

2019

Cybersecurity  
INSIDERS

# INSIDER THREAT REPORT



# INTRODUCTION

Insider threats have evolved into some of the costliest and most challenging risks facing organizations today.

In part, this shift is due to the fact that many organizations lack the ability to monitor risks associated with those trusted employees and contractors who act unwittingly or negligently. Making matters worse, the actions of well-concealed malicious insiders are frequently lost in daily waves of false-positive alerts and other noise generated by conventional security analytics solutions and tactics.

This important new report makes clear that an effective insider risk mitigation program can't rely solely on tools designed for detecting external threats, or isolated anomalies. It also shows that companies increasingly grasp the need for their analytics solutions to focus on information sources that provide evidence of human behavior and attitudes — rather than on network logs and device activity — as a means of getting ahead of their biggest threats.

The underlying theme here is what's referred to on page 10 of this report as “holistic risk management,” a new approach that places equal emphasis on “training, collaboration and awareness” on the one hand and “technology to automate detection, analysis and prevention of insider threats” on the other. We couldn't agree more.

Our sincere thanks go to Cybersecurity Insiders for conducting the online survey that underpins this report — and to everyone who took the time to think deeply about and answer its detailed questions.

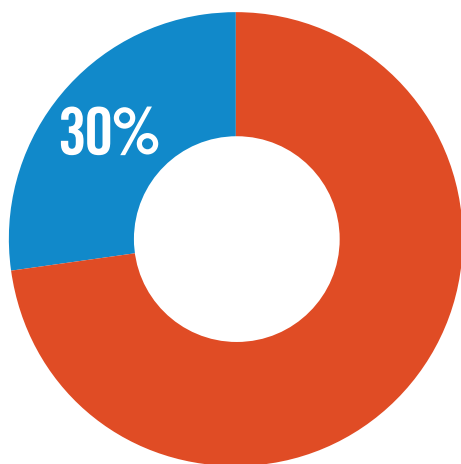
We hope you find this report informative, and useful to your own organization.

The Haystax Team

# 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.

## ► Have insider attacks become more or less frequent over the last 12 months?

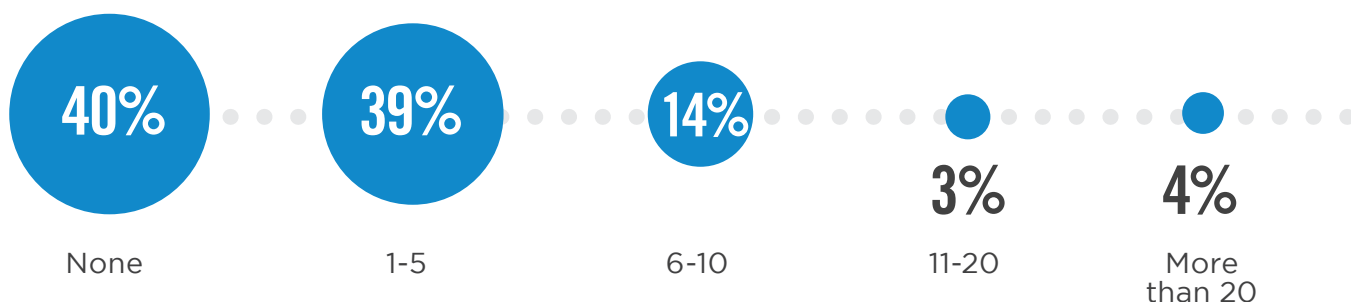


# 70%

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?



# 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 bad actors (62%). The ideal insider threat solution should detect and address all insider threats, regardless of the underlying motivation or cause.

## ► 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)

Other 2%

# 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.

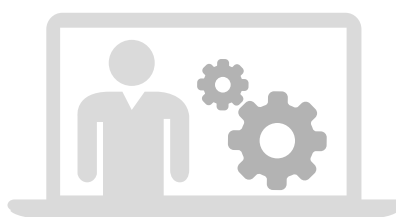
The survey indicates that privileged IT users (59%) pose the biggest insider security risk to organizations, followed by contractors (52%), regular employees and privileged business users (tied at 49%). Look for insider threat solutions that allow for profiling and anomaly detection within these defined groups.

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



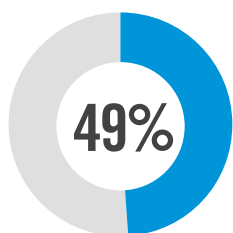
**59%**

**Privileged IT  
users/admins**

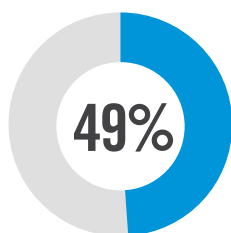


**52%**

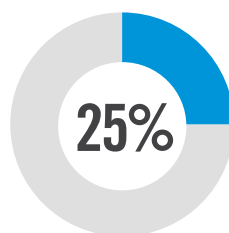
**Contractors/  
service providers/  
temporary workers**



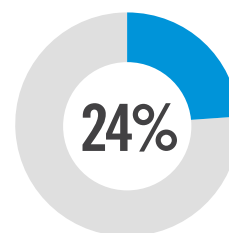
Regular  
employees



Privileged  
business users/  
executives



Other IT  
staff



Executive  
managers

Business partners 16% | Customers/clients 15% | None 5% | Not sure/other 5%

# MOTIVATIONS FOR INSIDER ATTACKS

To understand malicious insider threats, it is important to look at the underlying motivations of insiders. Our survey panel considers fraud (57%) and the resulting monetary gain (50%) the biggest factors that drive malicious insiders, followed by theft of intellectual property (43%). The ideal insider threat solution captures threats from all of these vectors, including financial, personal and professional stressors as indicators that a person is at risk or already an active insider threat.

## ► What motivations for malicious insider threats are you most concerned about?



57%

Fraud



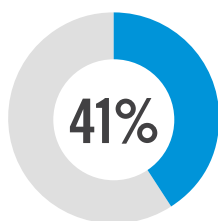
50%

Monetary  
gain

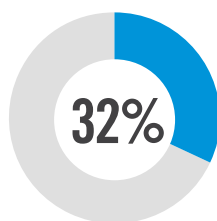


43%

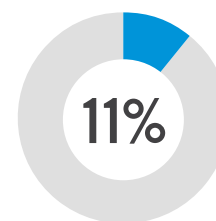
IP theft



Sabotage



Espionage



Professional  
benefit

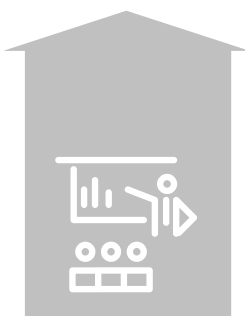
Not sure/other 8%

# 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.

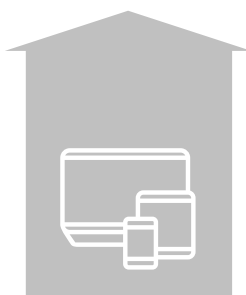
## ► What do you believe are the main reasons behind insider attacks?

56%



Lack of employee training/awareness

51%

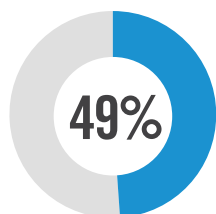


Increasing number of devices with access to sensitive data

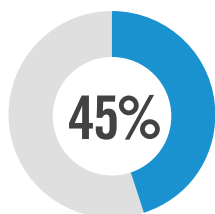
50%



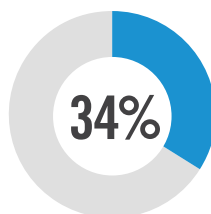
Insufficient data protection strategies or solutions



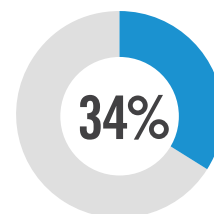
Data increasingly leaving the network perimeter via mobile devices and Web access



More employees, contractors, partners accessing the network



Technology is becoming more complex



Increasing amount of sensitive data

Increasing use of cloud apps and infrastructure 33% | Increased public knowledge or visibility of insider threats that were previously undisclosed 24% | Too many users with excessive access privileges 10% | More frustrated employees/contractors 7% | Not sure/other 10%

# DEPARTMENTS AT RISK

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

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



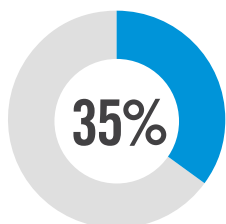
37%

Finance

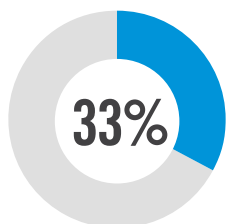


37%

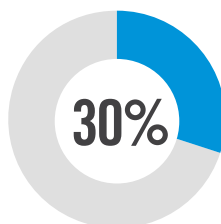
Support/customer  
success



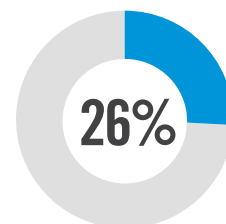
General  
administration



Sales



Human  
resources



Board of directors/  
executive  
management team

Marketing 26% | Research and Development 24% | Legal 9% | Other 11%



# 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?



**63%**

Customer  
data



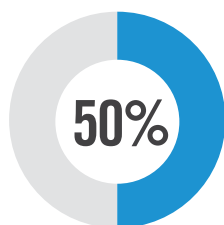
**55%**

Intellectual  
property

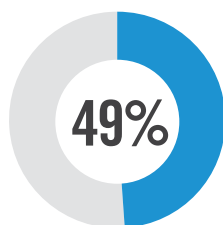


**52%**

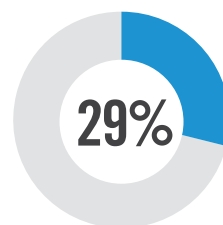
Financial  
data



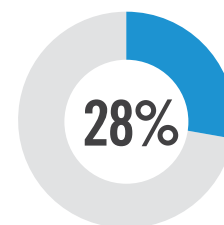
Employee  
data



Company  
data



Sales and  
marketing data



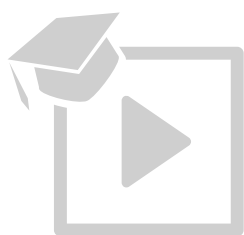
Healthcare  
data

Not sure/other 4%

# BARRIERS TO INSIDER THREAT MANAGEMENT

Lack of training and expertise (58%) remains 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%). This reinforces the need for holistic risk management where organization-wide training, collaboration and awareness are equally important as technology to automate detection, analysis and prevention of insider threats.

## ► What are the biggest barriers to better insider threat management?



**58%**

Lack of training  
& expertise



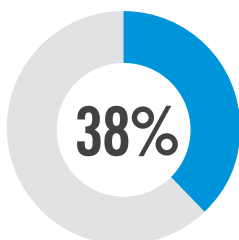
**57%**

Lack of collaboration  
between separate  
departments

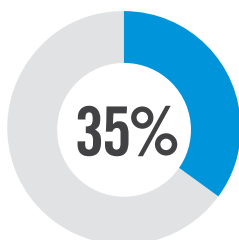


**52%**

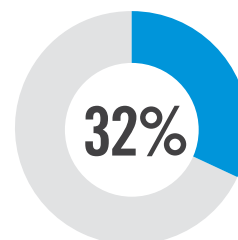
Lack of  
budget



Lack of staff



Lack of suitable  
technology



Not a priority

Not sure/other 6%

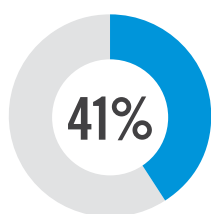
# COMBATING INSIDER THREATS

The most utilized tactic in combating insider threats is user training (51%) because it addresses both inadvertent insider threats as well as the human factor of recognizing insider attacks by the 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%).

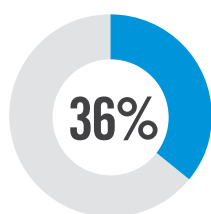
## ► How does your organization combat insider threats today?



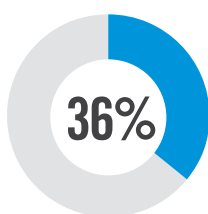
**51%**  
User training



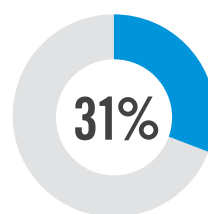
Information  
Security  
Governance  
Program



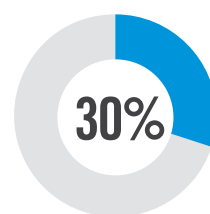
User activity  
monitoring



Background  
checks



Database  
Activity  
Monitoring



Secondary  
authentication

Specialized third-party applications and devices 20% | Native security features of underlying OS 20% | Managed Security Service Provider 16% | Custom tools and applications developed in-house 13% | We do not use anything 4% | Not sure/other 10%

# FOCUS ON DETERRENCE

While all methods of countering insider threats are important, organizations are shifting their focus towards deterrence of internal threats (62%) and less so on detection (60%) and post breach analysis (47%).

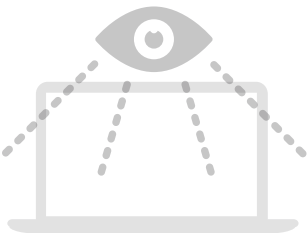
► What aspect(s) of insider threat management does your organization mostly focus on?



62%

## Deterrence

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



60%

## Detection

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



47%

## Analysis and post breach forensics

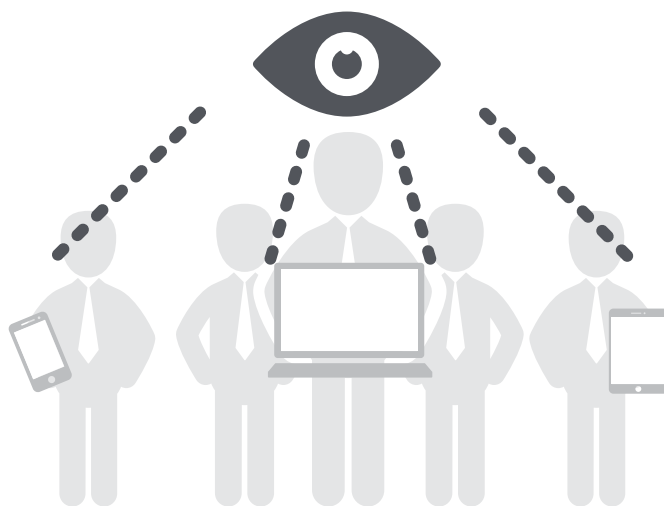
(e.g. SIEM, log analysis, etc.)

Deception (e.g., honeypots, etc.) 10% | None 6% | Other 2%

# USER BEHAVIOR MONITORING

The increasing volume of insider threats has caused cybersecurity professionals to take more proactive steps and deploy User Behavior Analytics (UBA) tools to detect, classify and alert anomalous behavior. Eighty-four percent of organizations monitor user behavior in one way or another, most commonly utilizing access logging (36%) and automated user behavior monitoring (27%).

## ▶ Do you monitor user behavior?



**38%**  
**YES**, but access  
logging only

**23%**  
**YES**, we use automated  
tools to monitor user  
behavior 24x7

**14%**  
**YES**, but only under  
specific circumstances  
(e.g., shadowing specific users)

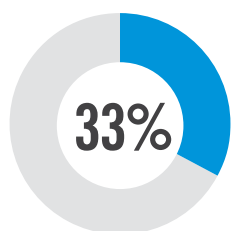
**19%**  
**NO**, we don't monitor  
user behavior at all

**7%**  
**YES**, but only after an incident  
(e.g., forensic analysis)

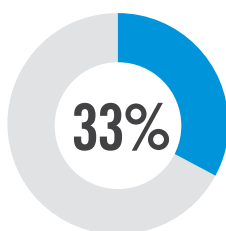
# VISIBILITY INTO USER BEHAVIOR

Organizations rely most commonly on server logs to track user behavior (45%), followed by dedicated user activity monitoring solutions (33%), and monitoring features natively provided by the business apps (30%).

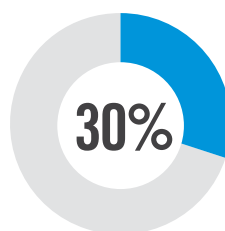
► What level of visibility do you have into user behavior within core applications?



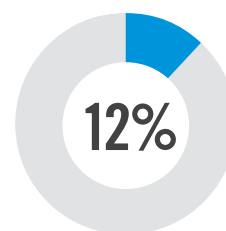
Have deployed  
user activity  
monitoring



In-app audit  
system/feature



No visibility  
at all



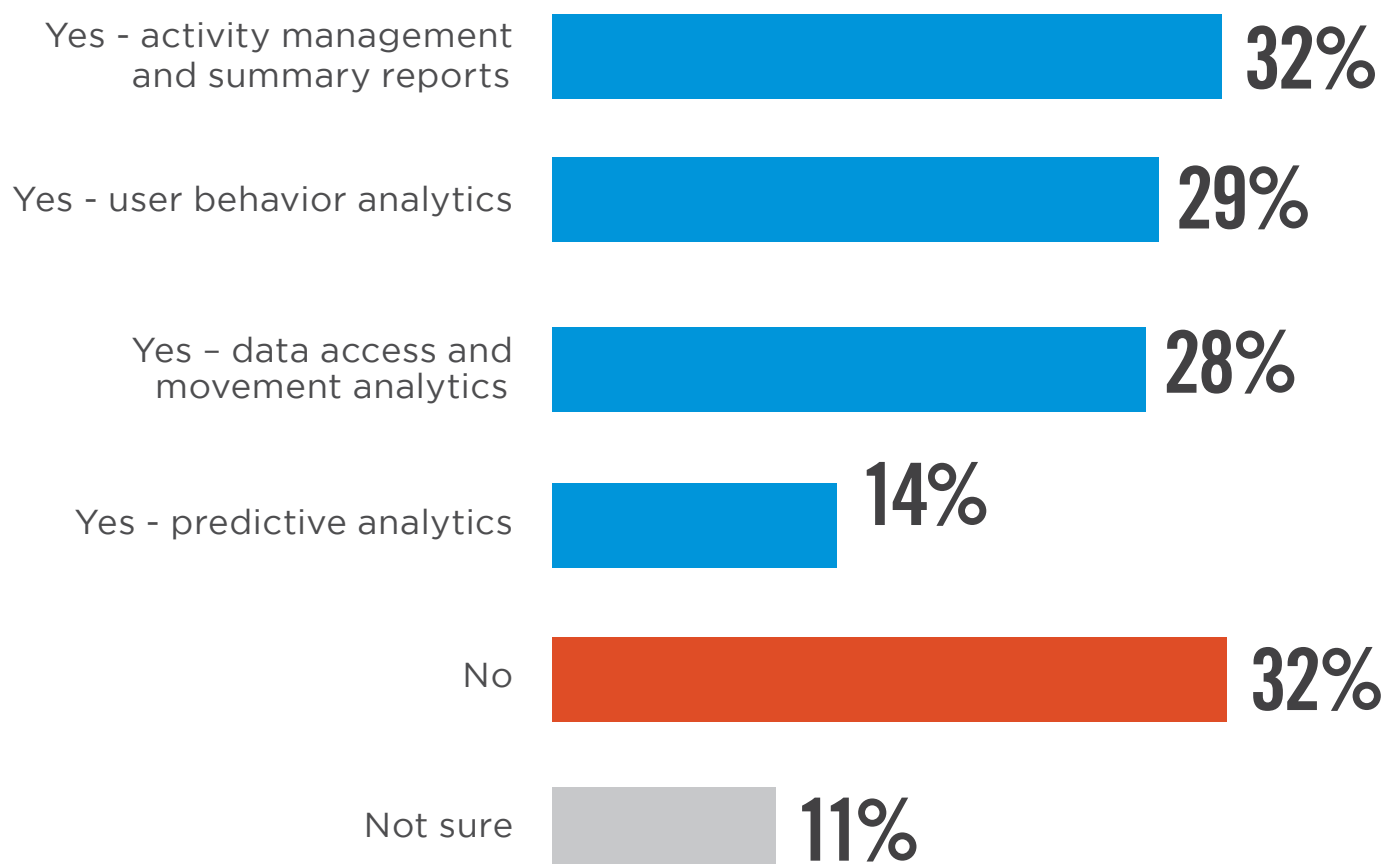
Have deployed  
keylogging

Not sure/other 15%

# INSIDER THREAT ANALYTICS

A majority of organizations utilize some form of analytics to determine insider threats, including activity management and reports (32%), user behavior analytics (29%), and data access and movement analytics (28%).

## ▶ Does your organization leverage analytics to determine insider threats?



# MOST EFFECTIVE TOOLS & TACTICS

The three most effective security tools and tactics deployed by organizations to protect against insider threats are tied for the number one spot: data loss prevention (DLP) (52%), identity and access management (IAM) (52%), and policies and training (52%). Forty-four percent of organizations utilize user behavior analytics (UBA) to strengthen their insider threat programs.

## ► What are the most effective security tools and tactics to protect against insider attacks?



52%

Data Loss Prevention (DLP)



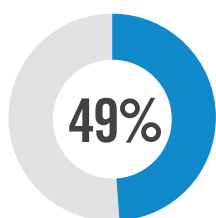
52%

Identity and Access Management (IAM)

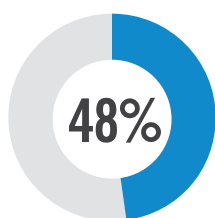


52%

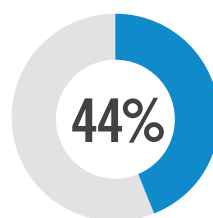
Policies & training



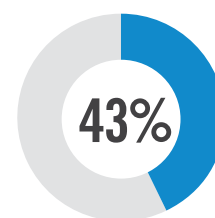
Encryption of data (at rest, in motion, in use)



Multi-factor authentication



User Behavior Analytics (UBA)



Security Information and Event Management (SIEM)

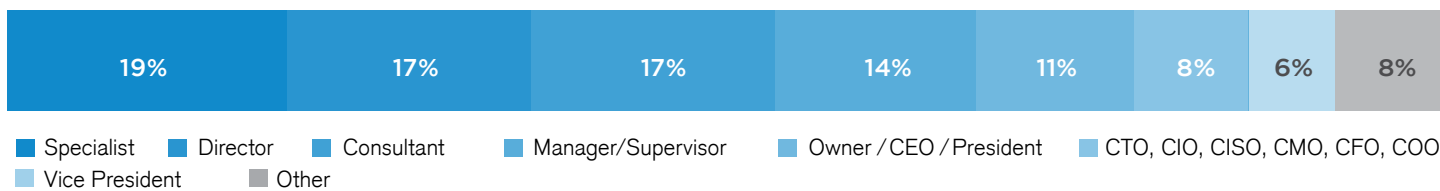
Data Access Monitoring 40% | File Activity Monitoring 40% | Endpoint and mobile security 39% | Security analytics & intelligence 39% | Intrusion Detection and Prevention (IDS/IPS) 37% | Sensitive and Private Data Identification/Classification 36% | Network defenses (firewalls) 35% | User monitoring 33% | Database Activity Monitoring 33% | Password vault/Privileged account vault 23% | Enterprise Digital Rights Management solutions (E-DRM) 20% | Cloud Access Security Broker (CASB) 18% | Tokenization 17% | Cloud Security as a Service 16% | Internal audits 9% | Network monitoring 8% | Whistleblowers 6% | Not sure/Other 9%



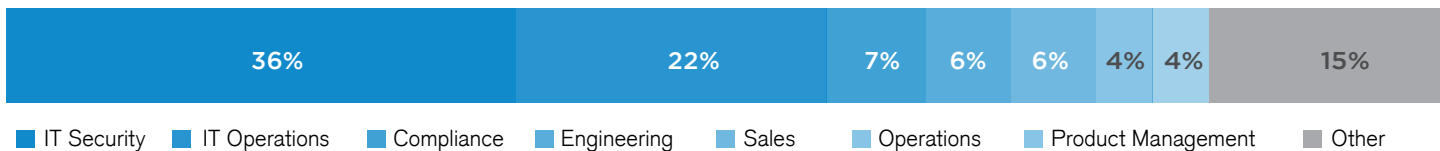
# METHODOLOGY & DEMOGRAPHICS

This Insider Threat Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in June 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.

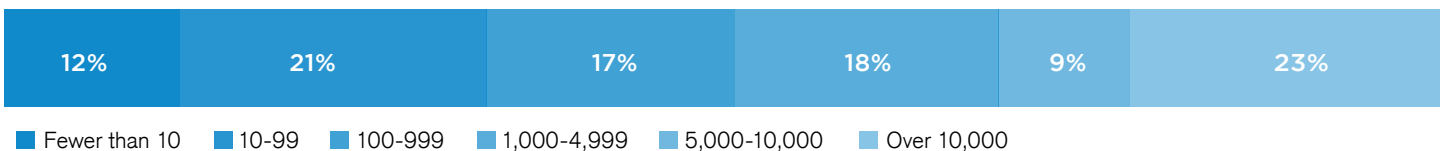
## CAREER LEVEL



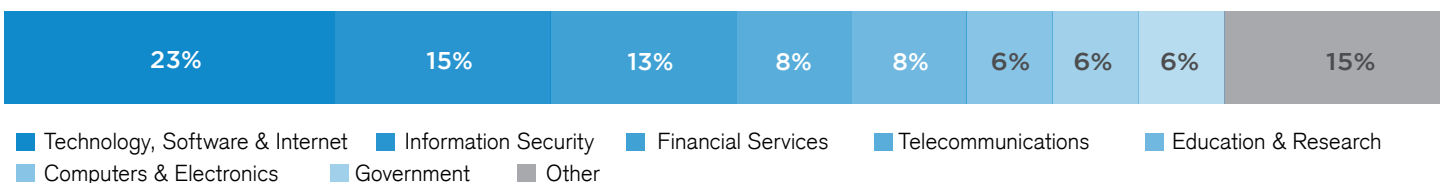
## DEPARTMENT



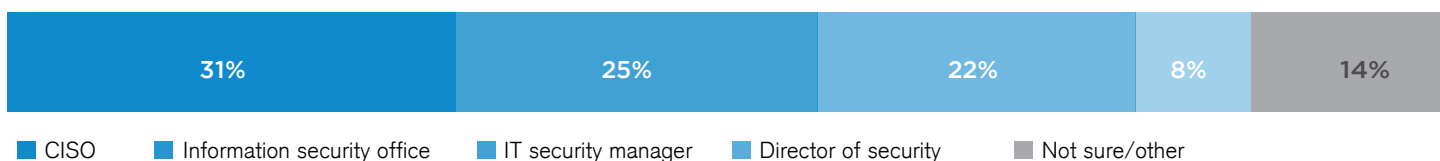
## COMPANY SIZE



## INDUSTRY



## WHO OVERSEES PROGRAMS





Haystax, a wholly-owned subsidiary of Fishtech Group, is a leading security analytics platform provider delivering advanced security analytics and risk management solutions that enable rapid understanding and response to virtually any type of cyber or physical threat.

Based on a patented model-driven approach that applies multiple artificial intelligence techniques, the Haystax Analytics Platform reasons like a team of expert analysts to detect complex threats and prioritize risks in real time at scale.

Top federal government agencies and large commercial enterprises, as well as state and local public-safety organizations, rely on Haystax for more effective protection of their critical systems, data, facilities and people.

[www.haystax.com](http://www.haystax.com)