Research Partners to conduct an in-depth study of cybersecurity professionals to gather fresh insights, reveal the latest trends, and provide actionable guidance on addressing insider threat.

The resulting Insider Threat Report is the most comprehensive research on the topic to date, revealing how IT and security professionals are dealing with risky insiders and how organizations are preparing to better protect their critical data and IT infrastructure.

We would like to thank CA Technologies for supporting this research.

In addition, we want to thank all survey participants who provided their time and input in support of this study.

We hope you will enjoy reading this report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity Insiders

✉ Holger.Schulze@Cybersecurity-Insiders.com

KEY SURVEY FINDINGS

1 Ninety percent of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).

2 A majority of 53% confirmed insider attacks against their organization in the previous 12 months (typically less than five attacks). Twenty-seven percent of organizations say insider attacks have become more frequent.

3 Organizations are shifting their focus on detection of insider threats (64%), followed by deterrence methods (58%) and analysis and post breach forensics (49%). The use of user behavior monitoring is accelerating; 94% of organizations deploy some method of monitoring users and 93% monitor access to sensitive data.

4 The most popular technologies to deter insider threats are Data Loss Prevention (DLP), encryption, and identity and access management solutions. To better detect active insider threats, companies deploy Intrusion Detection and Prevention (IDS), log management and SIEM platforms.

5 The vast majority (86%) of organizations already have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.

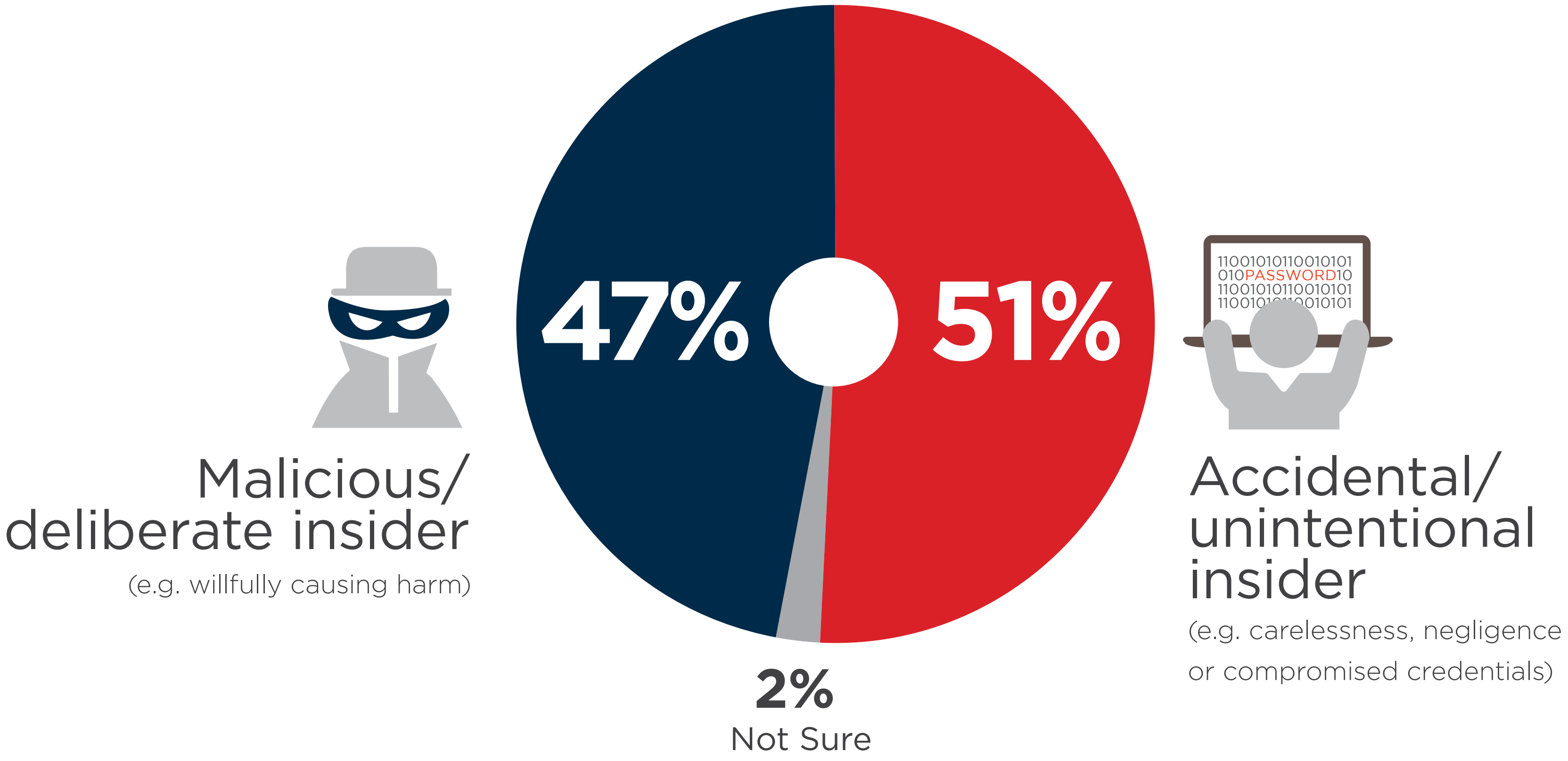
INSIDER THREAT

NATURE OF INSIDER THREATS

Too often, people associate the term "Insider Threats" in cybersecurity with malicious employees intending to directly harm the company through theft or sabotage. In truth, negligent employees or contractors unintentionally cause an equally high number of security breaches and leaks by accident.

In this year's survey, companies are equally worried about accidental/unintentional data breaches (51%) through user carelessness, negligence or compromised credentials as they are from deliberate malicious insiders (47%).

What type of insider threats are you most concerned about?



RISKY INSIDERS

Security professionals have a unique responsibility to detect, counter and respond to cyber attacks. This job becomes increasingly more challenging when threats come from within the organization from trusted and authorized users. It is often difficult to determine when users are simply doing their job function or something illegal or unethical.

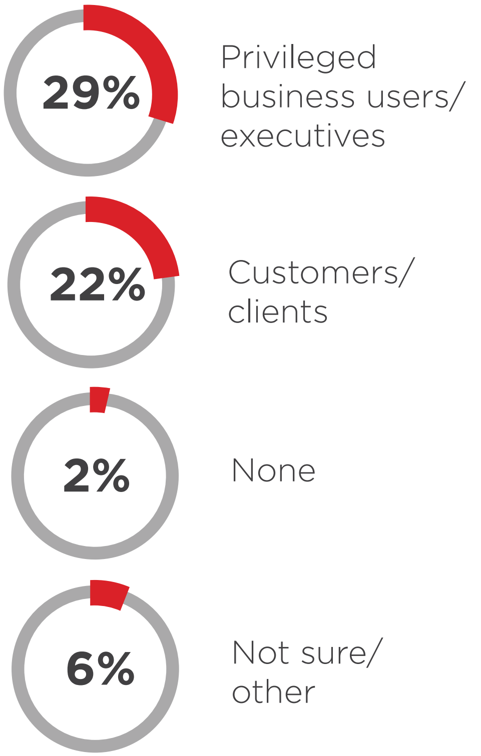
The survey indicated both regular employees (56%) and privileged IT users (55%) pose the biggest insider security risk to organizations, followed by contractors (42%).

What type(s) of insiders pose the biggest security risk to organizations?*

56%
Regular employees

55%
Privileged IT users/admins

42%
Contractors/service providers/ temporary workers



*Multi-response questions do not add up to 100%

MOST VULNERABLE DATA

Data is no longer just an IT asset; it's a core strategic asset, and some types of data are more valuable than others. Confidential business information, which encompasses company financials along with customer and employee data, is a highly strategic asset and equally a high-value target. Again this year, confidential business information (57%) takes the top spot as most vulnerable to insider attacks, followed by privileged account information (52%), and sensitive personal information (49%.

What type(s) of data are most vulnerable to insider attacks?

57% Confidential business information
(Financials, customer data, employee data)

52% Privileged account information
(Credentials, passwords, etc.)

49% Sensitive personal information
(PII/PHI)

32% Intellectual property
(Trade secrets, research product designs)

31% Employee data
(HR)

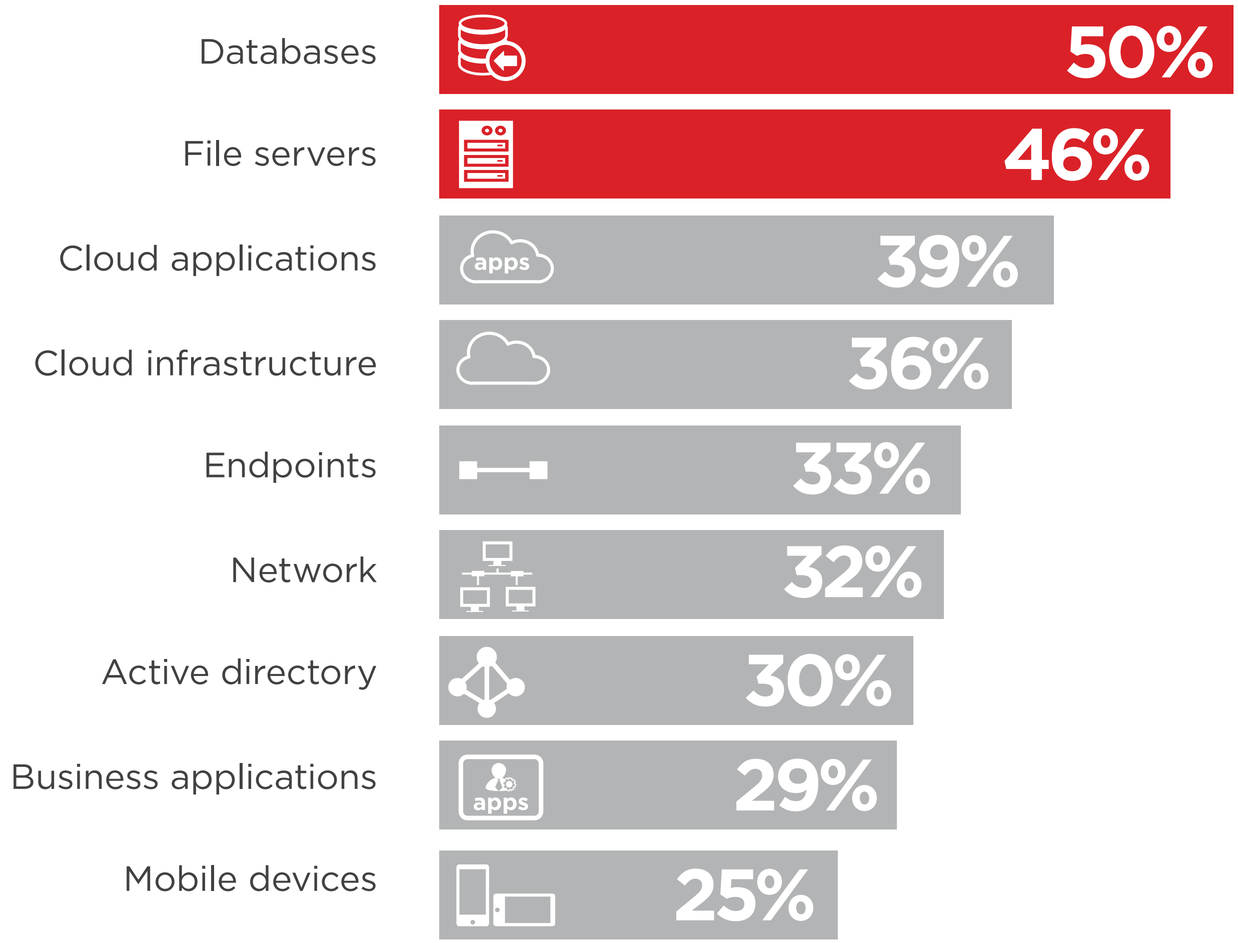
27% Operational/ infrastructure data
(Network, infrastructure controls)

Not sure / Other 1%

IT ASSETS AT RISK

Cybercriminals see a greater opportunity in targeting where corporate data is located in volume. Databases (50%) and corporate file servers (46%) pose the highest risk. In this year's survey, mobile devices are perceived as a lesser target and least vulnerable (25%).

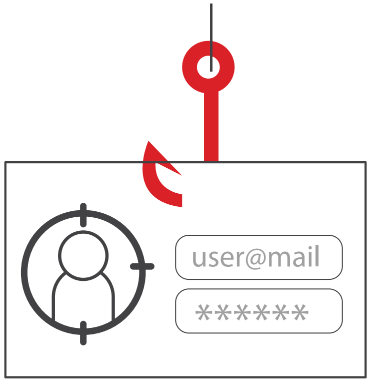
What IT assets are most vulnerable to insider attacks?



ACCIDENTAL INSIDERS

The most common culprit of insider threat is accidental exposure by employees. Cybersecurity experts view phishing attempts (67%) as the biggest vulnerability for accidental insider threats. Phishing attacks trick employees into sharing sensitive company information by posing as a legitimate business or trusted contact, and they often contain malware attachments or hyperlinks to compromised websites.

What do you see as the biggest enabler of accidental insider threats?



67% Phishing attempts

56% Weak/reused passwords

44% Unlocked devices

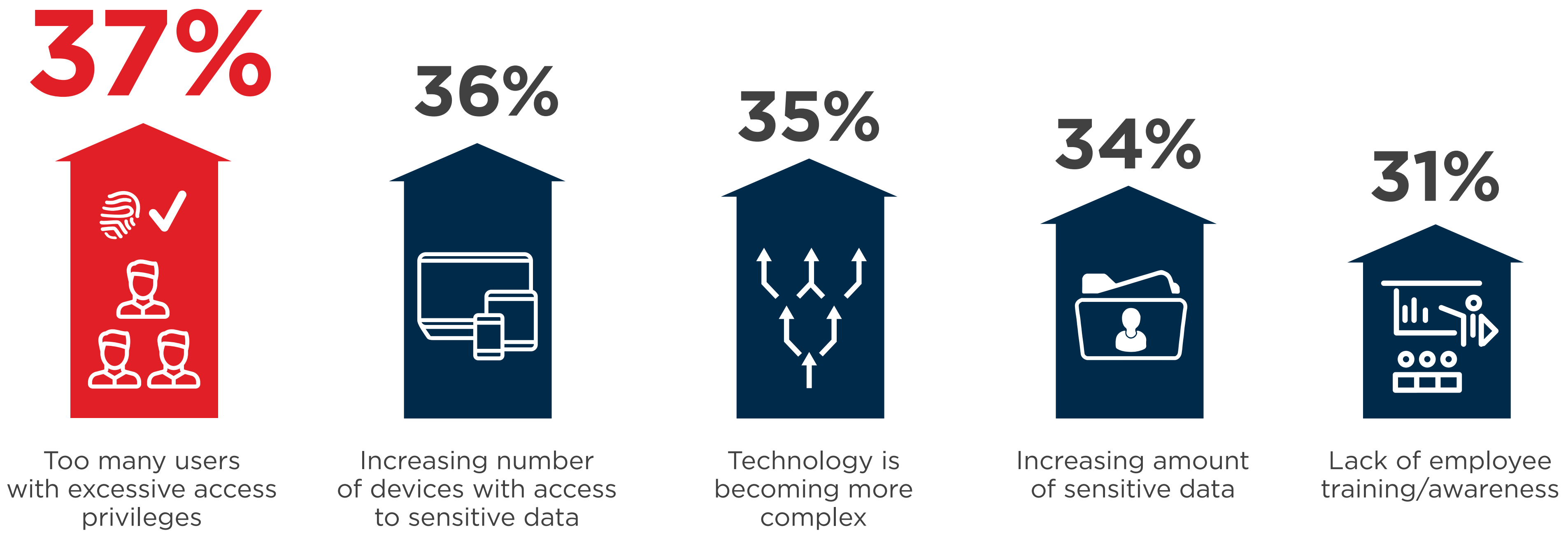
44% Bad password sharing practice

32% Unsecured WiFi networks

ENABLING RISK FACTORS

The survey reveals cybersecurity professionals perceive the following three responses as the top enablers for insider attacks: too many users with excessive access privileges (37%), increasing number of devices with access to sensitive data (36%), and technology becoming more complex (35%).

What do you believe are the main enablers of insider attacks?

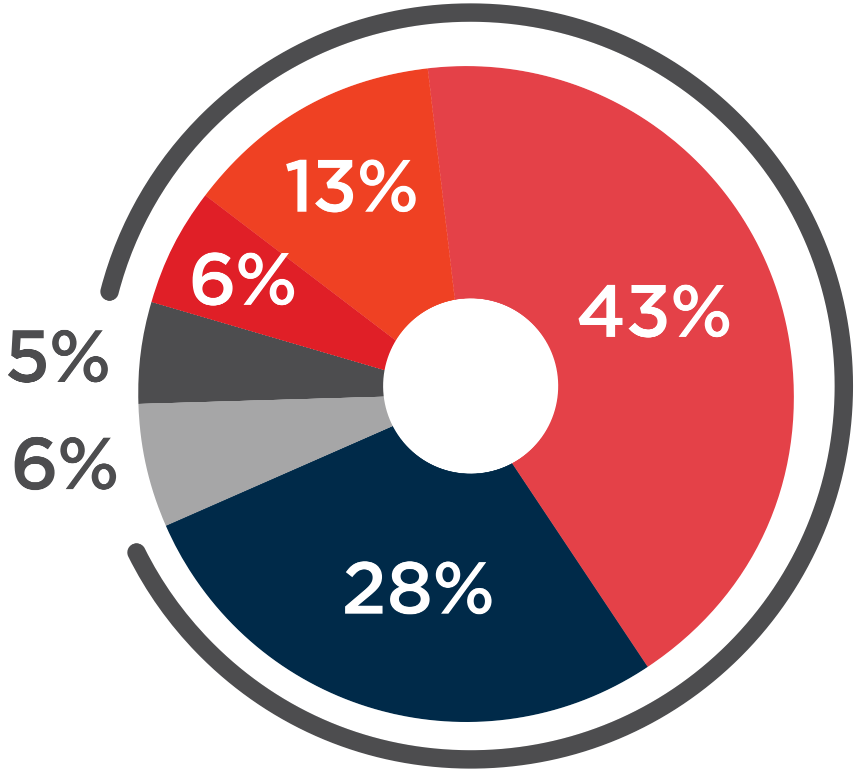


Insufficient data protection strategies or solutions 30% | Data increasingly leaving the network perimeter via mobile devices and web access 29% | Increased visibility of insider threats that were previously undisclosed 28% | Increasing use of cloud apps and infrastructure 28% | More employees, contractors, partners accessing the network 27% | More frustrated employees/contractors 19% | Not sure/others 8%

VULNERABILITY TO INSIDER THREAT

We asked cybersecurity professionals to assess their organization's vulnerability to insider threats. Ninety percent of organizations feel vulnerable. Only six percent say they are not at all vulnerable to an insider attack.

How vulnerable is your organization to insider threats?



90% feel vulnerable to insider threats

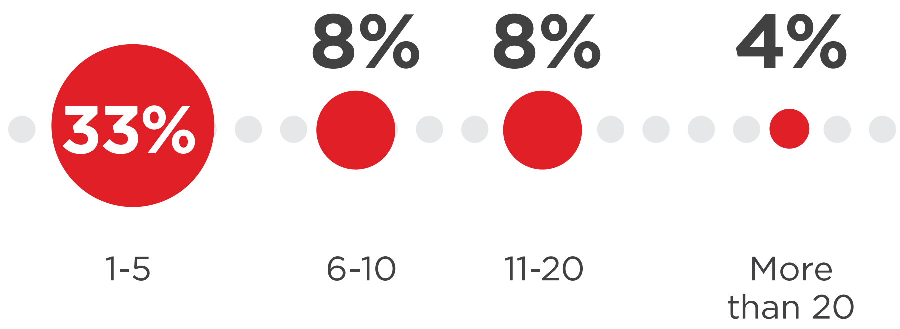
- 🟥 Extremely vulnerable
- 🟧 Very vulnerable
- 🟥 Moderately vulnerable
- ■ Slightly vulnerable
- ■ Not at all vulnerable
- ■ Cannot disclose/not sure

RECENT INSIDER ATTACKS

Looking back, 33% of organizations experienced five or less insider attacks in the last 12 months, while 20% experienced six or more attacks.

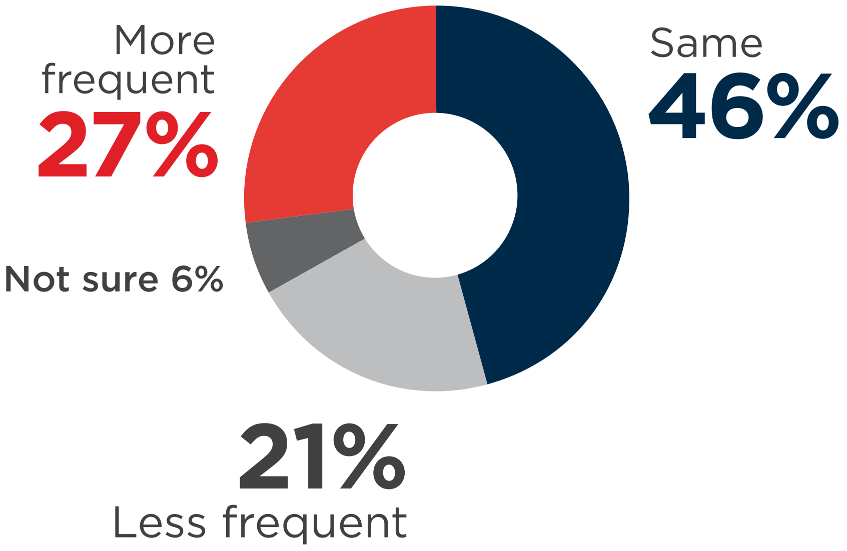
Twenty-seven percent say their organizations have experienced more frequent insider threats in the last 12 months. Nearly half of the security professionals (46%) polled believe the frequency of insider attacks has remained at the same levels while 21% say the frequency has decreased.

How many insider attacks did your organization experience in the last 12 months?



None/not sure 47%

Have insider attacks against your organization become more or less frequent over the last 12 months?

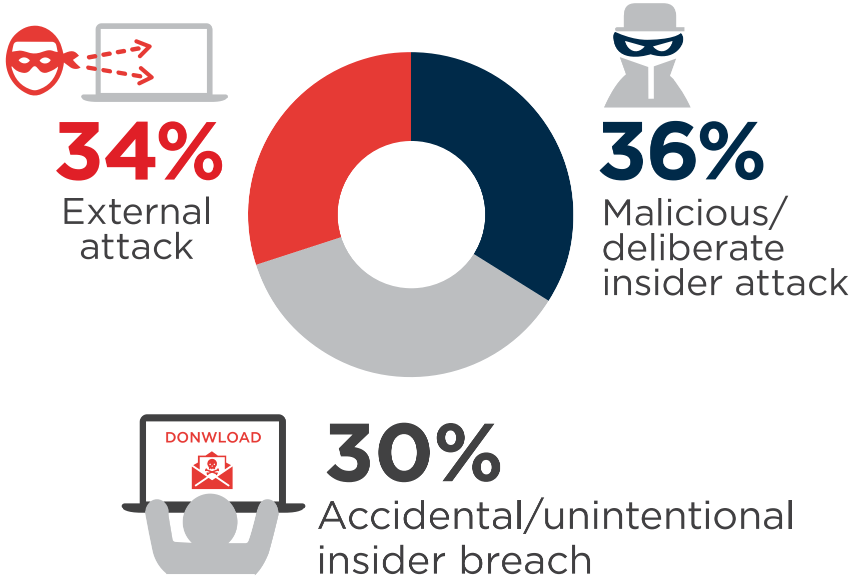


IMPACT OF INSIDER ATTACKS

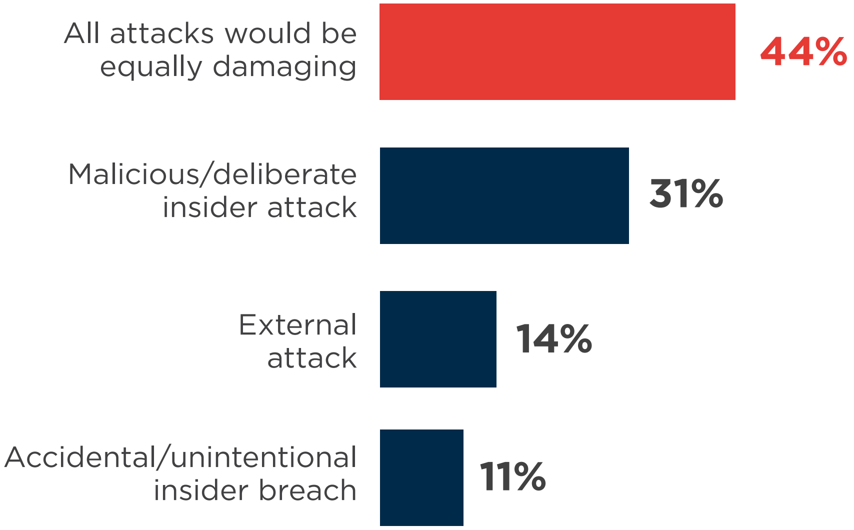
Two-thirds of organizations (66%) consider malicious insider attacks or accidental breaches more likely than external attacks.

Forty-four percent of organizations perceive all (malicious, external and accidental) attacks are as equally damaging, while 31% believe malicious /deliberate insider attacks are more damaging than external attacks (14%). The low weight placed on accidental insider breaches (11%) seems too low, perhaps underestimating the potential damages.

What threat do you consider most LIKELY to happen to your organization?



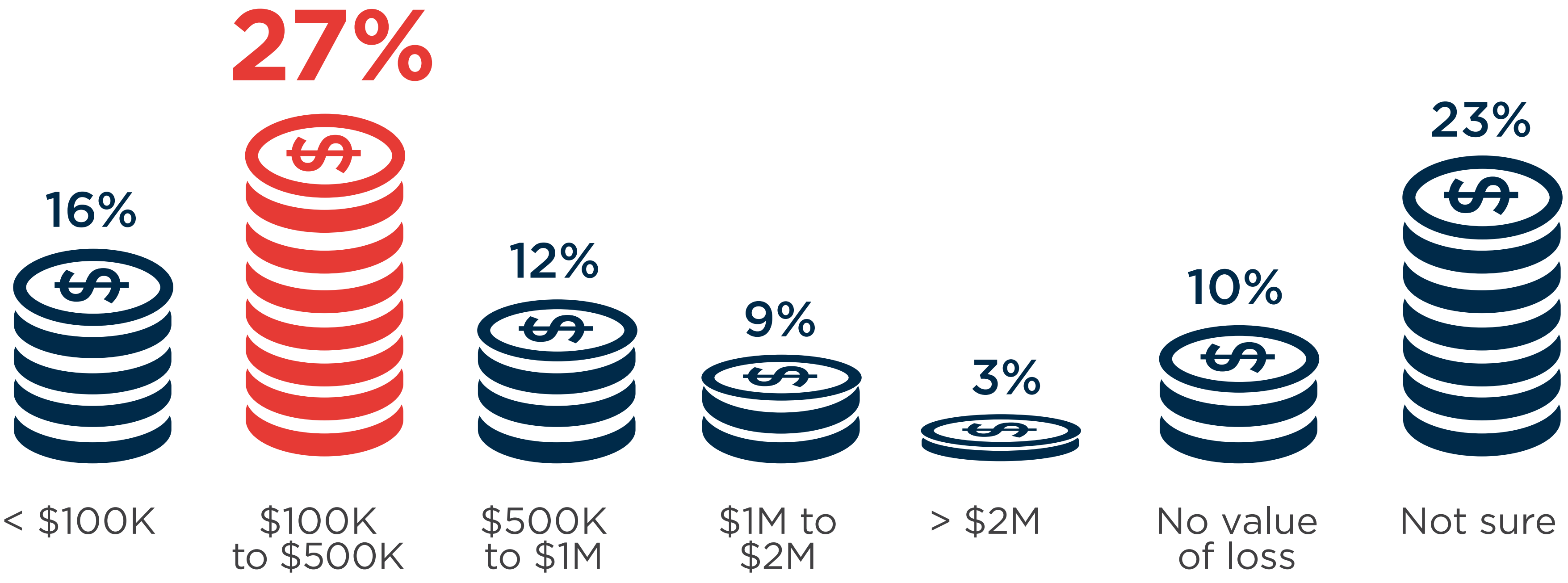
What threat do you consider more DAMAGING to your organization?



COSTLY INSIDER ATTACKS

While true cost of a major security incident are not easy to determine, the most common estimate is a range of $100,000 to $500,000 per successful insider attack (27%). Twenty-four percent expect damages to exceed $500,000.

What would you estimate is the potential cost/loss of an insider attack in US Dollars?



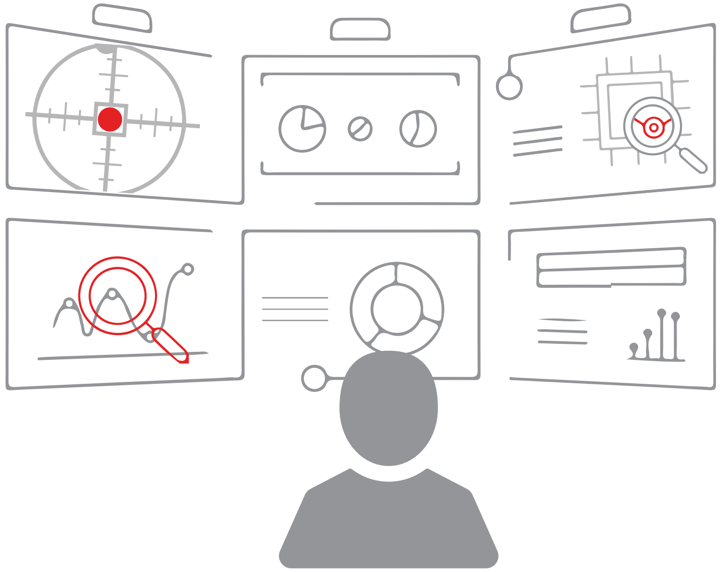
DETECTION

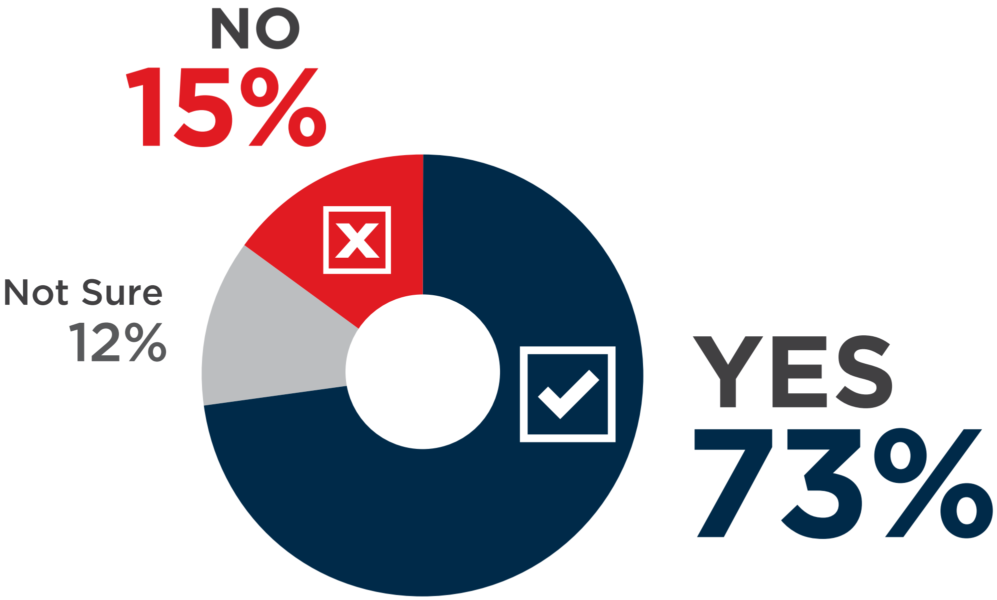
INSIDER RISK CONTROLS

Insider data threats present another layer of complexity for IT professionals to manage, requiring careful planning with regards to access controls, user permissions and monitoring user actions. Fifteen percent of organizations said they do not have adequate controls in place.

The good news is security practitioners realize that advanced detection and prevention are key, the majority of respondents (73%) have implemented security controls and policies to deal with impeding threats.

Does your organization have the appropriate controls to detect and prevent an insider attack?





DETERRENCE CONTROLS

An organization's control framework is the set of safeguards, separation of duties and recommended actions for IT professionals to use to minimize security risks and exposure. We asked security practitioners what security controls they use to deal with inevitable insider threats.

Data Loss Prevention (DLP) (60%) and encryption of data (at rest, in motion, in use) (60%) were both tied for the top spot. Respondents said Identity and Access Management (IAM) (56%) and endpoint and mobile security (50%) were also deployed to avert insider attacks.

▶ **What controls do you have in place to deter insider threats?**

60%
Data Loss Prevention
(DLP)

60%
Encryption of data
(at rest, in motion, in use)

56%
Identity and Access Management
(IAM)

50%
Endpoint and mobile security

29%
Cloud Access Security
(CASB)

Enterprise Digital Rights Management Solutions (E-DRM) 29% | Privileged account vault 27% | Other 1%

DETECTION CONTROLS

There are numerous methods and security tools available to help cybersecurity professionals detect and analyze insider attacks. A vast majority of the respondents identified the use of more than one security tool in their organization. By merging and analyzing these disparate sources, organizations are better able to deal with security breaches.

The survey concluded that most insider exploits are detected through Intrusion Detection and Prevention (IDS/IPS) (63%), Log Management (62%) and Security Information and Event Management (SIEM) (51%) tools.

What controls do you have in place to detect and analyze insider attacks?

63% Intrusion Detection and Prevention (IDS/IPS)

62% Log management

51% Security Information and Event Management (SIEM)

40% Predictive analytics

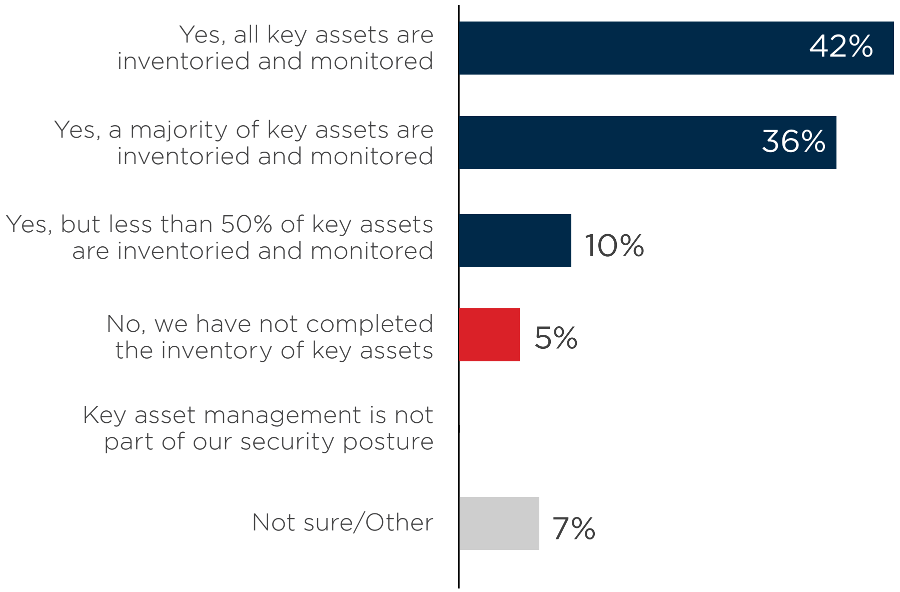
User and Entity Behaviour Analytics (UEBA) 39% | Other 2%

MONITORING OF SENSITIVE ASSETS

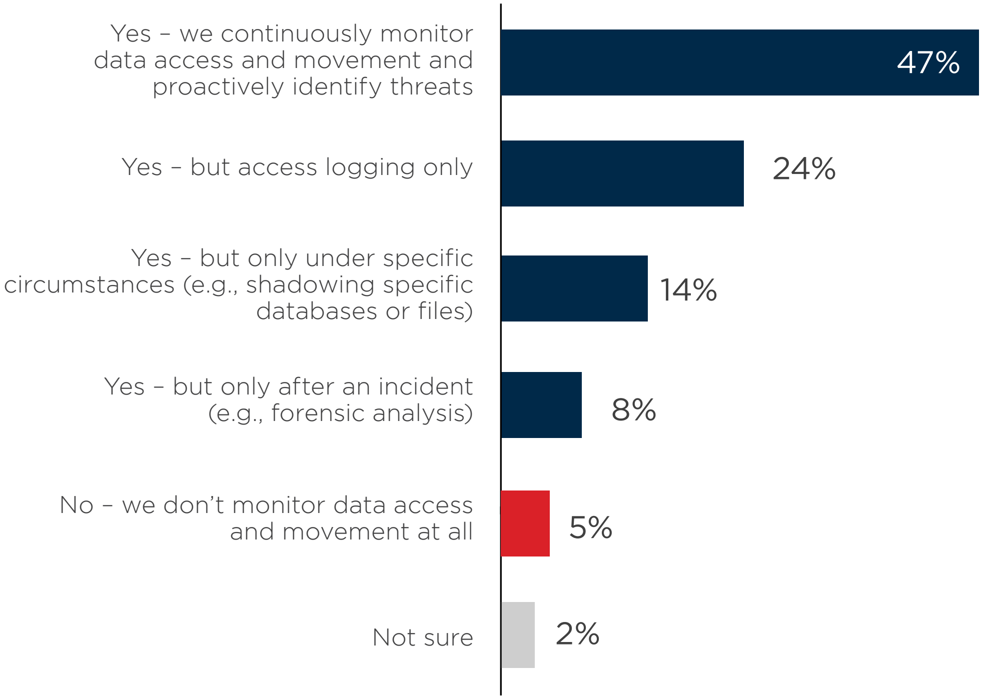
Identification, tracking and monitoring of key assets and system resources can help avert or limit an organization's exposure to insider attacks. When security professionals manage and monitor their key assets, they are able to react faster and with more precision to mitigate incidents. More than three-fourths (78%) of respondents inventory and monitor all or the majority of their key assets.

An overwhelming majority (93%) of organizations monitor access to sensitive data. The level of monitoring varies; 47% continuously monitor data access and movement to proactively identify threats. Remarkably, five percent do not monitor data access and movement at all.

Do you monitor key assets and system resources?



Do you monitor access to sensitive data?

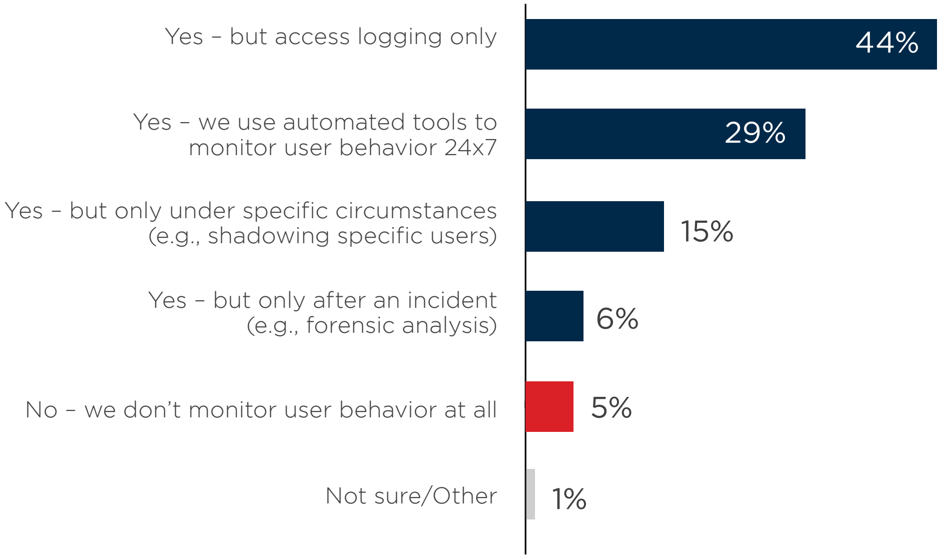


INSIDER MONITORING

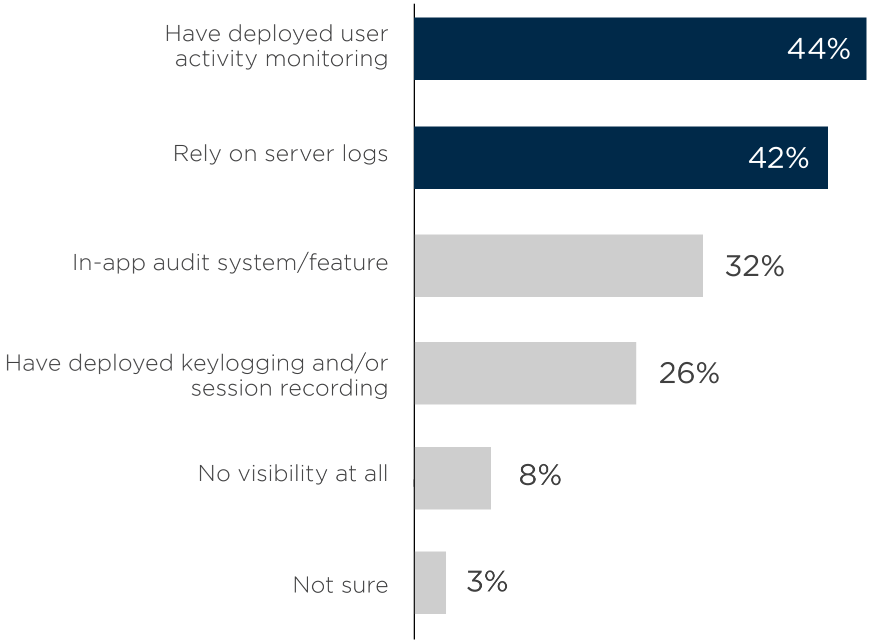
The increasing volume of insider threats have caused cybersecurity professionals to take more action and deploy User Behavior Analytics (UBA) tools and solutions to help detect, classify and alert anomalous behavior. The number of organizations monitoring their user behavior has increased significantly compared to last year (94% this year compared to 42% last year). The number of organizations that don't monitor their users dropped from 21% last year to only six percent this year.

In this year's survey, respondents said that they leverage User Activity Monitoring (UAM) (44%) as their top solution to manage user behavior within core applications, followed closely by the use of server logs (42%). Eight percent of respondents have no visibility at all, a decrease from last year of five points, which signals that organizations are investing in tools and resources to have better visibility into user activity.

Do you monitor user behavior?



What level of visibility do you have into user behavior within core applications?

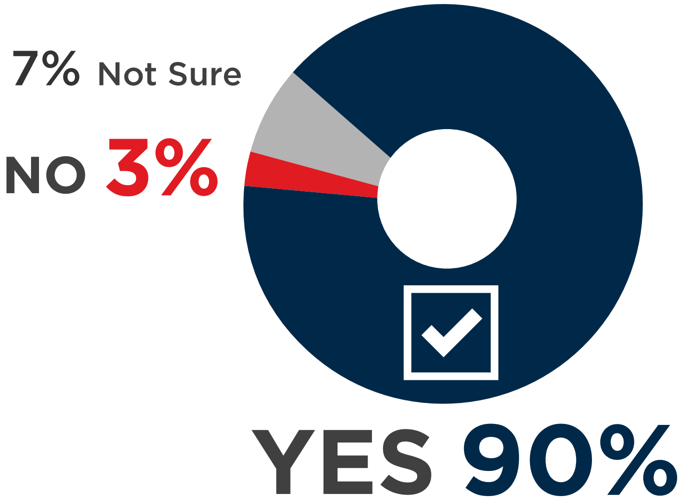


INSIDER MONITORING

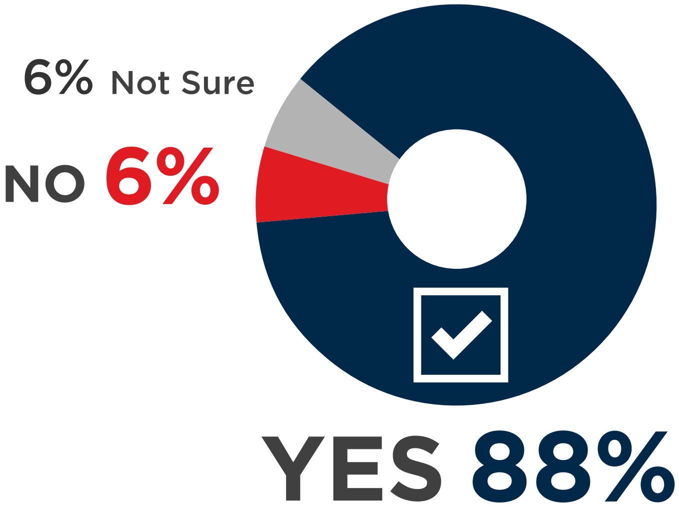
Every organization must be vigilant when it comes to data protection. Not all insider threats are malicious; some are the result of an honest mistake or careless employee behavior. Monitoring allows cybersecurity professionals to decrease their risk exposure by quickly detecting unusual employee system activity. Ninety percent of the respondents believe that it is necessary to monitor access to the organization's sensitive data.

Identification of high-risk insiders is a key part of a threat prevention strategy. One way to identify these individuals is to profile their behavior and work patterns. Hostility toward other employees, late or excessive missing work, undue work outside normal work hours, and declining performance are just some of the indicators. Organizations surveyed strongly believe it is necessary to identify high-risk insiders based on their behaviors (88%).

Do you think it's necessary to monitor and profile how insiders are accessing your sensitive data?



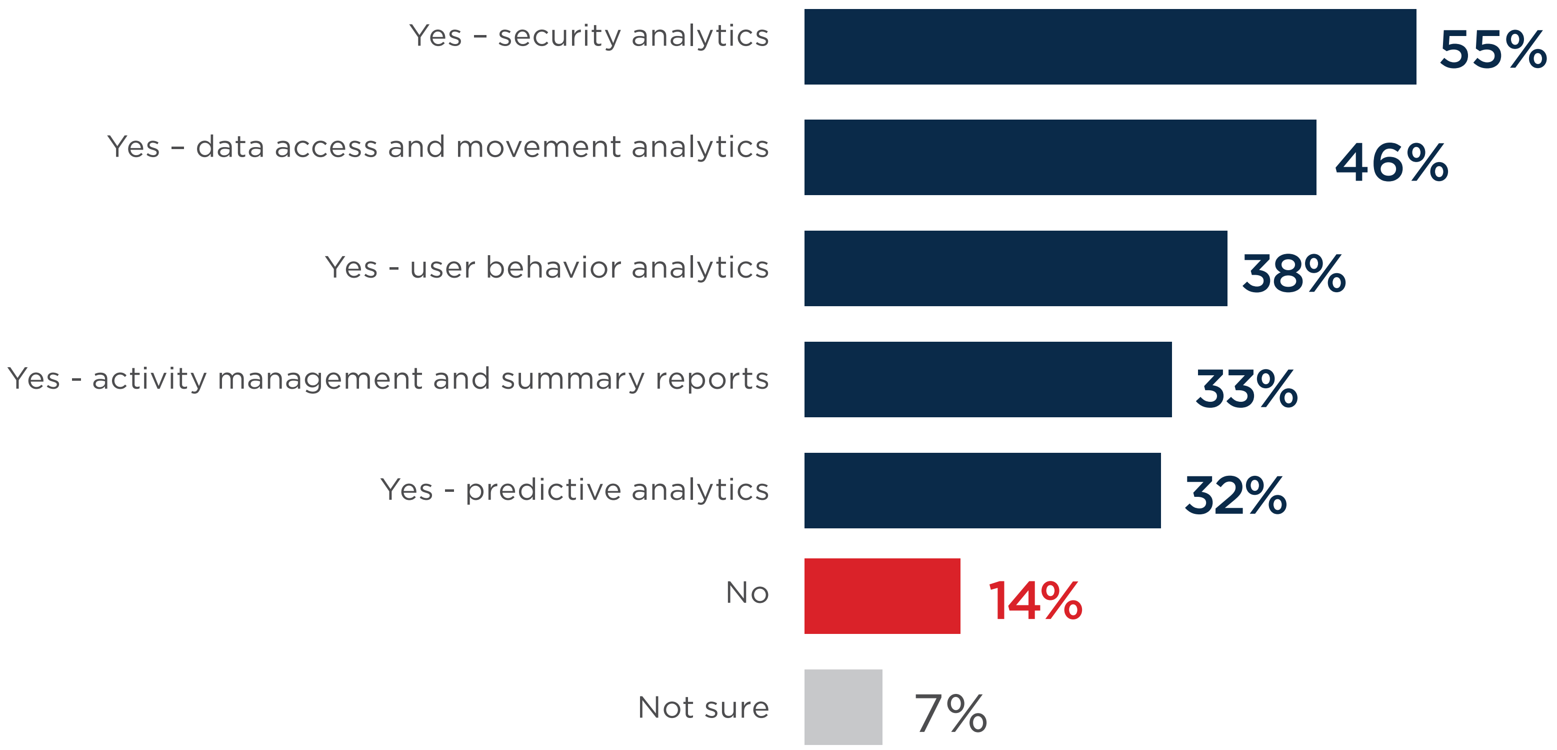
Do you think it's necessary to identify high-risk insiders based on their behaviors?



ADOPTION OF ANALYTICS

The number of organizations that do not leverage threat analytics continues to decline year after year. This year, only 14% of respondents said they do not use analytics, compared to 30% last year.

Does your organization leverage analytics to determine insider threats?



INSIDER THREAT PROGRAM

FOCUS ON DETECTION

Organizations are shifting their focus on detection of internal threats. In this year's survey, detection (64%) surpassed deterrence methods (58%) to take the top spot, followed by analysis and post breach forensics (49%).

What aspect(s) of insider threat management does your organization primarily focus on?

64%

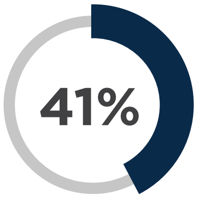
Detection
(e.g., user monitoring, IDS, etc.)

58%

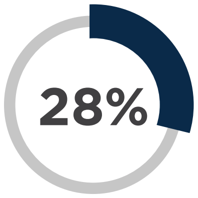
Deterrence
(e.g., access controls, encryption, policies, etc.)

49%

Analysis and post breach forensics
(e.g., SIEM, log analysis, etc.)



Post breach remediation
(e.g., backup/disaster recovery, etc.)

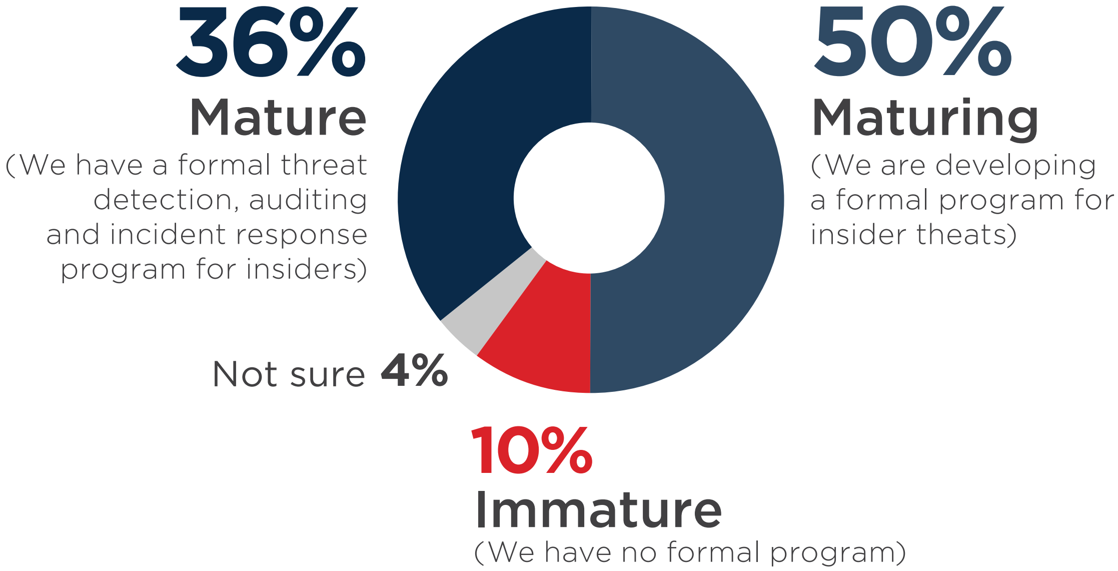


Deception
(e.g., honeypots, etc.)

INSIDER PROGRAM MATURITY

The survey reveals that organizations have recognized the growing significance of insider threats and are investing resources to develop comprehensive incident response plans. A vast majority (86%) of organizations have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.

How would you rate the maturity of your insider threat program?

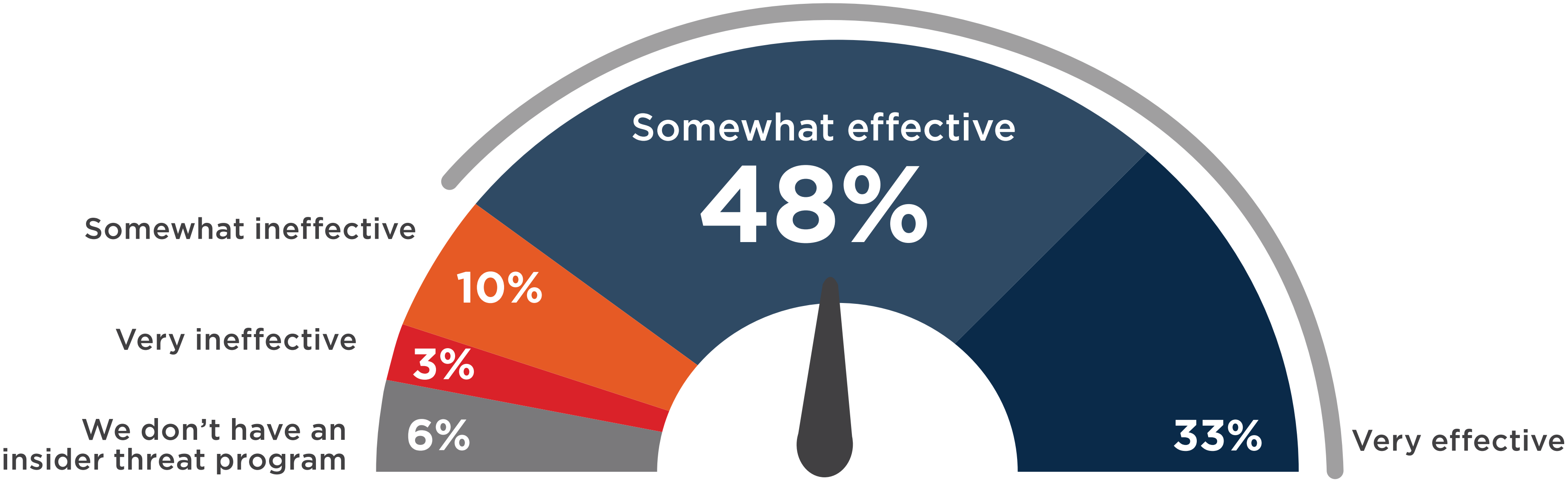

36%
Mature
(We have a formal threat detection, auditing and incident response program for insiders)
50%
Maturing
(We are developing a formal program for insider theats)
Not sure 4%
10%
Immature
(We have no formal program)

INSIDER THREAT CONFIDENCE

A majority of respondents surveyed (81%) say their organizations are moderately to very effective when it comes to addressing insider threat prevention and detection. Thirteen percent expressed that their organization's insider threat programs are ineffective, while six percent do not have a program in place.

▶ **How effective do you consider your insider threat prevention and detection methods?**

81% think their organizations are moderately to very effective addressing insider threat prevention and detection

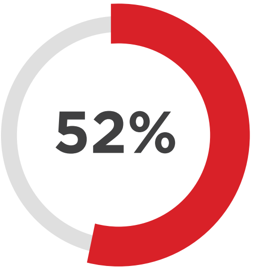


BARRIERS TO INSIDER THREAT MANAGEMENT

For the third year in a row, lack of training and expertise (52%) remain the biggest barrier to better insider threat management. Other barriers include the lack of suitable technology (43%), while tied for third place in this year's survey are both lack of collaboration between departments (34%) and lack of budget (34%). Notably, lack of budget fell from second place last year to third this year.

What are the biggest barriers to better insider threat management?

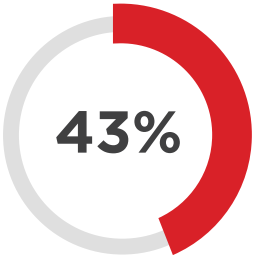
#1



Lack of training and expertise

⬇ **8% p.p.** from last year

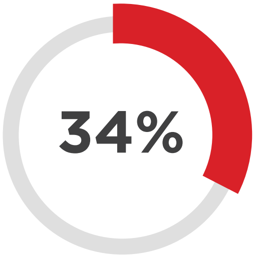
#2



Lack of suitable technology

⬆ **15% p.p.** from last year

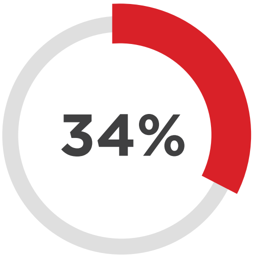
#3



Lack of collaboration between separate departments

⬇ **14% p.p.** from last year

#4



Lack of budget

⬇ **16% p.p.** from last year

Lack of staff 22% | Not a priority 10% | Not sure / Other 5%

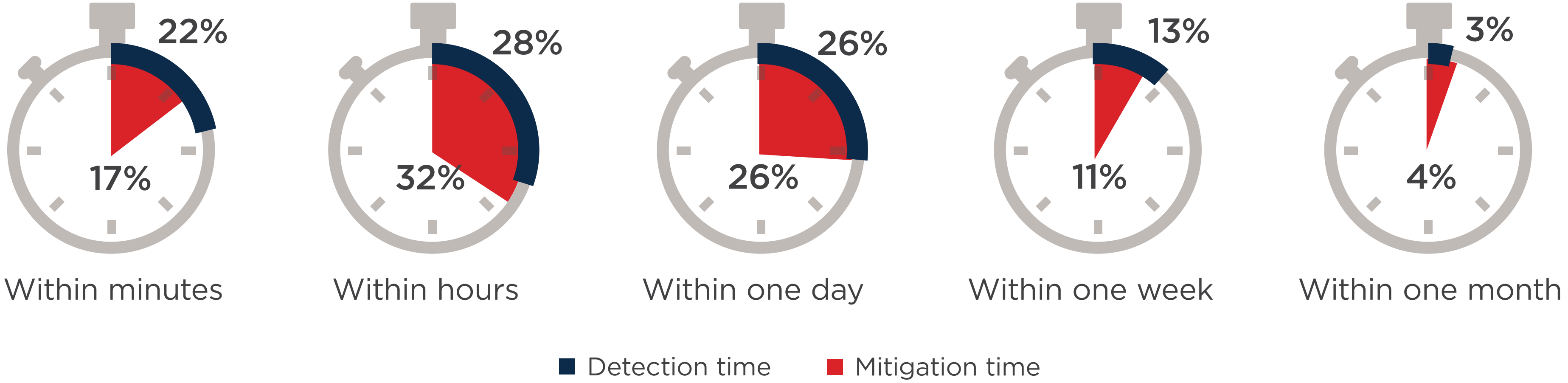
SPEED OF DETECTION & MITIGATION

Detecting and preventing insider attacks is much more challenging than external breaches, as they are users with legitimate access that unwittingly create vulnerabilities or intend to maliciously exploit an organization's cyber assets. Slightly more than one-fifth of respondents claim detection of insider threats is within minutes (22%), while 28% say within hours.

In this year's survey, organizations are even more confident in their ability to quickly recover from insider attacks. Most organizations feel they could recover from an attack within a week (89%) up 18% from the previous year. Only two percent of companies believed they would never fully recover.

How long does it typically take your organization to detect an insider attack?

How long does it typically take your organization to mitigate and stop an insider attack?



50% organizations detect an insider attack within hours

Not sure 8%

49% organizations mitigate and stop an insider attack within hours

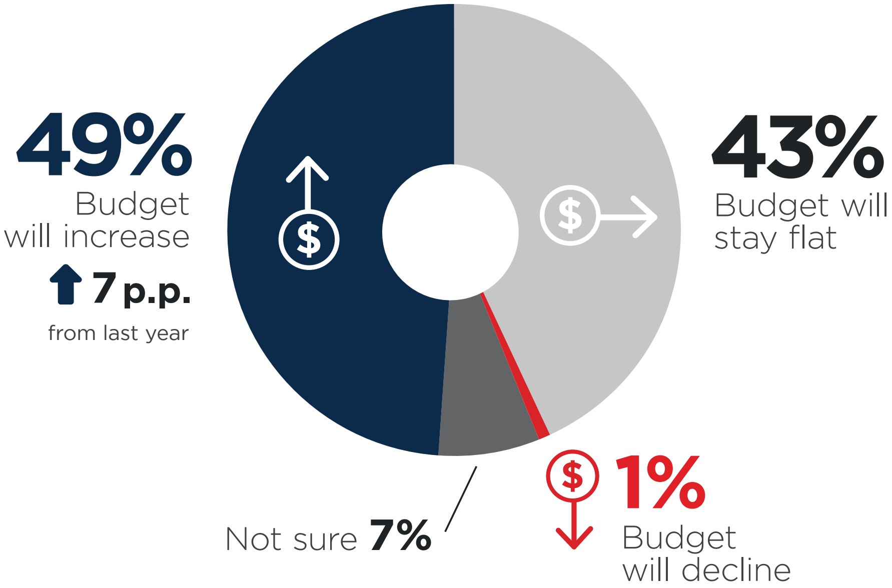
Not sure 10%

BUDGET TRENDS

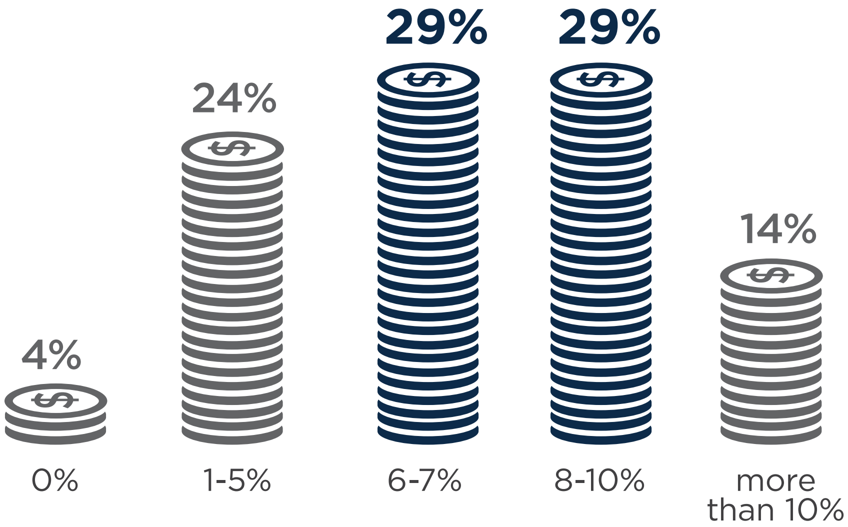
Looking ahead, close to half of the surveyed organizations (49%) expect budget increases. Forty-three percent expect their IT budgets to remain flat, while only one percent foresee their security funding shrinking. This is a marked improvement in budget outlook compared to last year's survey.

Defending against security attacks is an ongoing challenge; cybersecurity professionals are equally concerned about the rise in the volume and frequency of both external and insider attacks. Forty-three percent of organizations allocate over eight percent of their IT security budget to preventing, detecting, and mitigating insider threats.

▶ How is your security budget changing over the next 12 months?



▶ How much of your IT security budget is devoted to preventing, detecting and mitigating insider threats?



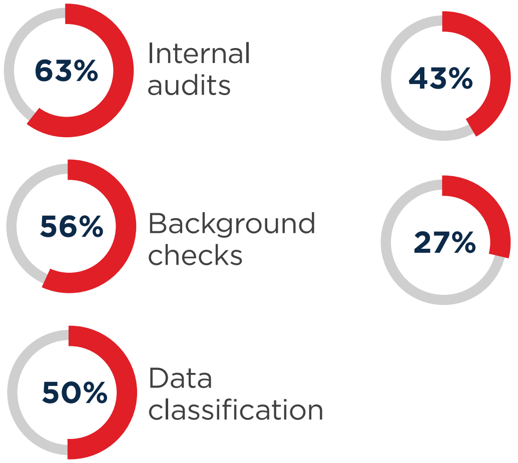
INSIDER THREAT TRAINING

Having a well understood information security policy and documented procedures help protect organizations and reduce risk from both internal and external cyber threats. The primary policy-based insider threat management methods that organization's have in place are the use of company policies and training (68%), internal audits (63%), and background checks (56%).

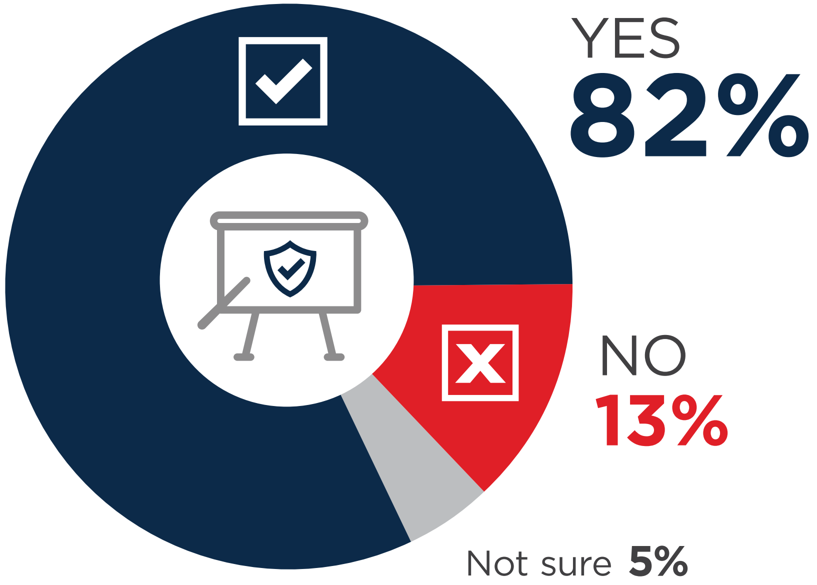
Organizations realize that prevention and awareness is are key cornerstone in the defense against insider security breaches; an overwhelming majority (82%) have implemented insider security programs.

What administrative policies and procedures do you have in place for insider threat management?

68% Policies and training



Do you offer training to your employees and staff on how to minimize insider security risks?



SPONSOR OVERVIEW

SPONSOR OVERVIEW

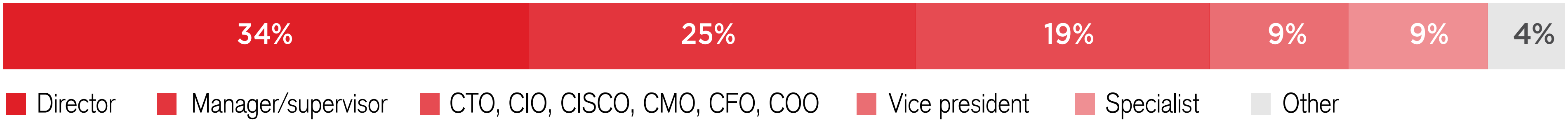
CA Technologies | www.ca.com

CA Technologies (NASDAQ:CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business in every industry. From planning, to development, to management and security, CA is working with companies worldwide to change the way we live, transact, and communicate – across mobile, private and public cloud, distributed and mainframe environments.

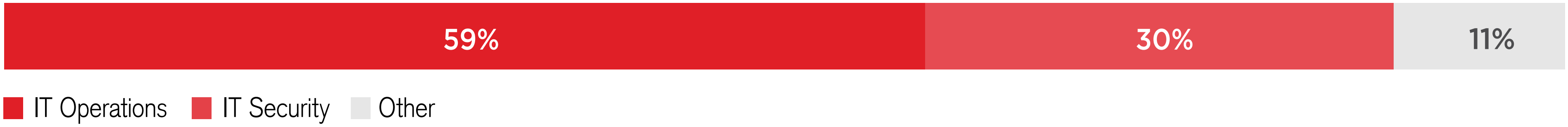
METHODOLOGY & DEMOGRAPHICS

This research is based on the results of a comprehensive online survey of 472 cybersecurity professionals to gain deep insight into the insider threat faced by organizations and the solutions to detect, remediate, and prevent it. The respondents range from technical executives to managers and IT security practitioners, representing organizations of varying sizes across all industries.

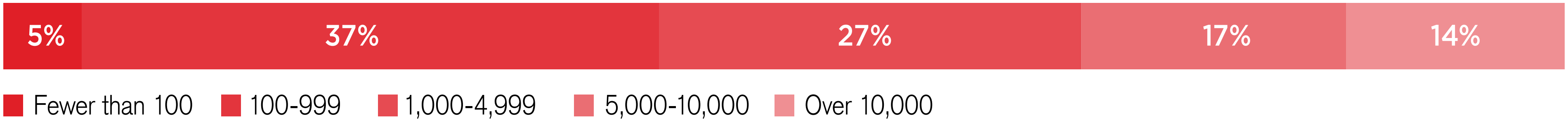
JOB TITLE



DEPARTMENT



COMPANY SIZE


Fewer than 100
Over 10,000