2019
MID-YEAR

Cybersecurity
INSIDERS

INSIDER THREAT REPORT

helpsystems

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
- 56% consider their monitoring, detecting and responding to insider threats only somewhat effective or worse
- 54% see insider attacks as harder to detect compared to external cyber attacks
- 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 HelpSystems 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 bad actors (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)

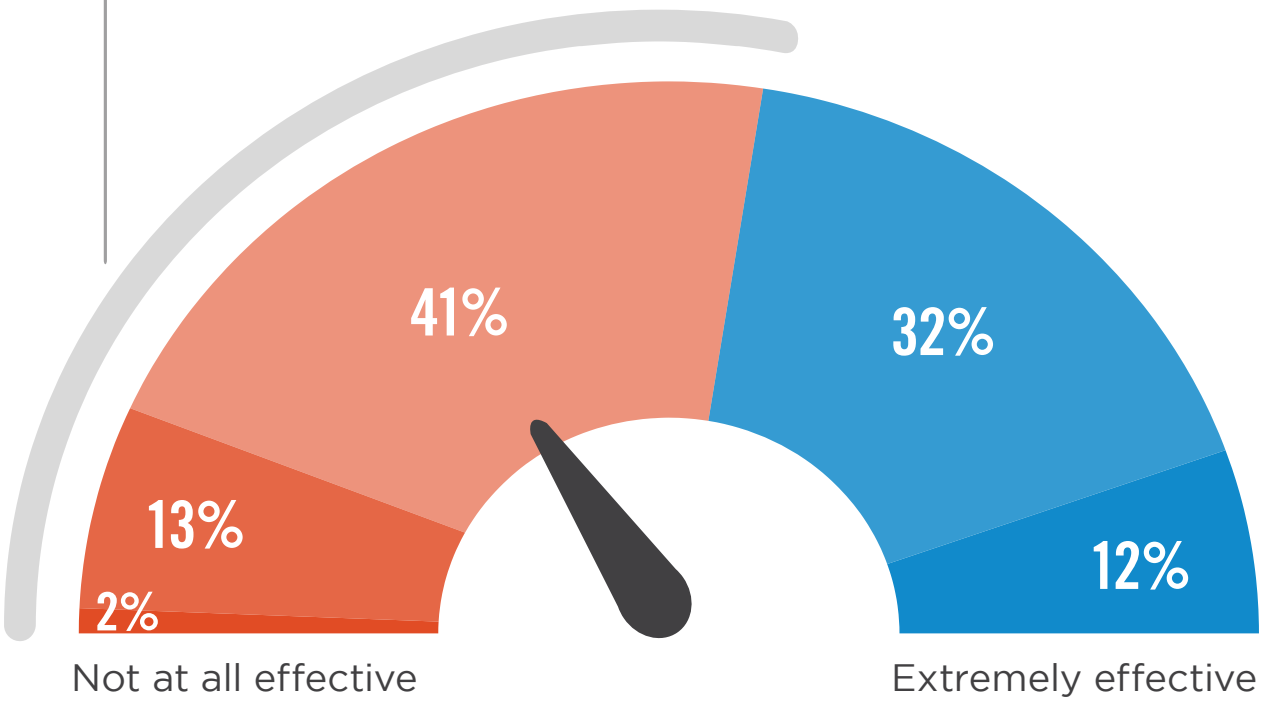
Other 2%

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.

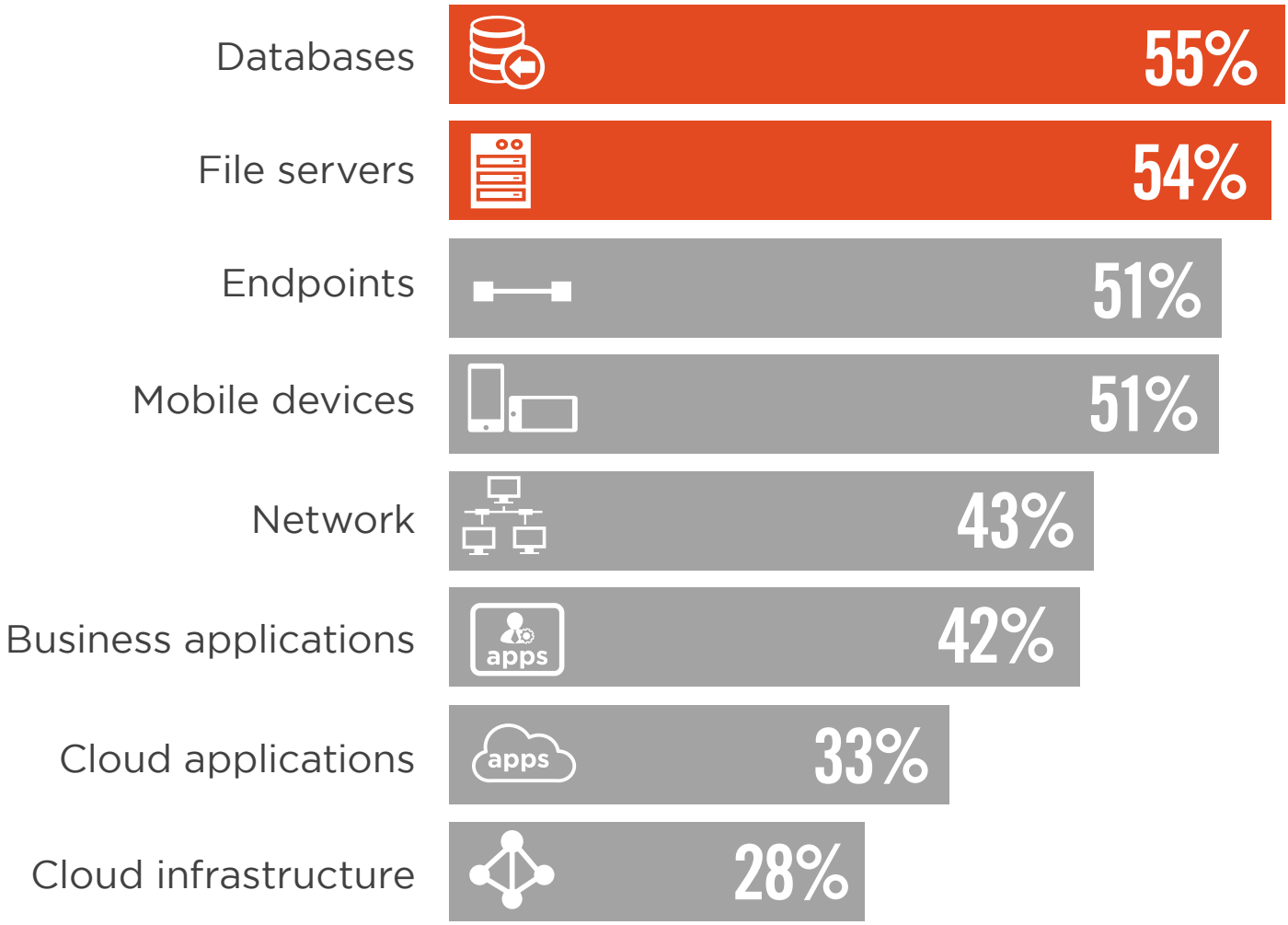


Not at all effective | Not so effective | Somewhat effective | Very effective | Extremely effective

IT ASSETS AT RISK

Cybercriminals see a greater opportunity in targeting where corporate data is located in volume. Databases (55%) and corporate file servers (54%) pose the highest risk, followed by endpoints and mobile devices tying at 51%.

What IT assets are most vulnerable to insider attacks?



Not sure/other 5%

RISKY INSIDERS

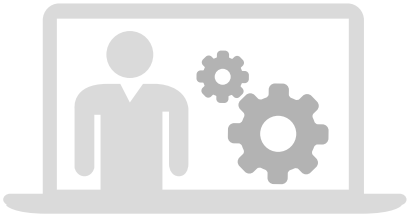
Protecting organizations against cyber threats becomes significantly more challenging when the threats come from within the organization, from trusted and authorized users. It can be difficult to determine when users are simply doing their job function or actually doing something malicious or negligent.

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?

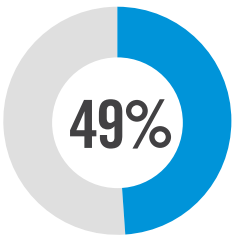
59%

Privileged IT users/admins

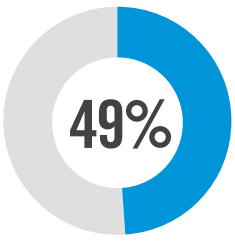


52%

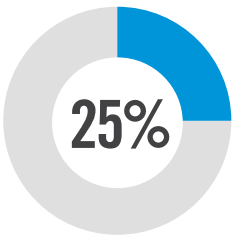
Contractors/ service providers/ temporary workers



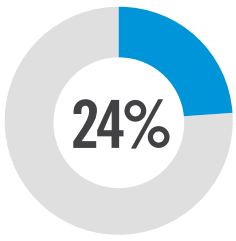
Regular employees



Privileged business users/ executives



Other IT staff



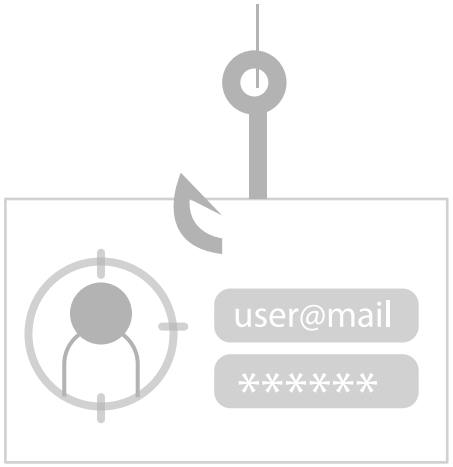
Executive managers

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

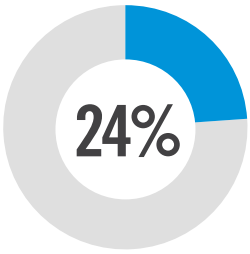
ACCIDENTAL INSIDERS

Cybersecurity experts view phishing attempts (43%) 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.

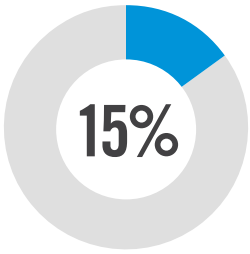
What are the most common accidental insider threats you are most concerned about?



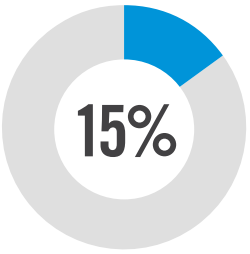
43% Phishing attempts



Poor passwords



Spear-phishing



Orphaned accounts

Other 3%

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?

39%

Cloud storage & file sharing apps

(DropBox, OneDrive, etc.)

38%

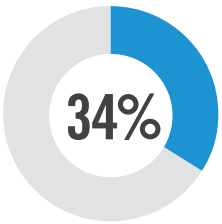
Collaboration & communication

(email, messaging, etc.)

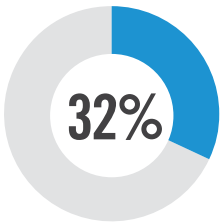
35%

Productivity

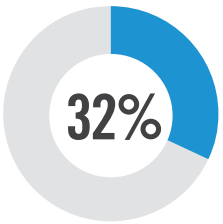
(Office 365, word processing, spreadsheets, etc.)



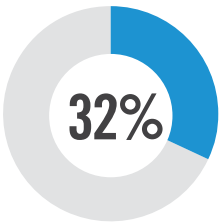
Website



Custom business applications



IT operations



Social media (Facebook, LinkedIn, Twitter, etc.)

Finance & accounting 28% | Cloud applications 27% | Business intelligence/analytics 25% | Sales & marketing (CRM, marketing automation, etc.) 25% | Application development & testing 23% | Content management 22% | HR 21% | Supply chain management 17% | Disaster recovery/storage/archiving 16% | Project management 12% | Not sure/other 3%

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%

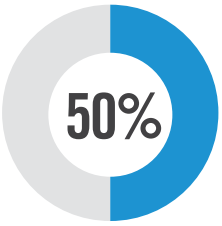
Customer data

55%

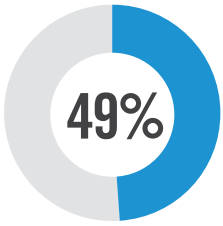
Intellectual property

52%

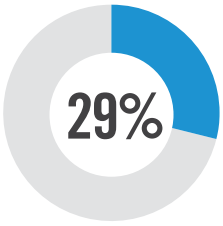
Financial data



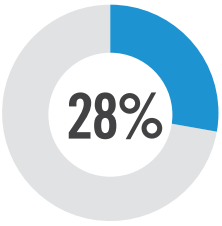
Employee data



Company data



Sales and marketing data



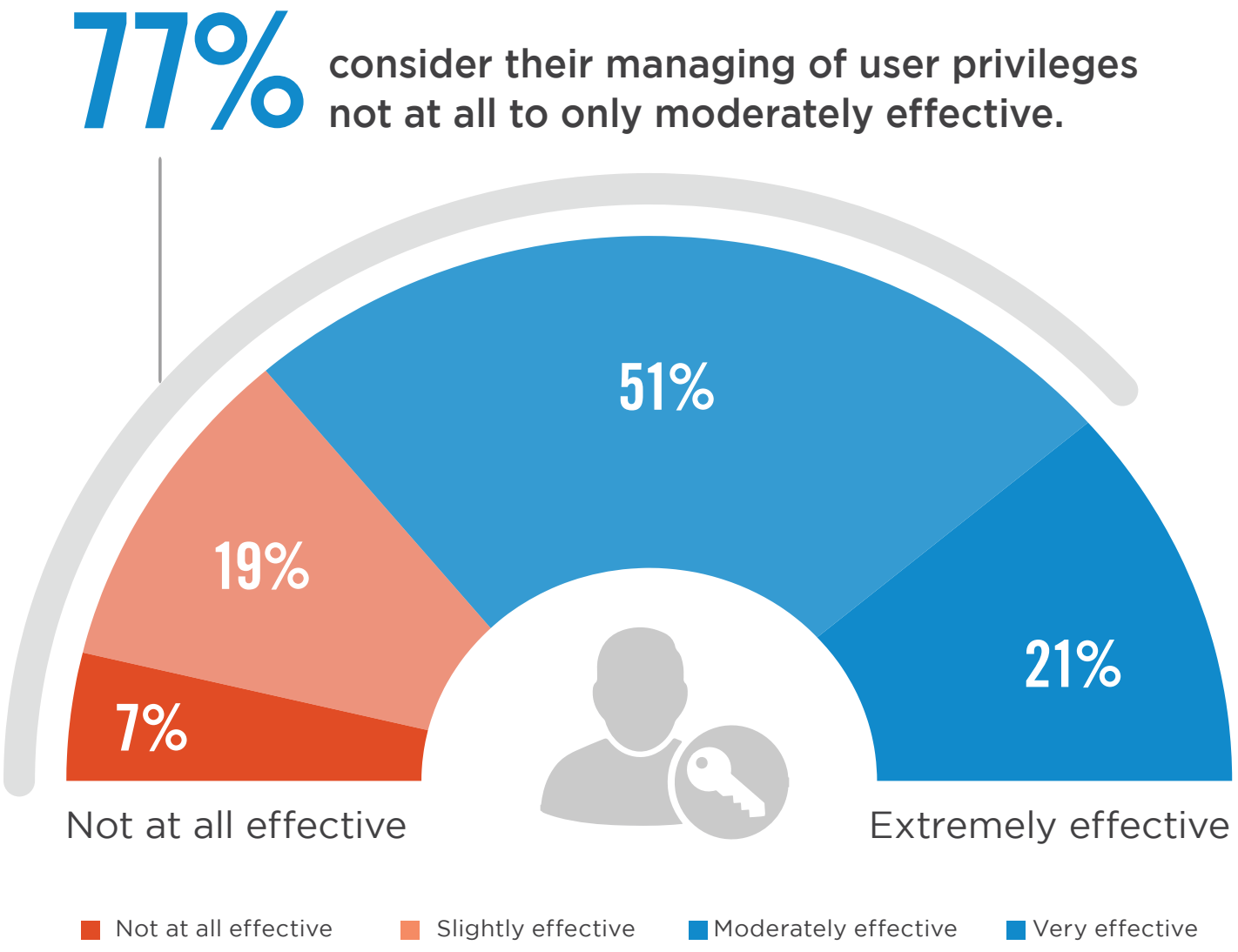
Healthcare data

Not sure/other 4%

MANAGING USER PRIVILEGES

Almost eight of ten organizations (77%) consider their management of user privileges not at all effective to only moderately effective.

How effective is your organization at managing user privileges?

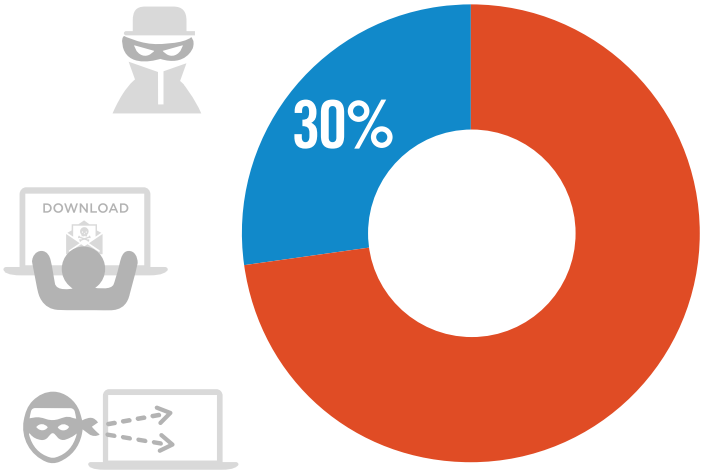


Not sure/other 2%

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?

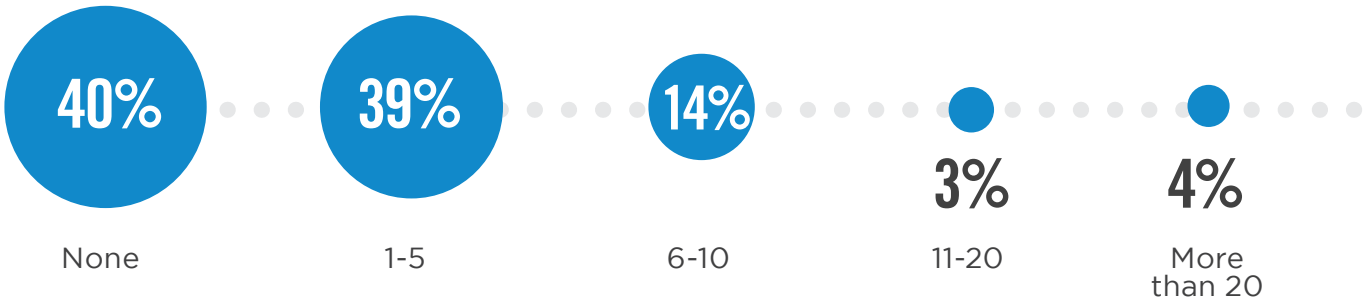


70%

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?

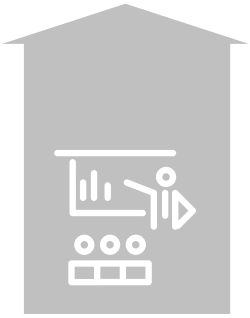


CONTRIBUTING FACTORS

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.

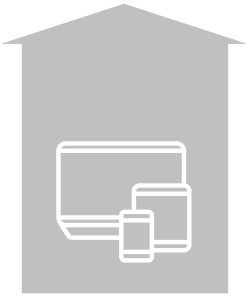
What do you believe are the main reasons behind insider attacks?

56%



Lack of employee training/awareness

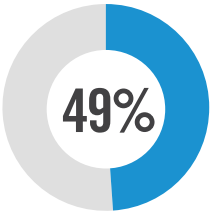
51%



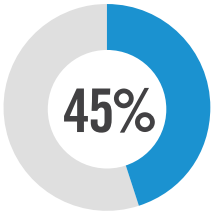
Increasing number of devices with access to sensitive data

50%

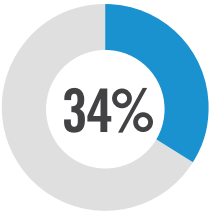
Insufficient data protection strategies or solutions



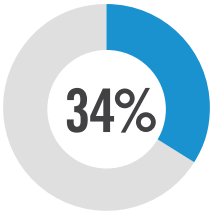
Data increasingly leaving the network perimeter via mobile devices and Web access



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%

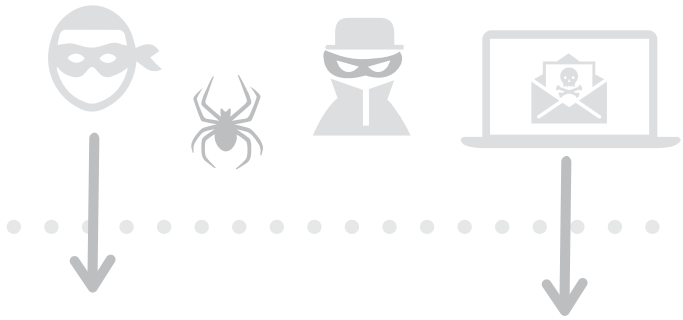
INSIDER VULNERABILITY

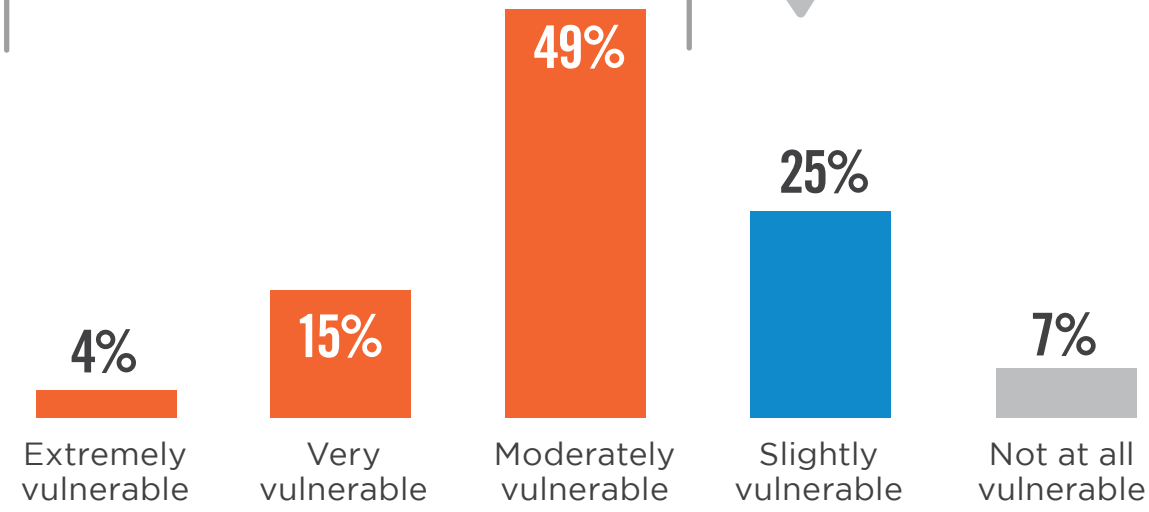
We asked cybersecurity professionals to assess their organization's vulnerability to insider threats. An overwhelming 68% of organizations feel moderately to extremely vulnerable. Only 7% say they are not at all vulnerable to an insider attack. Insider threats present another layer of complexity for IT professionals to manage, requiring careful planning with regards to access controls, user permissions, and monitoring user actions.

How vulnerable is your organization to insider threats?

68%

feel extremely to moderately vulnerable to insider attacks.





An alarming 28% of organizations said they do not have adequate controls in place (just as alarming, another 23% are not sure). The good news is security practitioners realize that advanced detection and prevention of insider threats is key; 49% of respondents have already implemented security controls and policies to deal with insider threats.

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

INTERNAL VS. EXTERNAL ATTACKS

When comparing internal attacks to external cybersecurity attacks, a majority (54%) confirms that internal attacks are more difficult to detect and prevent than external cyber attacks. Since insiders have approved access privileges, it can be challenging to distinguish legitimate use cases from malicious attacks.

How difficult is it to detect and prevent insider attacks compared to external cyber attacks?

54%

More difficult than detecting and preventing external cyber attacks

36%

About as difficult as detecting and preventing external cyber attacks

10%

Less difficult than detecting and preventing external cyber attacks

RISK CONTROLS

Organizations use a number of security controls to safeguard their organizations and minimize risk. Seventy-nine percent of respondents indicated perimeter defense tools as important for managing their risk of cyber attacks, followed by database and file monitoring (65%), and security events dashboards (57%).

What risk controls are important for managing the risk of cyber attack occurrences?

79%

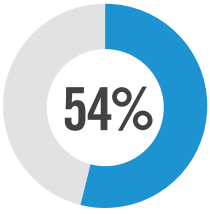
Security perimeter defense tools

65%

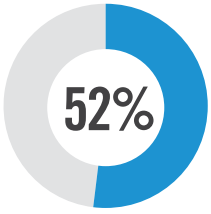
Database and file monitoring tools

57%

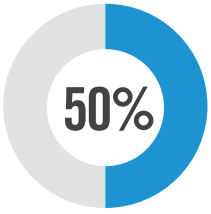
Security events dashboards



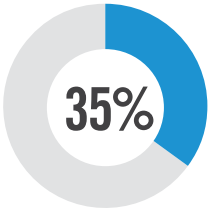
Access violations key risk indicators by database or system



Security event remediation processes



Data loss and corruption key risk indicators



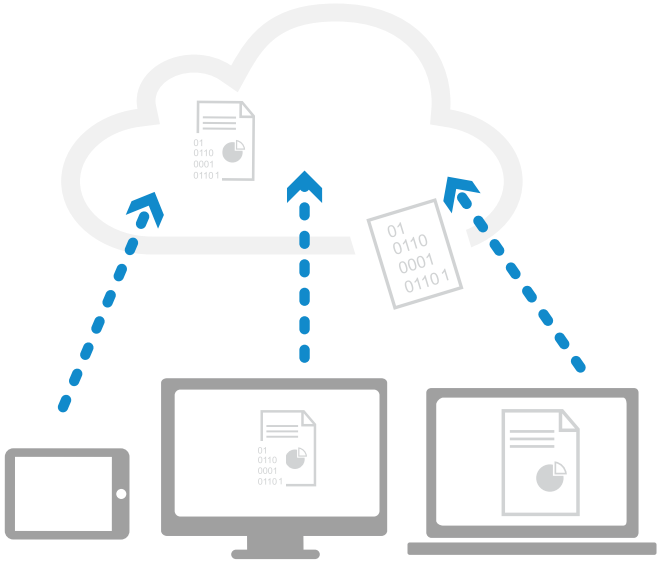
System of record monitoring

System downtime key risk indicators 27% | Not sure/other 8%

INSIDER ATTACKS IN THE CLOUD

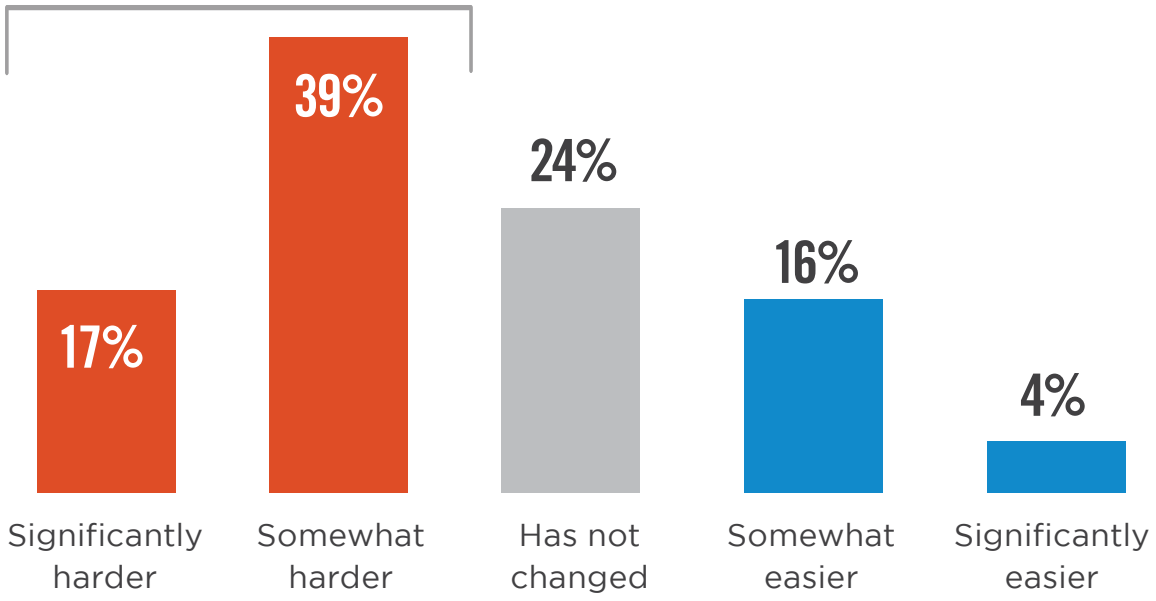
The shift to cloud computing is making the detection of insider attacks more difficult, as confirmed by 56% of cybersecurity professionals.

Since migrating to the cloud, how has detecting insider attacks changed?



56%

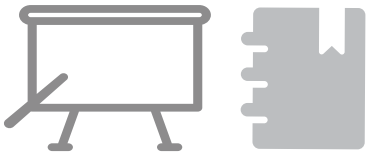
believe that detecting insider attacks has become significantly to somewhat harder.



MOST EFFECTIVE TOOLS & TACTICS

The most effective security tools and tactics deployed by organizations to protect against insider threats are policies and training (53%), closely followed by data loss/leakage solutions (52%), encryption of sensitive data (50%), and identity and access management solutions (50%). Data Loss Prevention (DLP) software monitors and protects sensitive data by helping control what data users can transfer, so unauthorized users can't accidentally or maliciously share it outside the organization. Identity and Access Management (IAM) technology enables organizations to grant individuals and roles with appropriate access to the technology and resources needed.

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

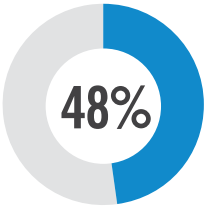


53% Policies & training

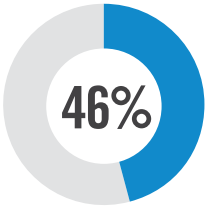
52% Data Loss Prevention (DLP)

50% Encryption of data (at rest, in motion, in use)

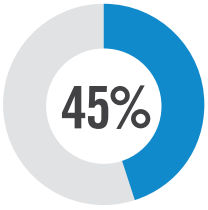
50% Identity and Access Management (IAM)



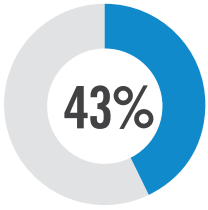
User behavior anomaly detection



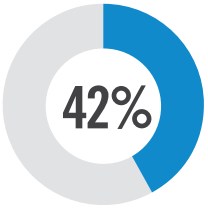
Security Information and Event Management (SIEM)



Multi-factor authentication



User monitoring



File activity monitoring

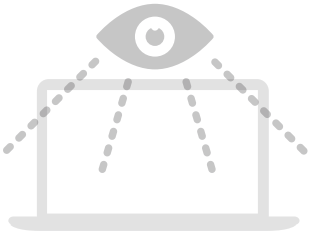
Security analytics & intelligence 40% | Intrusion Detection and Prevention (IDS/IPS) 38% | Endpoint and mobile security 38% | Data access monitoring 38% | Network defenses (firewalls) 37% | Sensitive and private data identification 33% | Database Activity Monitoring (DAM) 32% | Password vault 21% | Tokenization 21% | Cloud Access Security Broker (CASB) 21% | Enterprise Digital Rights Management solutions (E-DRM) 21% | Cloud Security as a Service 15% | Not sure/other 10%

FOCUS ON DETECTION

While all methods of countering insider threats are important, organizations are shifting their focus on deterrence of internal threats (62%) over 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.)

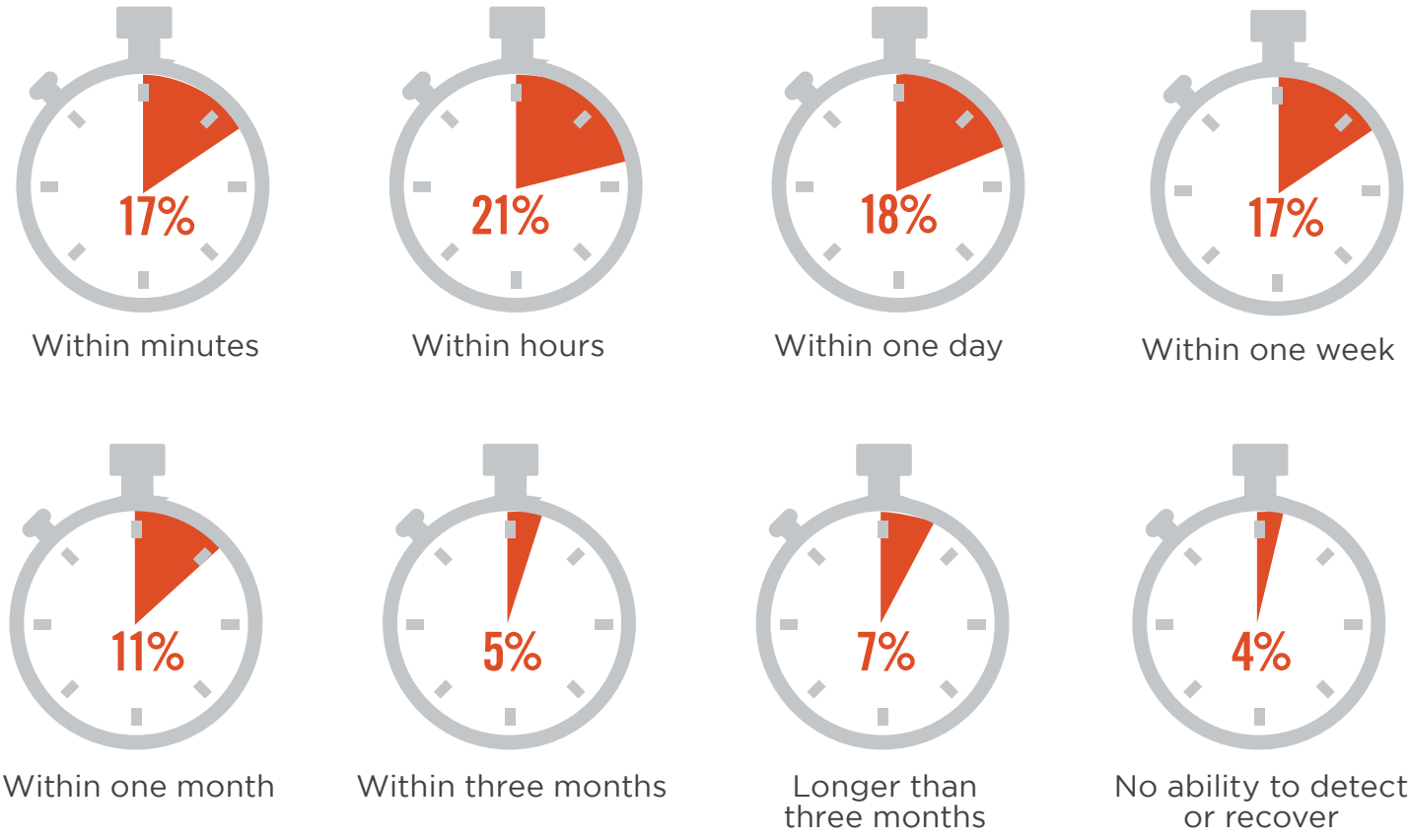
47% **Analysis and post breach forensics**
(e.g. SIEM, log analysis, etc.)

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

SPEED OF DETECTION & MITIGATION

More than half the respondents claim they can detect insider threats within the same day (56%) and 17% even within minutes of an attack. This seems very optimistic considering insider attacks often span long periods of dwell time due to the difficulty in detecting malicious attacks (compared to legitimate use).

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

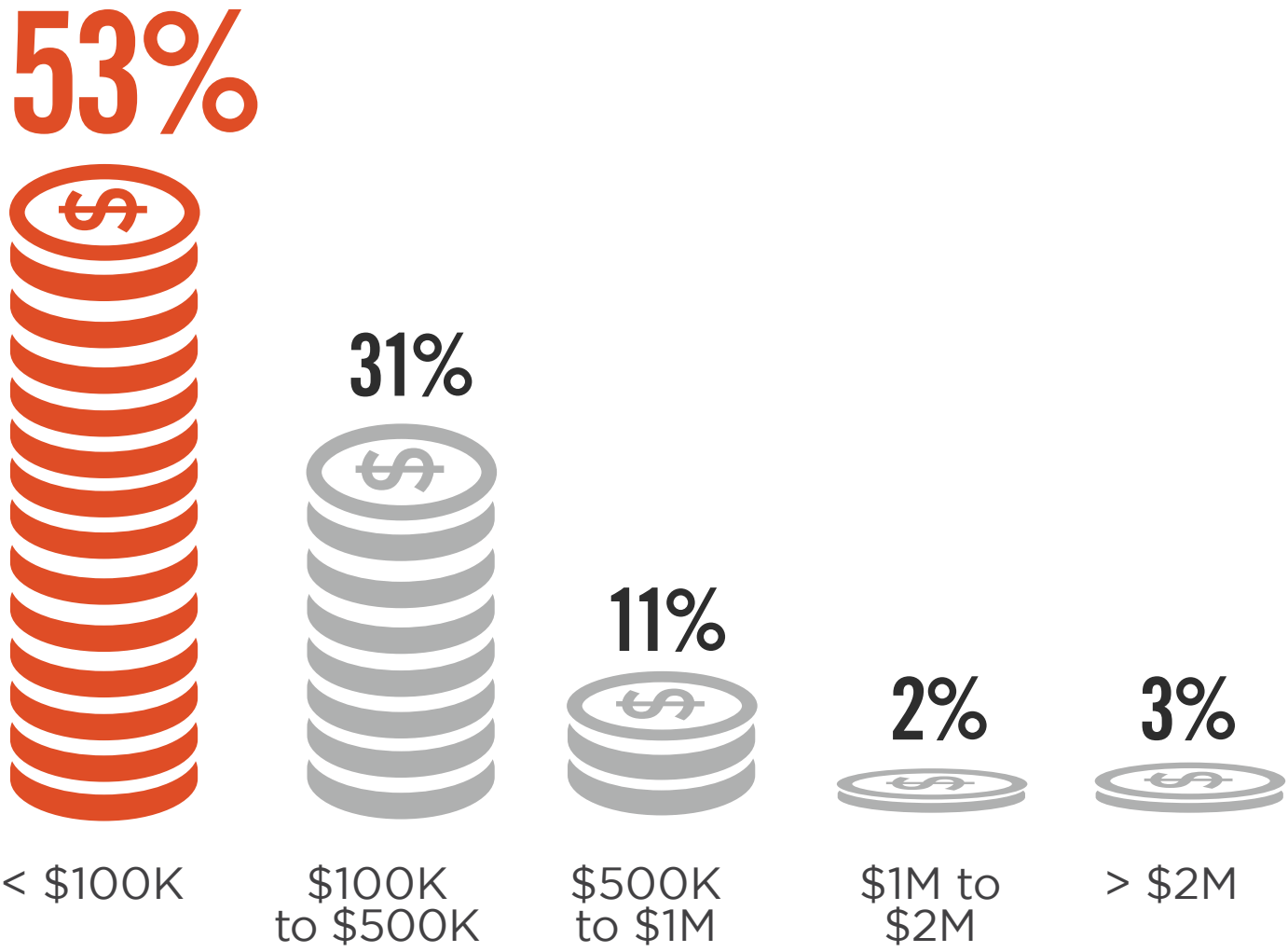


56% detect insider attacks within a day

COSTLY INSIDER ATTACKS

While the true cost of a major security incident is not easy to determine, the most common estimate is less than $100,000 per successful insider attack (53%). Thirty-one percent expect damages between $100,000 to $500,000.

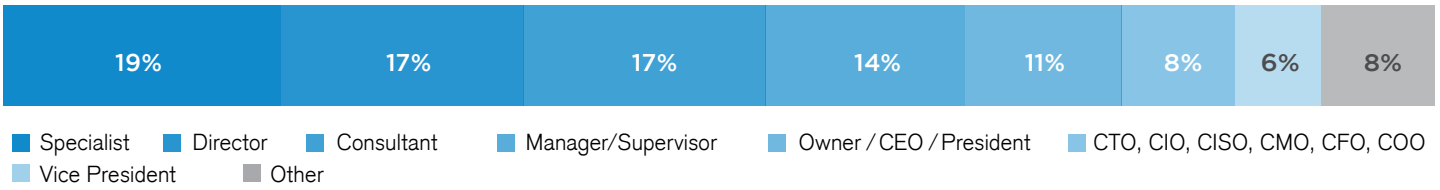
What is the estimated average cost of remediation after an insider attack?



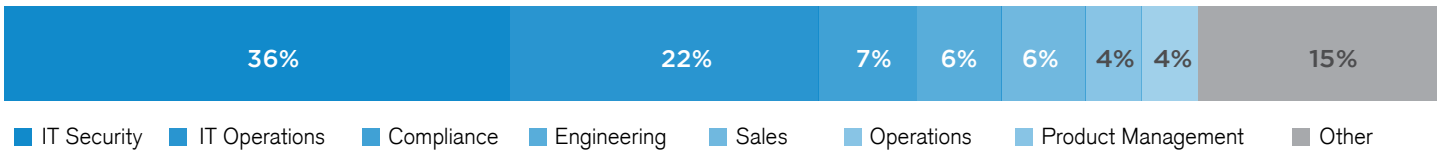
METHODOLOGY & DEMOGRAPHICS

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.

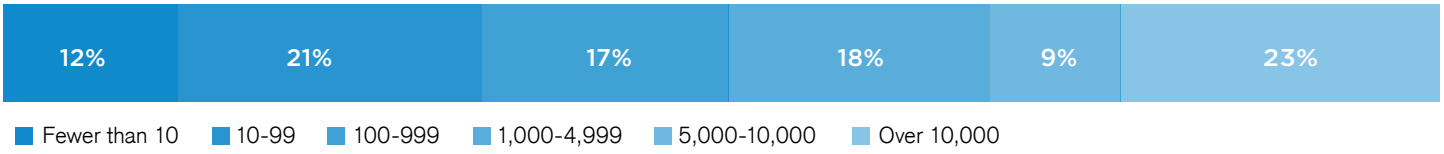
CAREER LEVEL



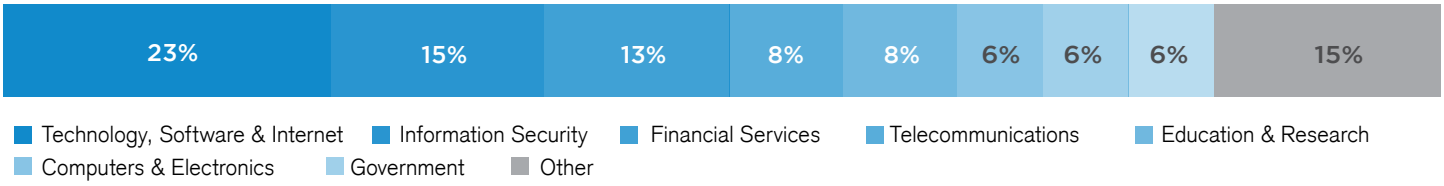
DEPARTMENT



COMPANY SIZE



INDUSTRY



HelpSystems helps you protect business-critical data with a suite of integrated and automated security solutions for defense in depth, comprehensive visibility, and streamlined reporting across your on-prem and cloud environments.

www.helpsystems.com