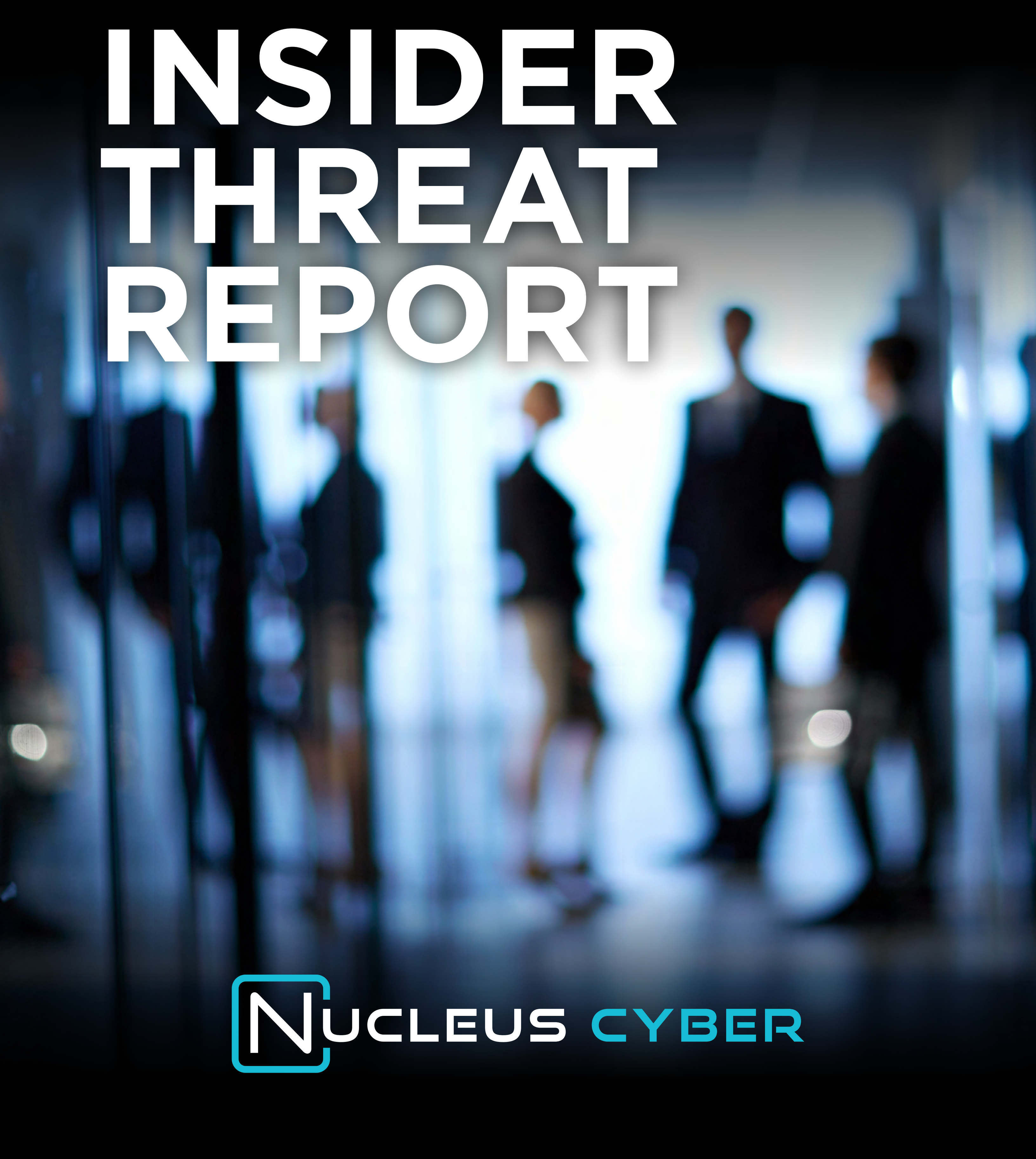
2019

Cybersecurity INSIDERS

INSIDER THREAT REPORT



NUCLEUS CYBER

INTRODUCTION

Today's most damaging security threats are often not originating from malicious outsiders or malware but from trusted insiders with access to sensitive data and systems - both malicious insiders and negligent insiders.

The 2019 Insider Threat Report reveals the latest trends and challenges facing organizations, how IT and security professionals are dealing with risky insiders, and how organizations are preparing to better protect their critical data and IT infrastructure.

Key findings include:

- 70% of organizations confirm insider attacks are becoming more frequent
- 68% feel extremely to moderately vulnerable to insider attacks
- 39% identified cloud storage and file sharing apps as the most vulnerable to insider attacks
- 85% of organizations find it moderately difficult to very difficult to determine the actual damage of an insider attack
- 56% believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud

This 2019 Insider Threat Report has been produced by Cybersecurity Insiders, the 400,000 member community for information security professionals, to explore how organizations are responding to the evolving insider security threats.

Many thanks to Nucleus Cyber for supporting this important research project.

We hope you'll find this report informative and helpful as you continue your efforts in protecting your IT environments against insider threats.

Thank you,
Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

TYPES OF INSIDER THREATS

The term “Insider Threat” is often associated with malicious employees intending to directly harm the company through theft or sabotage. In truth, negligent employees or contractors can unintentionally pose an equally high risk of security breaches and leaks by accident.

In this year’s survey, companies are more worried about inadvertent insider breaches (70%) and negligent data breaches (66%) than they are about malicious intent by insiders (62%).

What type of insider threats are you most concerned about?

70%

Inadvertent data breach/ leak

(e.g. careless user causing accidental breach)

66%

Negligent data breach

(e.g. user willfully ignoring policy, but not malicious)

62%

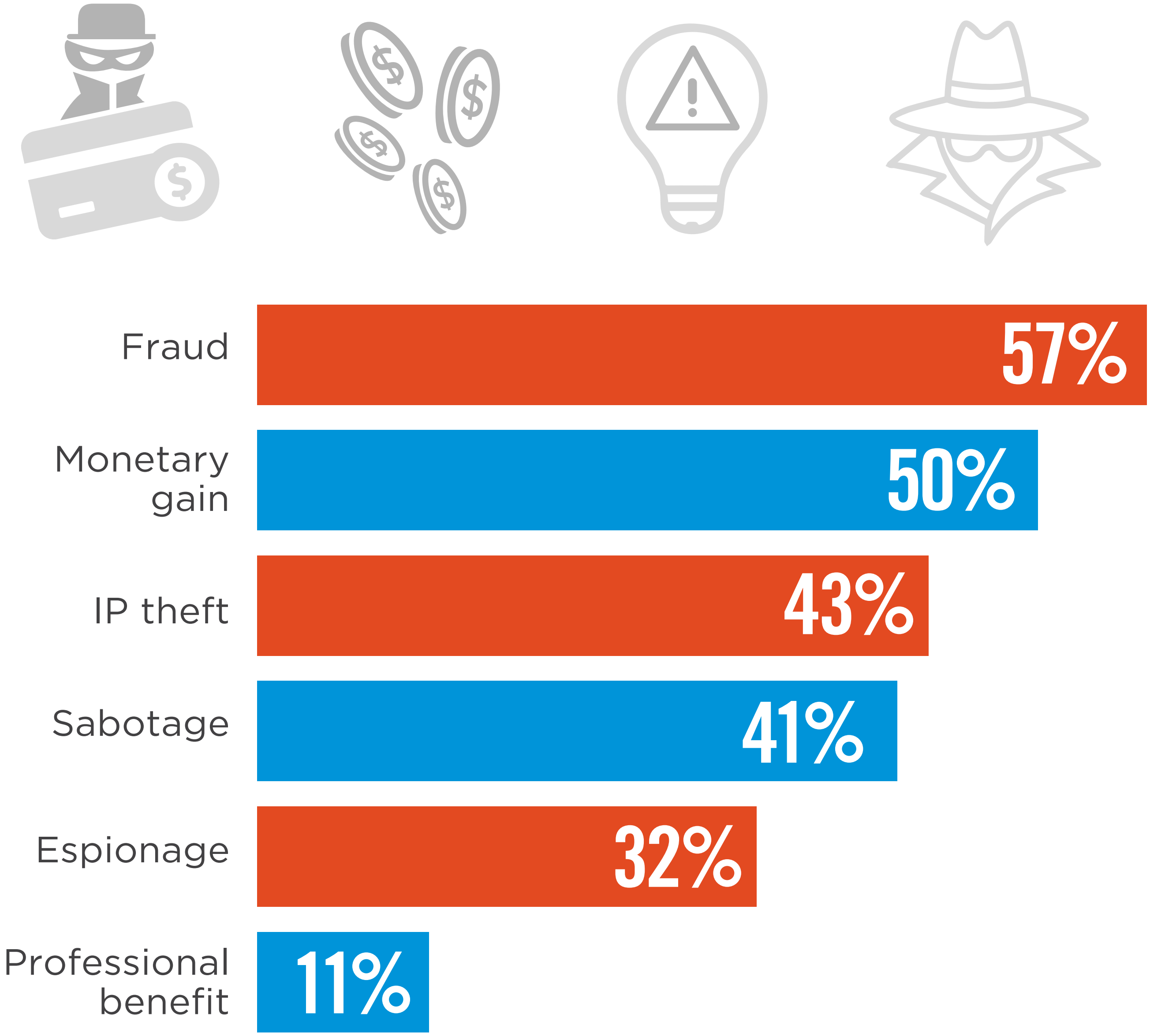
Malicious data breach

(e.g. user willfully causing harm)

MOTIVATIONS FOR INSIDER ATTACKS

To understand malicious insider threats, it's important to look at the underlying motivations of insiders. Our survey panel considers fraud (57%) and monetary gain (50%) the biggest factors that drive malicious insiders, followed by theft of intellectual property (43%).

▶ **What motivations for malicious insider threats are you most concerned about?**

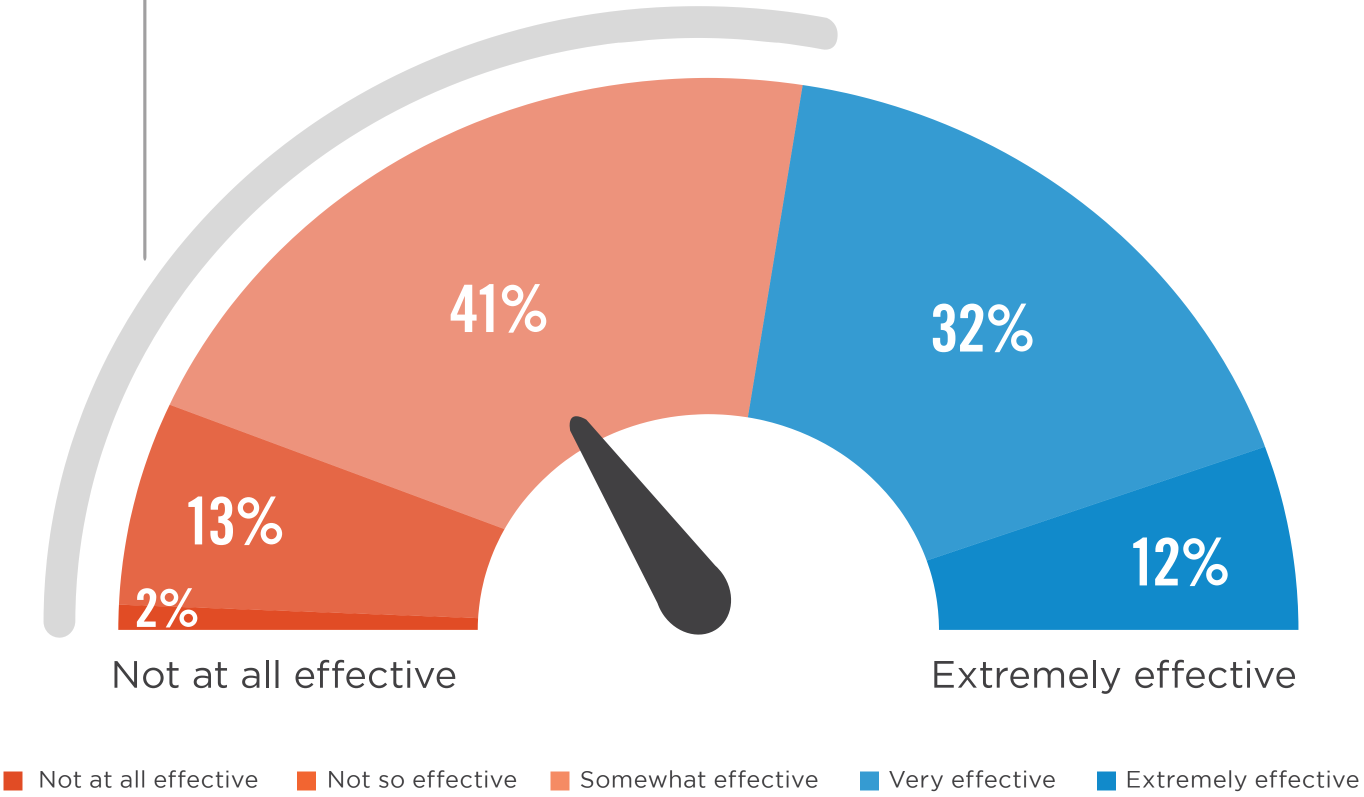


INSIDER THREAT
DISCOVERY AND RESPONSE

A majority of organizations consider themselves only somewhat effective or worse (56%) when it comes to monitoring, detecting and responding to insider threats.

How would you characterize the effectiveness of your organization to monitor, detect, and respond to insider threats?

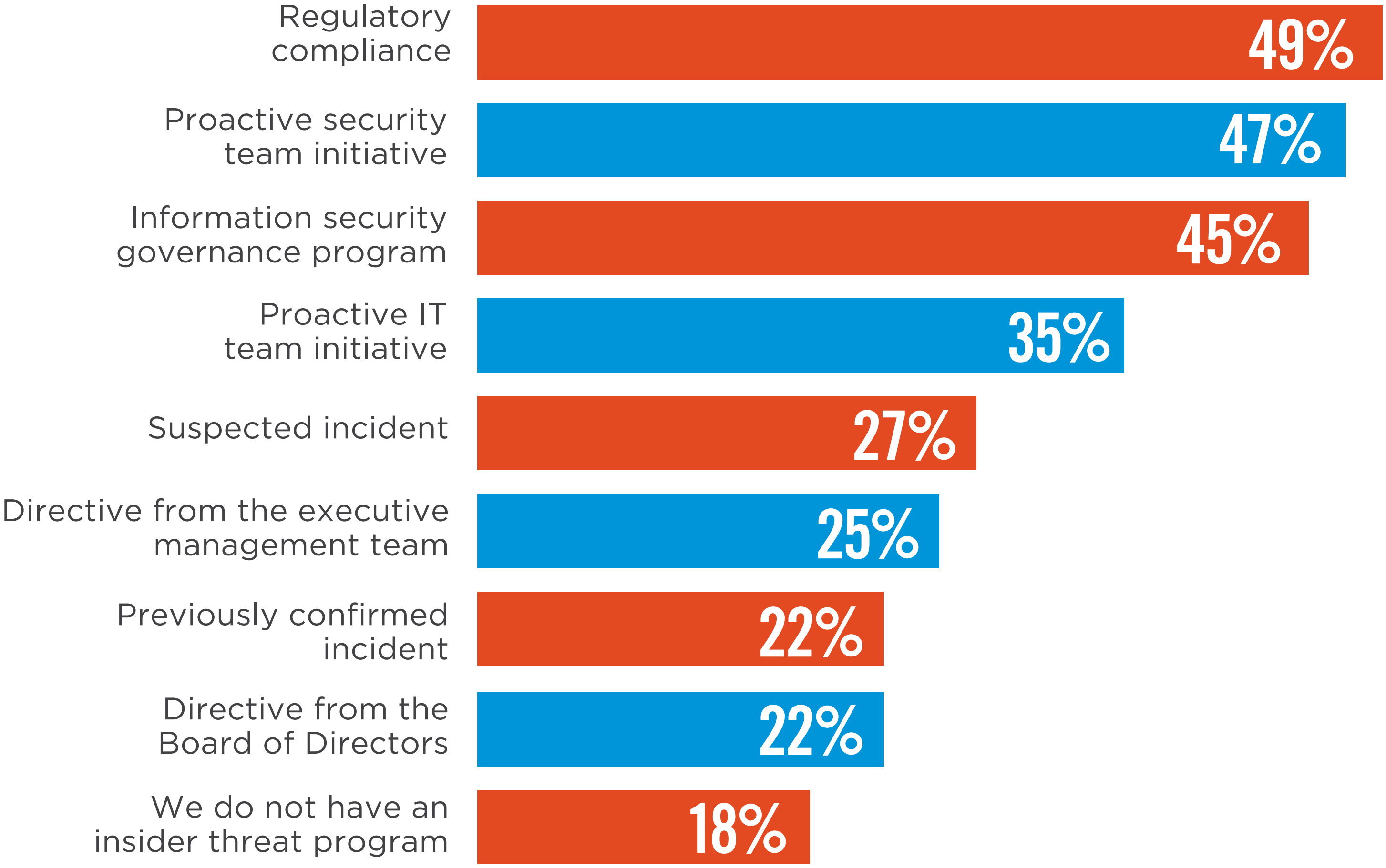
56% consider their monitoring, detecting and responding to insider threats somewhat effective or worse.



INSIDER THREAT PROGRAM DRIVERS

The creation of formal insider threat programs is typically driven by an organization's compliance requirements (49%) and proactive security programs (47%), rather than a response to insider incidents.

What is the primary driver of your insider threat program?

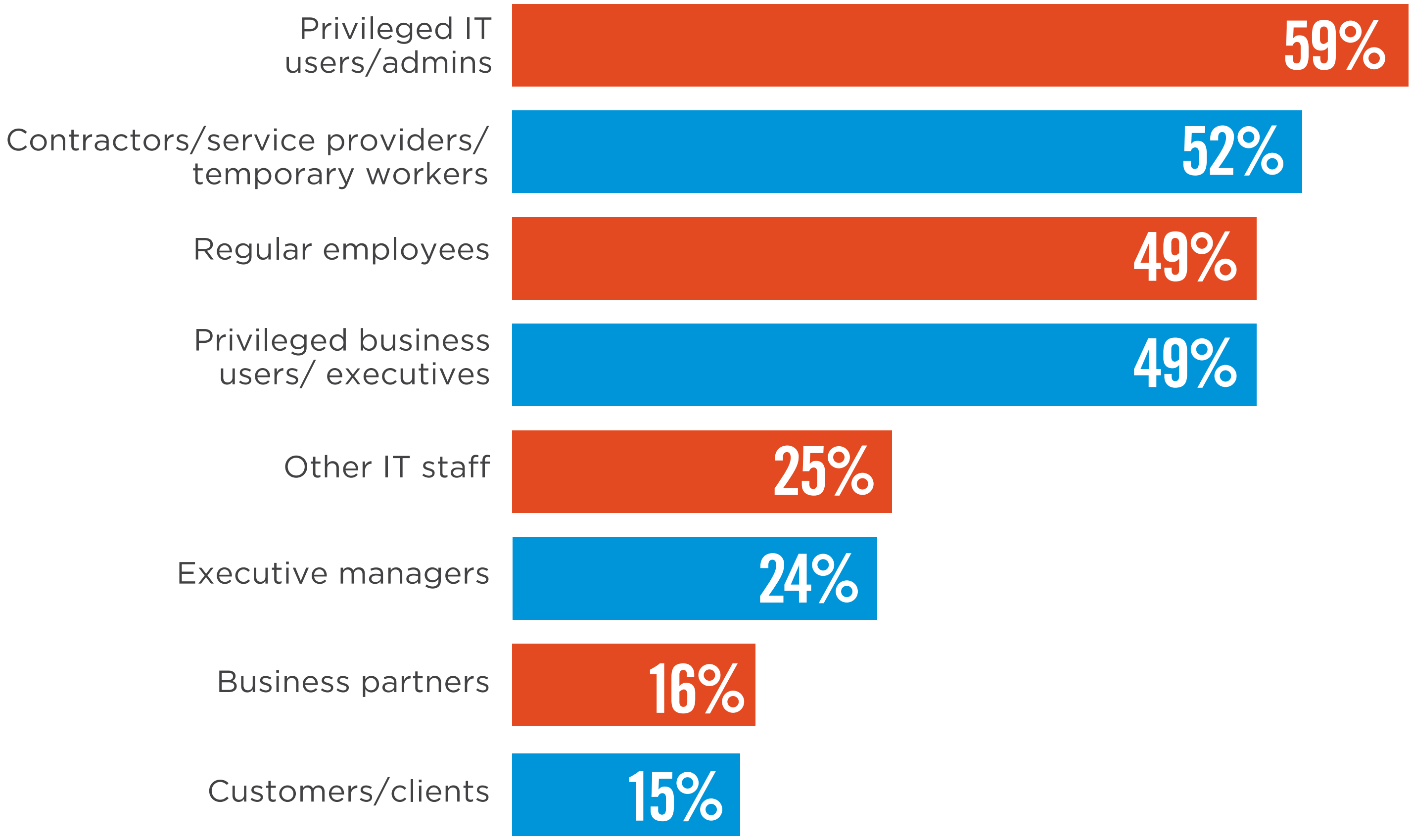


RISKY INSIDERS

Protecting organizations against cyber threats becomes significantly more challenging when the threats come from within the organization, from trusted and authorized users. It can be difficult to determine when users are simply doing their job function or actually doing something malicious or negligent.

The survey indicates that privileged IT users (59%) pose the biggest insider security risk to organizations, followed by contractors (52%), and regular employees and privileged business users (tied at 49%).

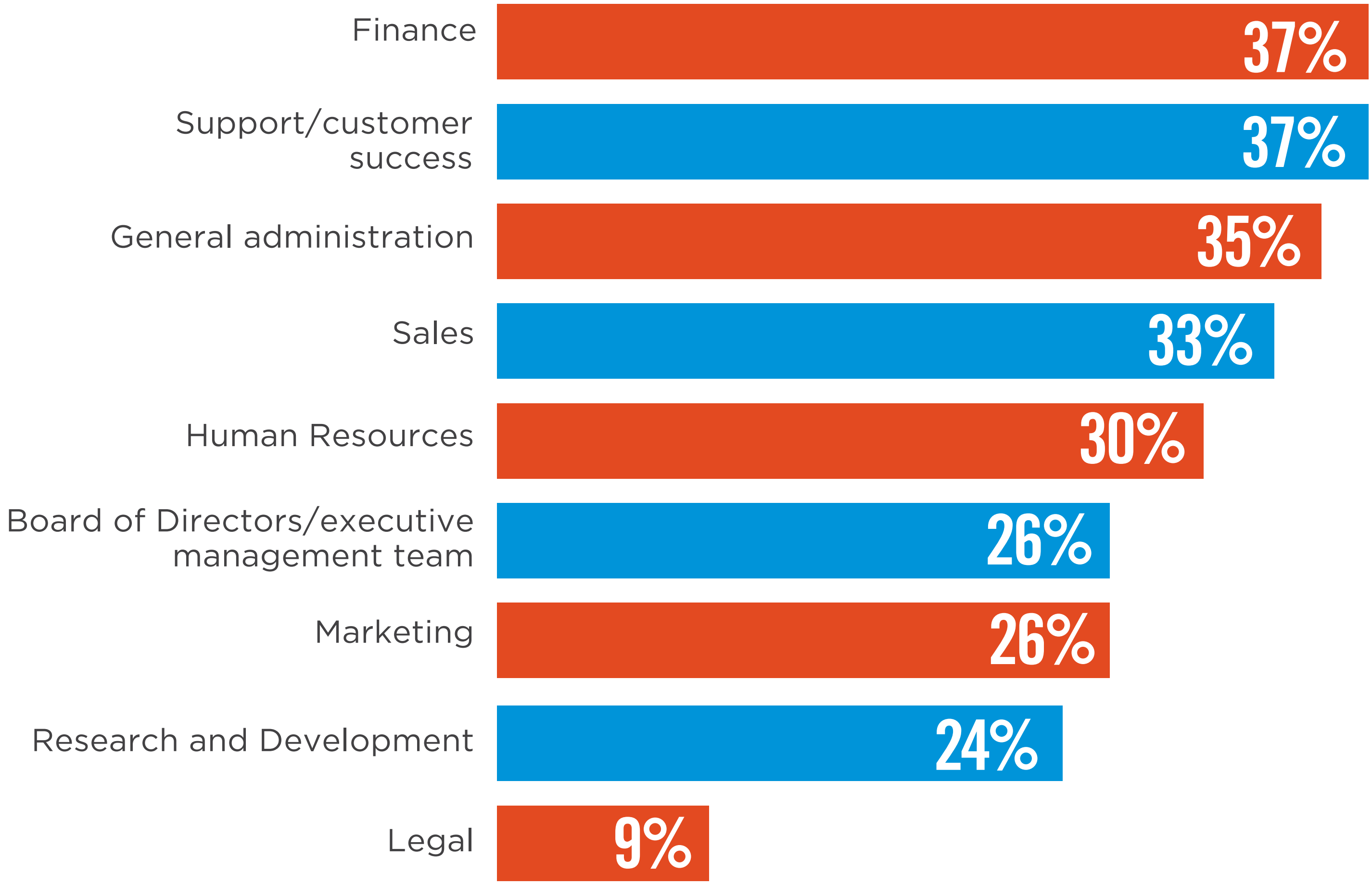
What type(s) of insiders pose the biggest security risk to organizations?



DEPARTMENTS AT RISK

Organizations in our survey consider their finance departments (37%), customer support (37%) and general administration (35%) as the highest risk of insider threats.

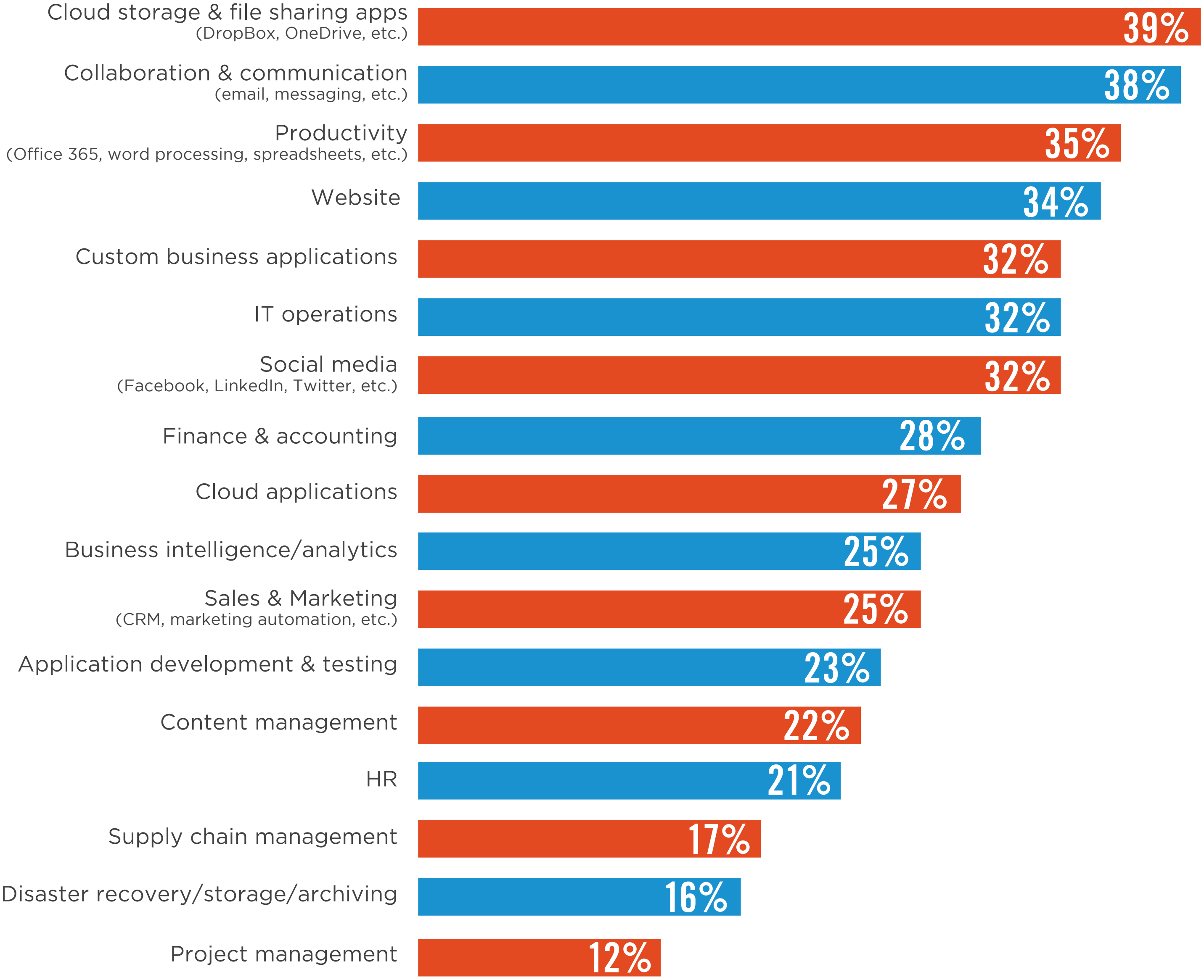
Which departments or groups within your organization present the biggest risk for insider threats?



MOST VULNERABLE APPLICATIONS

Cybersecurity professionals view cloud storage and file sharing apps (such as Dropbox, OneDrive, etc.) as most vulnerable to insider attacks (39%), closely followed by collaboration and communications apps (such as email, messaging, etc.) (38%), and productivity apps (35%).

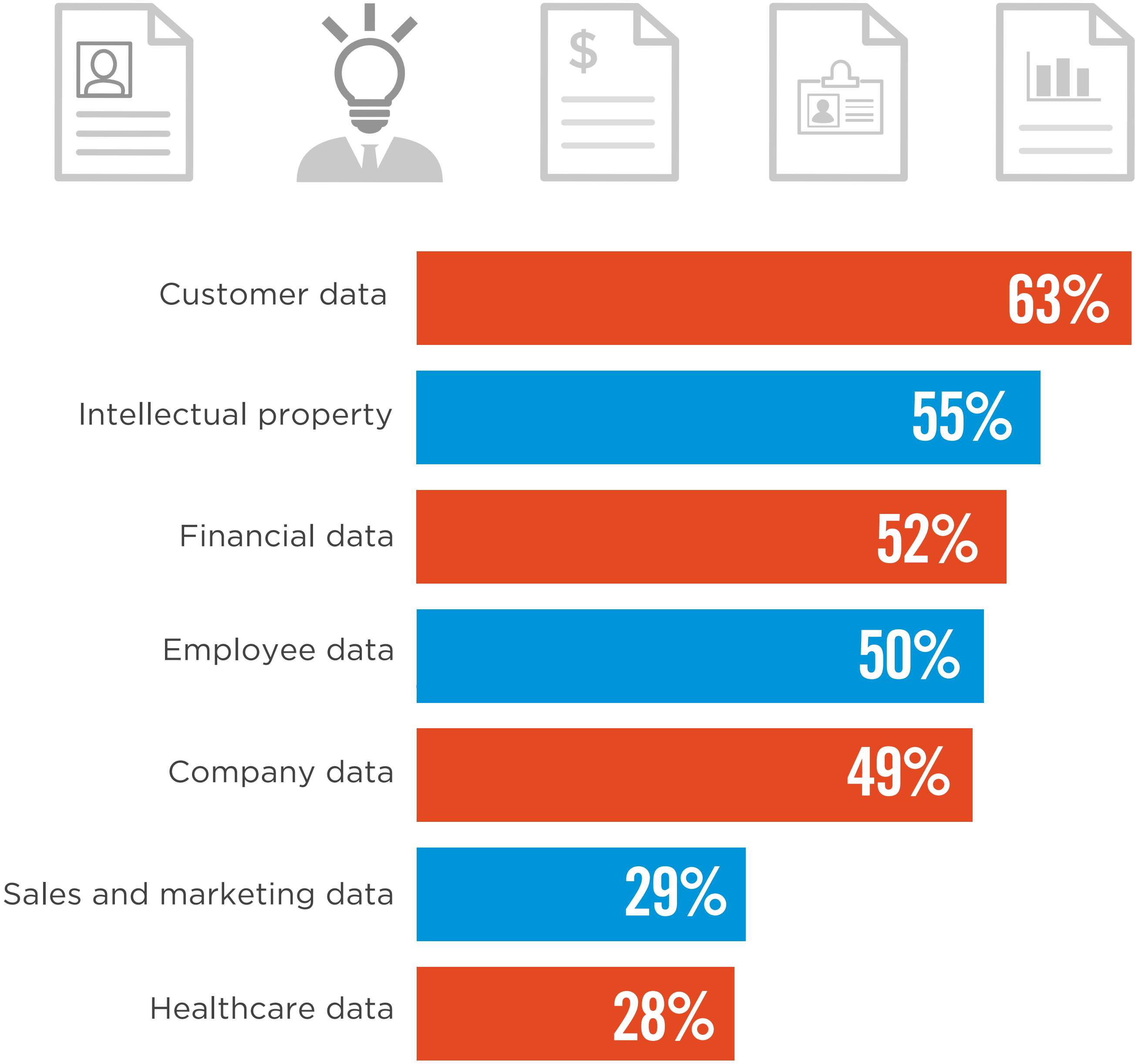
In your opinion, what types of applications are most vulnerable to insider attacks?



MOST VULNERABLE DATA

Data is a core strategic asset and some types of data are more valuable than others as a target of insider attacks. This year, customer data (63%) takes the top spot as data most vulnerable to insider attacks, followed by intellectual property (55%) and financial data (52%).

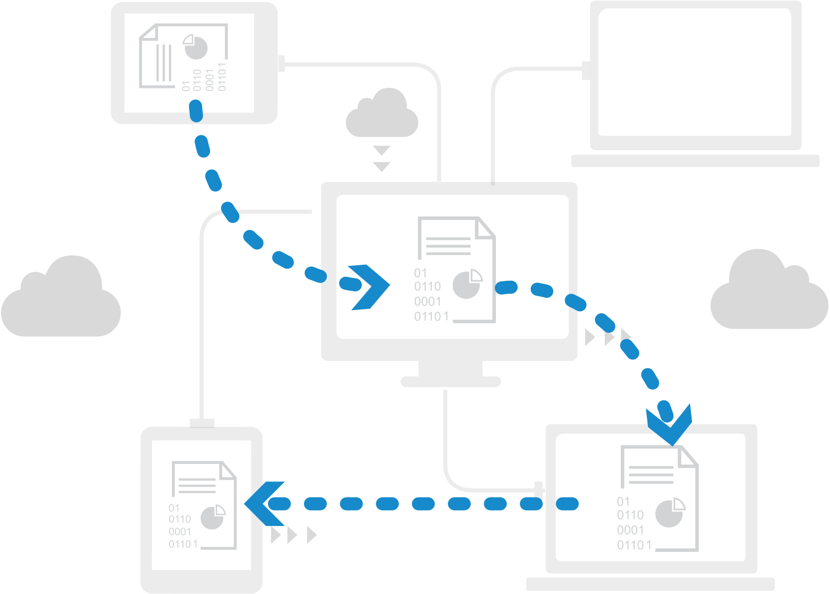
What types of data are most vulnerable to insider attacks?

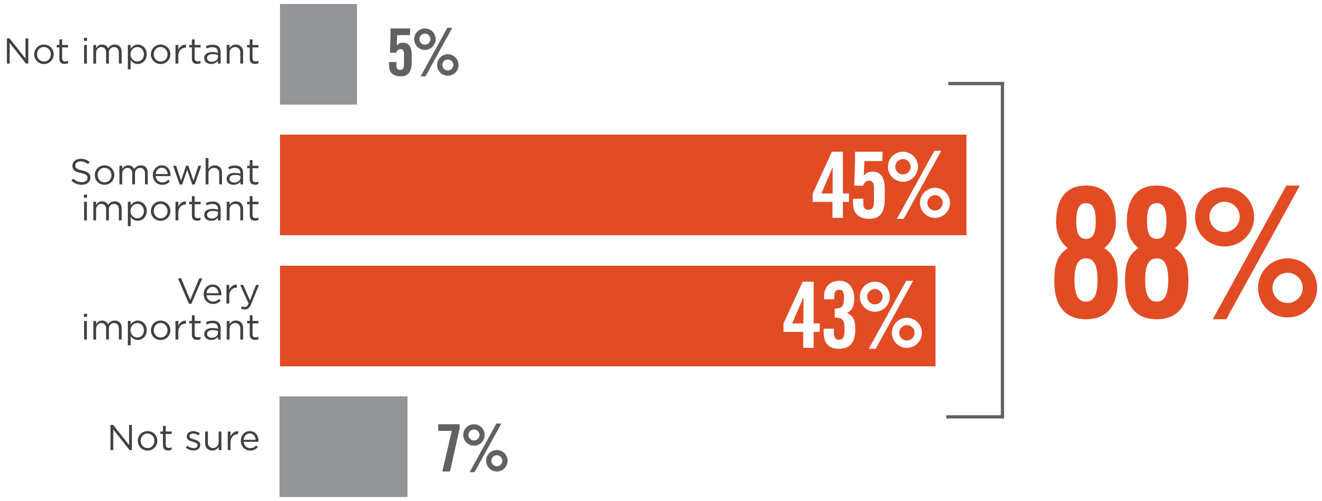


FILE TRACKING

Tracking the movement of sensitive files across the network is somewhat important to very important to 88% of organizations.

How important is tracking file movement across your network for your data security strategy?

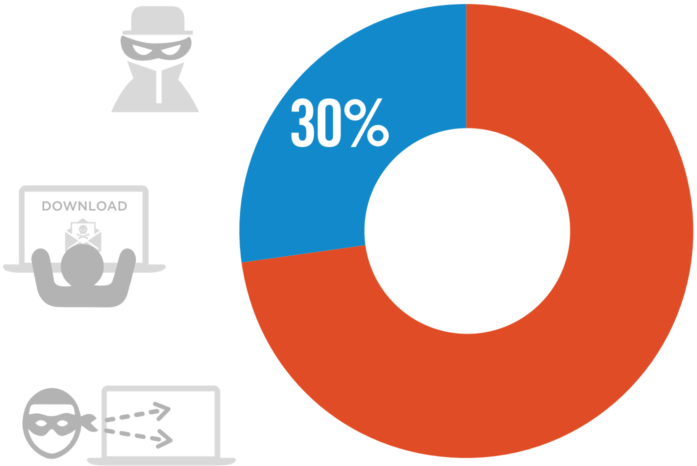




RISE OF INSIDER ATTACKS

A significant majority of organizations (70%) observed that insider attacks have become more frequent over the last 12 months. In fact, 60% have experienced one or more insider attacks within the last 12 months.

Do you think insider attacks have generally become more frequent over the last 12 months?

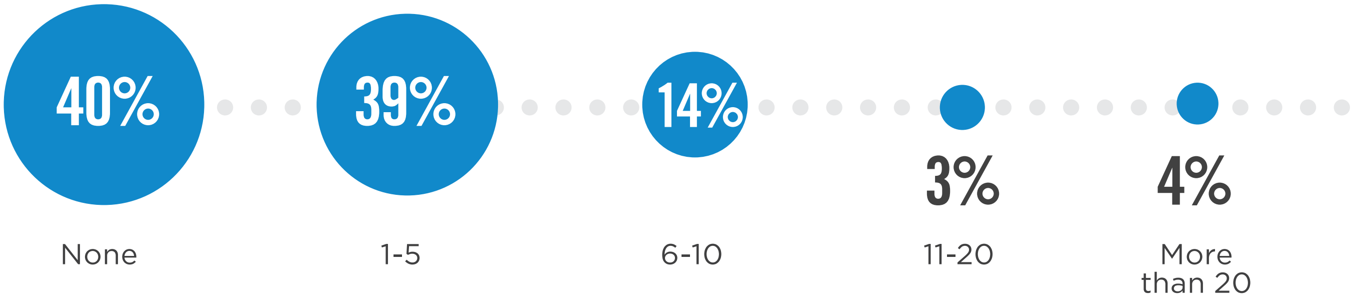


70%

Think insider attacks have become more frequent in the past 12 months.

🟧 Yes 🟦 No

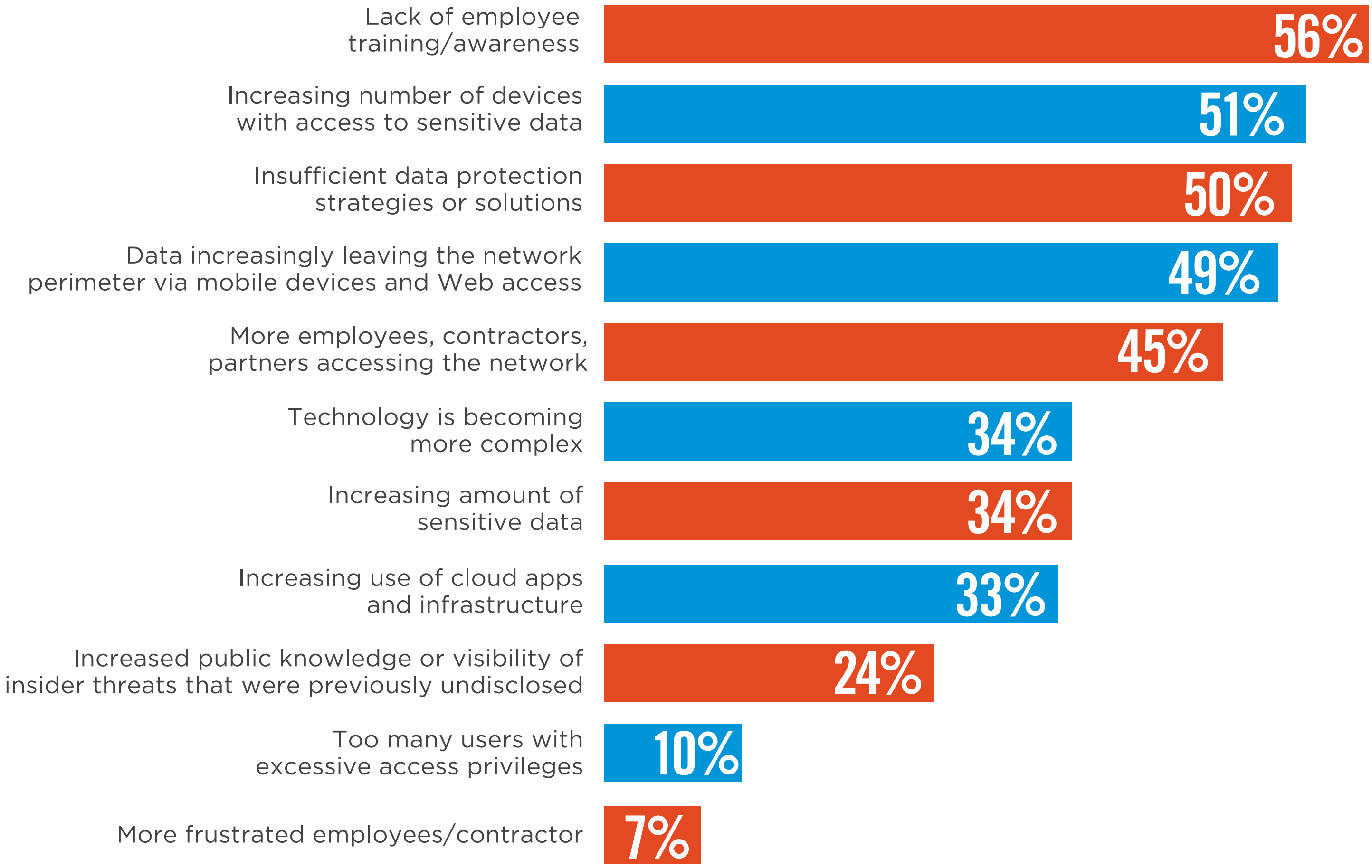
How many insider attacks did your organization experience in the last 12 months?



CONTRIBUTING FACTORS

Fifty-six percent believe the most critical factor enabling insider attacks is the lack of employee awareness and training. Another key factor is the proliferation of devices with access to sensitive data (51%), enabling data to leave the traditional perimeter more easily.

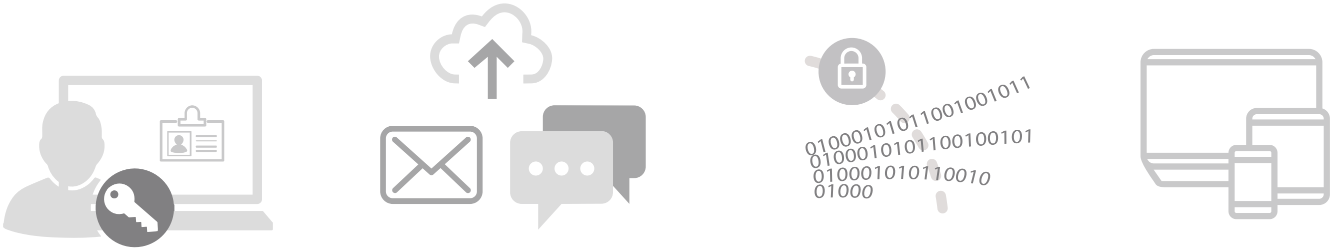
What do you believe are the main reasons behind insider attacks?

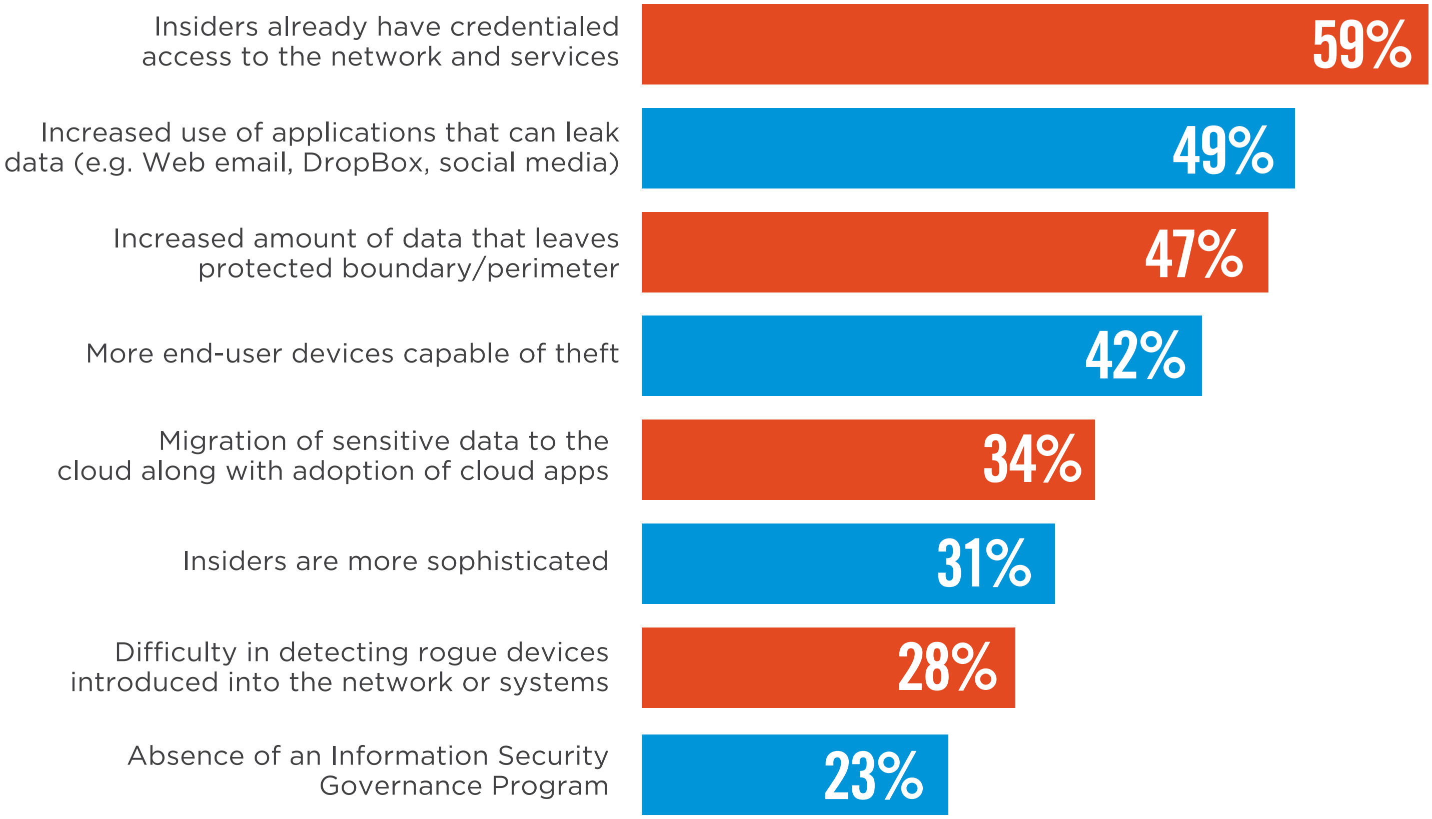


DETECTION AND PREVENTION

Because insiders often have elevated access privileges to sensitive data and applications, it becomes increasingly difficult to detect malicious insider activity (59%). Combined with the proliferation of data sharing apps (49%) and more data leaving the traditional network perimeter (47%), the conditions for successful insider attacks are becoming more difficult to control.

What makes the detection and prevention of insider attacks increasingly difficult compared to a year ago?



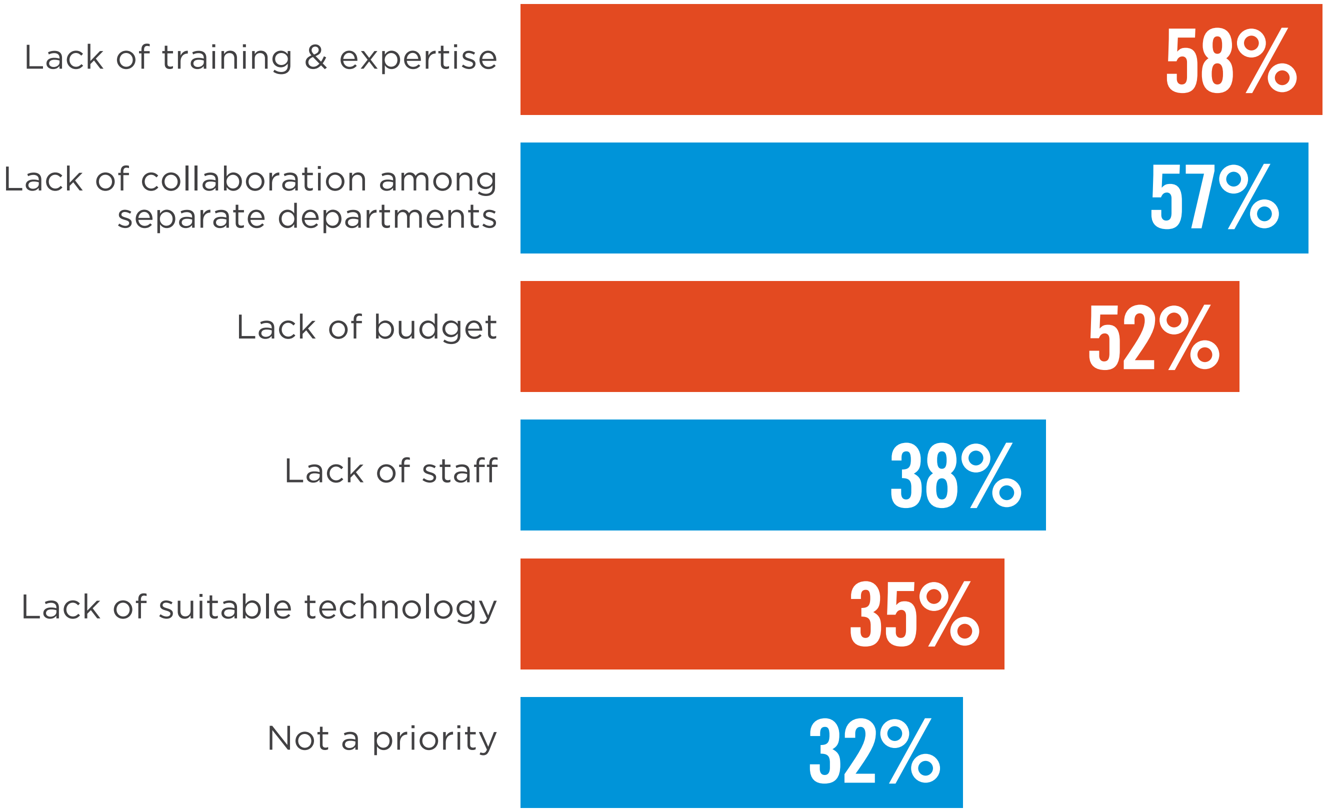


Insiders already have credentialed access to the network and services
59%
Increased use of applications that can leak data (e.g. Web email, DropBox, social media)
49%
Increased amount of data that leaves protected boundary/perimeter
47%
More end-user devices capable of theft
42%
Migration of sensitive data to the cloud along with adoption of cloud apps
34%
Insiders are more sophisticated
31%
Difficulty in detecting rogue devices introduced into the network or systems
28%
Absence of an Information Security Governance Program
23%

BARRIERS TO INSIDER THREAT MANAGEMENT

Lack of training and expertise (58%) are perceived as the key barrier to better insider threat management. Other important barriers include the lack of collaboration among departments (57%) and lack of budget (52%). Notably, lack of suitable technology continues to decline in importance as a barrier to better insider threat management (35%).

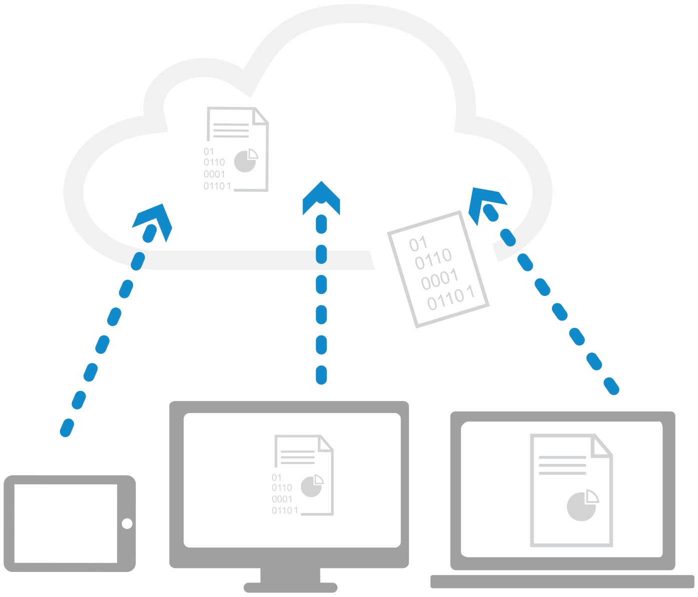
What are the biggest barriers to better insider threat management?



INSIDER ATTACKS IN THE CLOUD

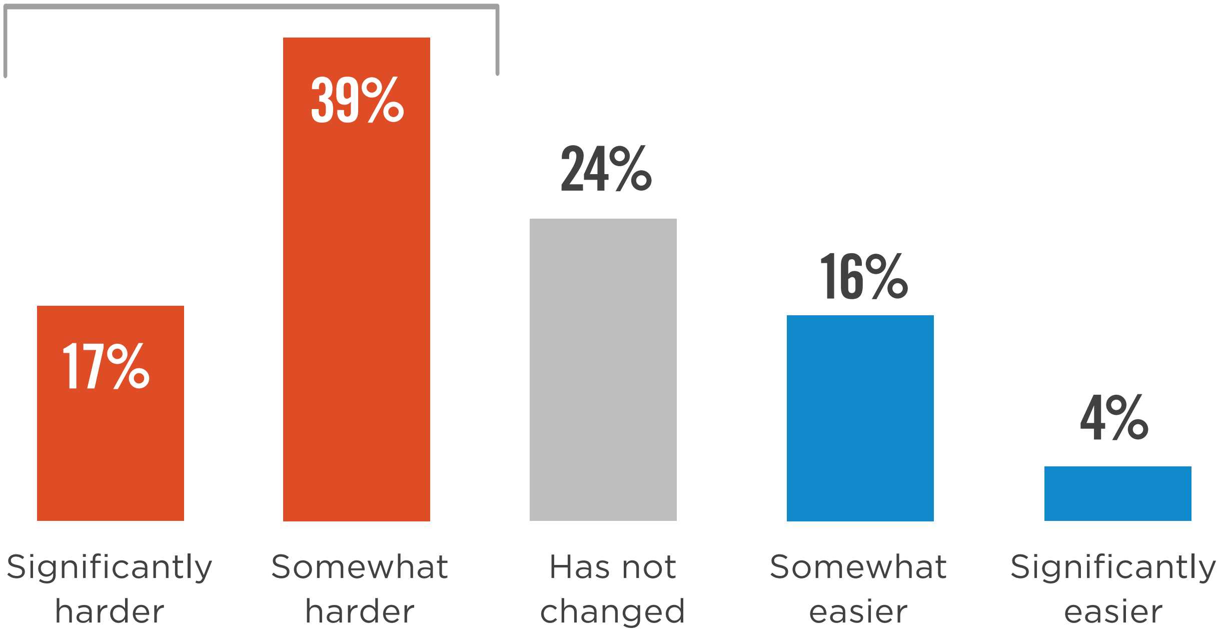
The shift to cloud computing is making the detection of insider attacks more difficult, as confirmed by 56% of cybersecurity professionals.

Since migrating to the cloud, detecting insider attacks is...



56%

Believe that detecting insider attacks has become significantly to somewhat harder.



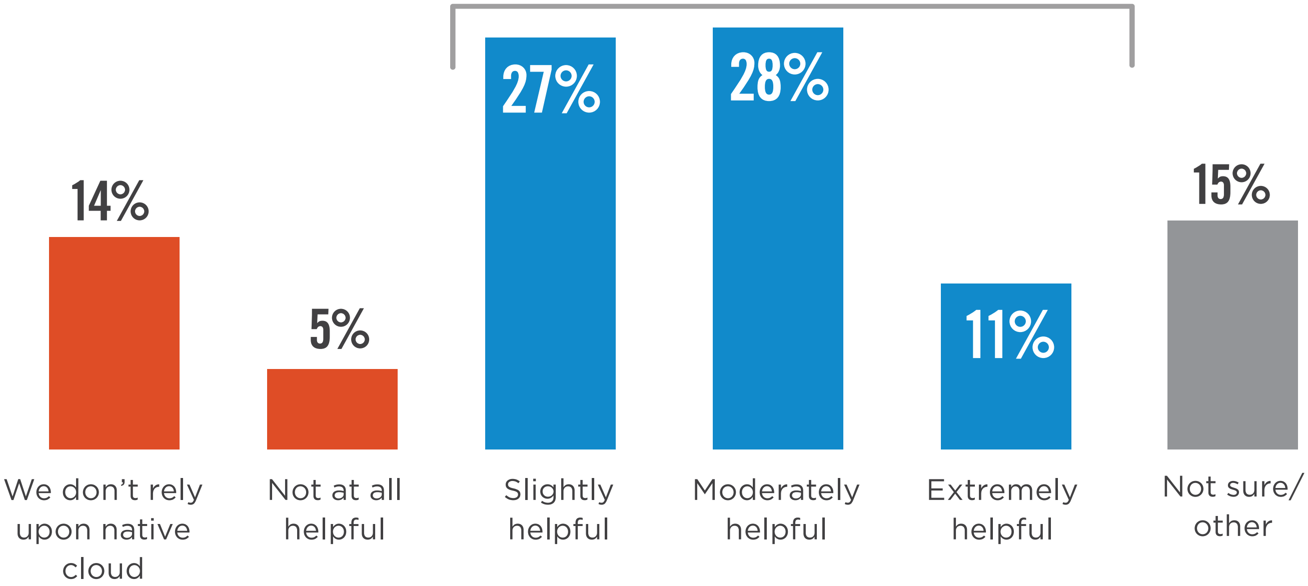
NATIVE CLOUD FUNCTIONALITY

Sixty-six percent of cybersecurity professionals agree that native cloud features are helpful for the detection of insider attacks.

▶ **For detecting insider attacks, native cloud app functionality is ...**

66%

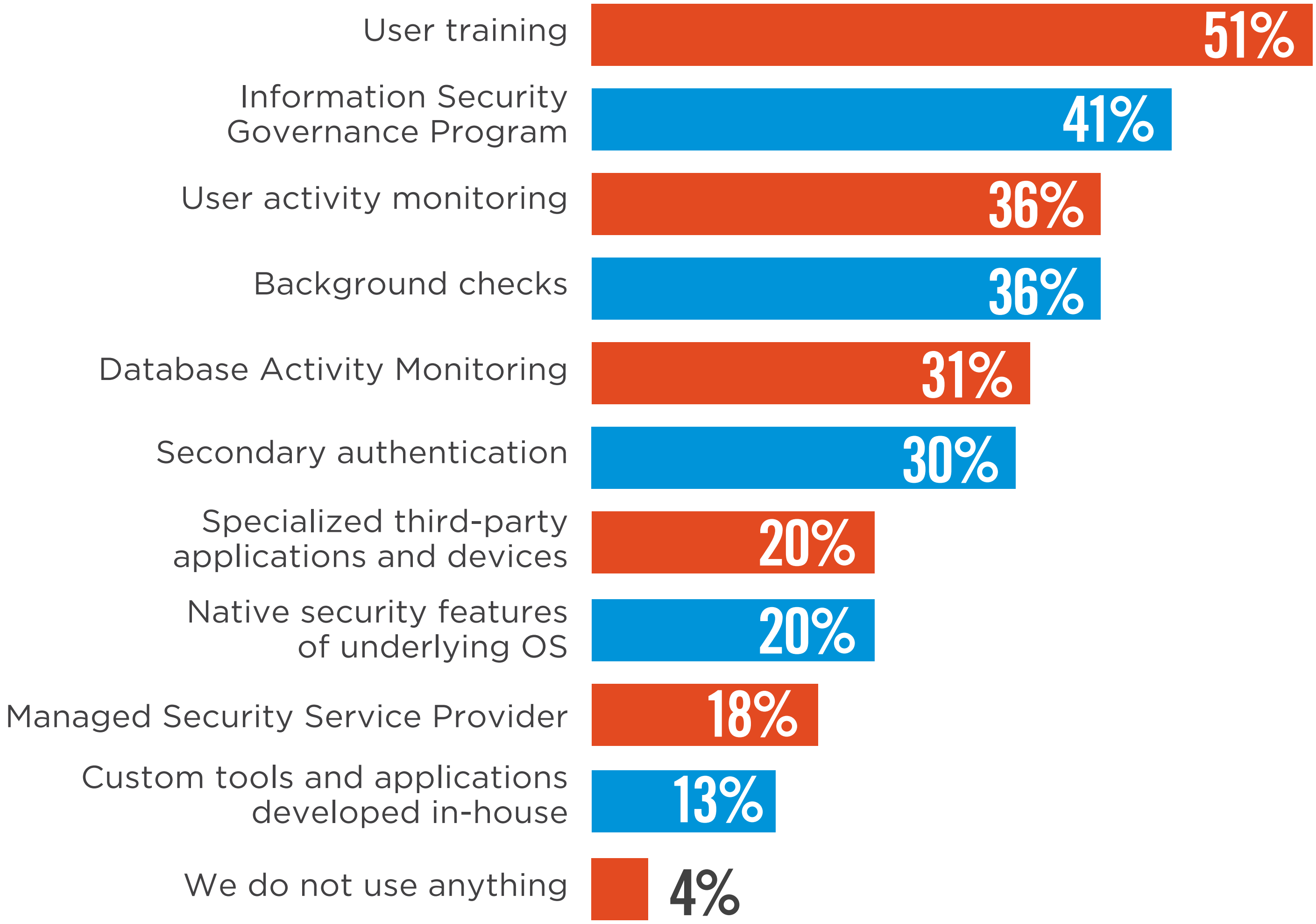
Agree that native cloud features are helpful for the detection of insider attacks.



COMBATING INSIDER THREATS

The most utilized tactic in combating insider threats is user training (51%) to address both inadvertent insider threats due to human error as well as recognizing unusual and suspicious behavior often exhibited by malicious insiders. This is followed by dedicated Information Security Governance Programs to systematically address insider threats (41%) and user activity monitoring (36%) tying with background checks.

How does your organization combat insider threats today?

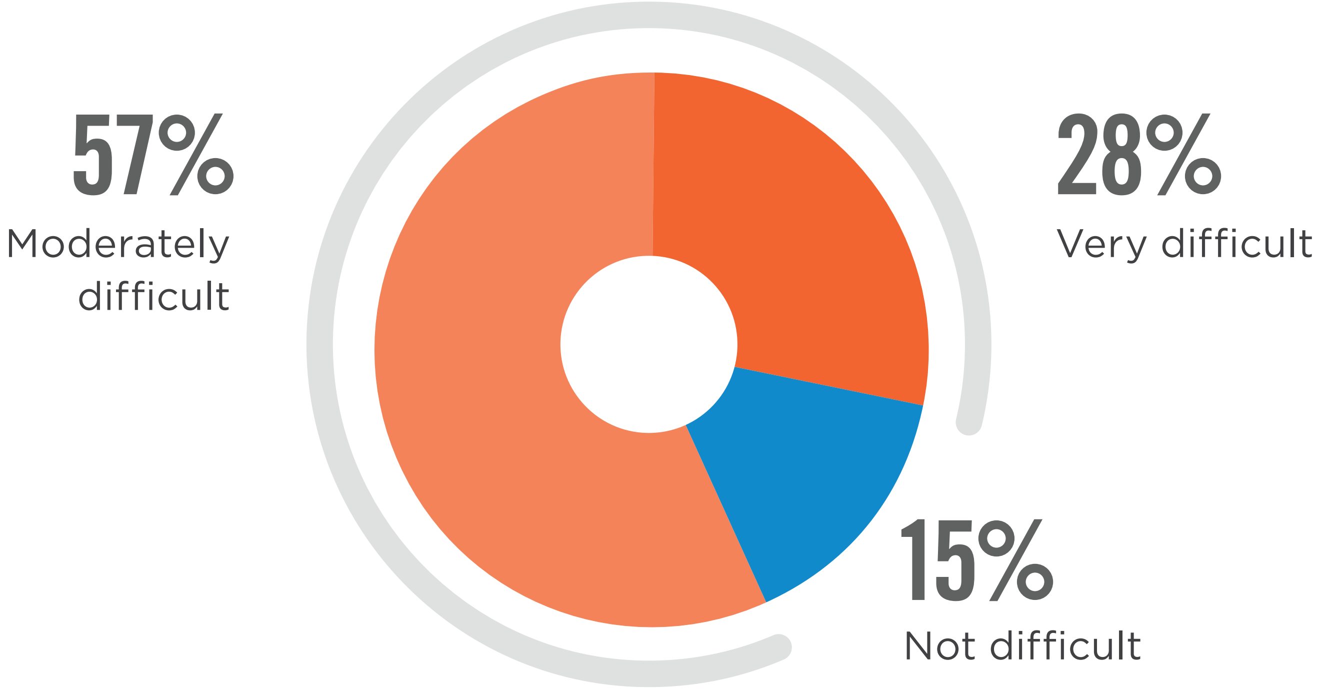


DAMAGES FROM INSIDER ATTACKS

Eighty-five percent of organizations find it moderately difficult to very difficult to determine the actual damage of an insider attack.

▶ **Within your organization, how difficult is it to determine the actual damage of an occurred insider attack?**

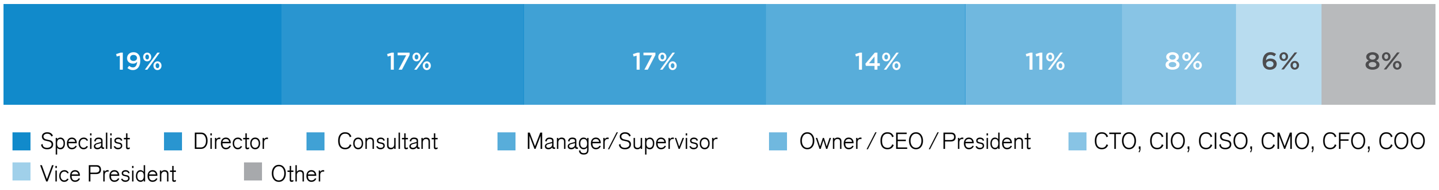
85% Find it moderately difficult to very difficult to determine the actual damage of an insider attack.



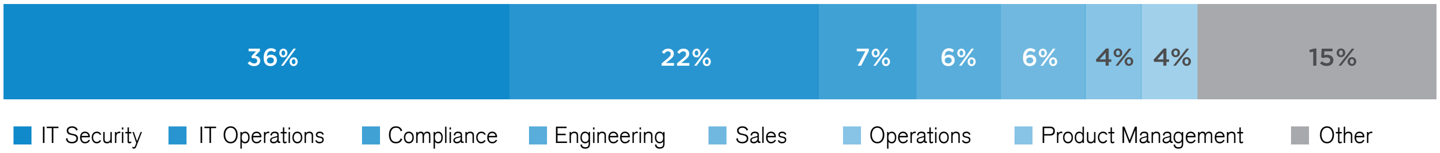
METHODOLOGY & DEMOGRAPHICS

This Insider Threat Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in June of 2019 to gain deep insight into the latest trends, key challenges and solutions for insider threat management. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

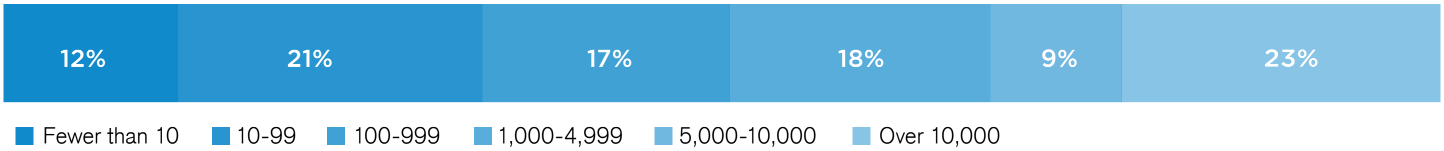
CAREER LEVEL



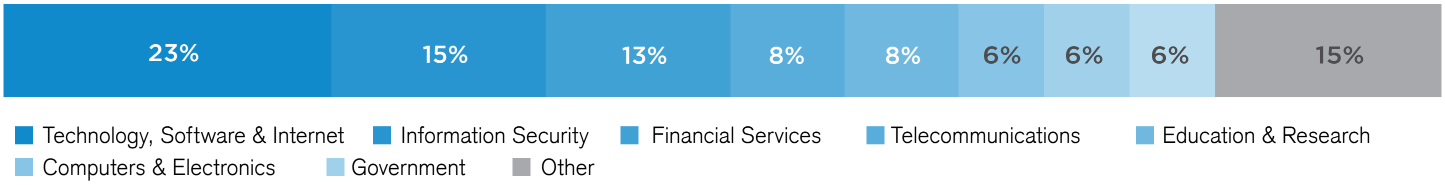
DEPARTMENT



COMPANY SIZE



INDUSTRY



NUCLEUS CYBER

Nucleus Cyber is the intelligent data-centric security solution for the modern workplace providing dynamic, granular data security that leverages existing infrastructure investments. The NC Protect platform dynamically adjusts file security based on real-time comparison of user context and file content to enforce data governance policies for more secure collaboration. It minimizes data loss and misuse risk for a wide range of digital environments including Microsoft SharePoint, Office 365, Teams, Yammer, Dropbox and file shares, to provide a single, centralized data security solution.

For more information visit **www.nucleuscyber.com**
or follow **@nucleuscyber.**