2019

Cybersecurity
INSIDERS

INSIDER THREAT REPORT

SECURONIX™

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:

- 68% of organizations feel moderately to extremely vulnerable to insider attacks
- 73% of organizations confirm insider attacks are becoming more frequent
- 39% identified cloud storage and file sharing apps as the most vulnerable to insider attacks
- 56% believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud
- 59% think that privileged IT users pose the biggest insider security risk to organizations

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 security threats in the cloud.

We would like to thank Securonix for supporting this unique research.

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 somewhat 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%

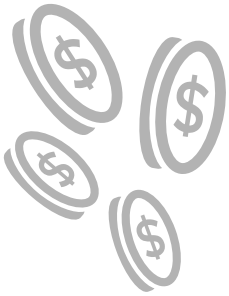
MOTIVATIONS FOR INSIDER ATTACKS

To understand malicious insider threats, it is important to look at the underlying motivations of insiders. Our survey panel considers fraud (57%) and 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

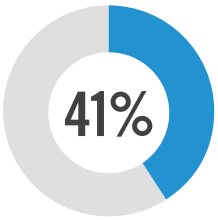


50%

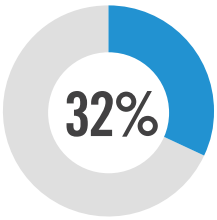
Monetary gain

43%

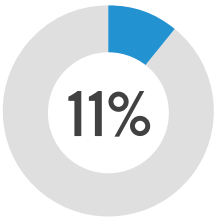
IP theft



Sabotage



Espionage



Professional benefit

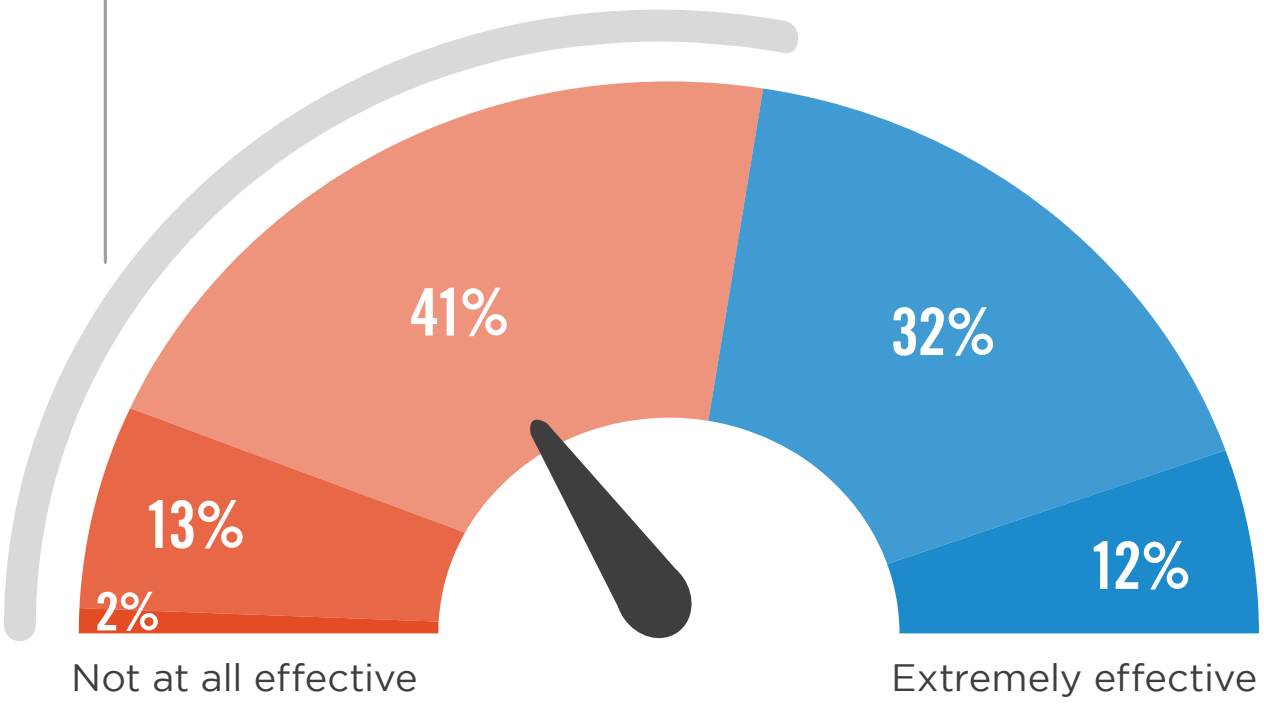
Not sure/other 8%

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

RISKY INSIDERS

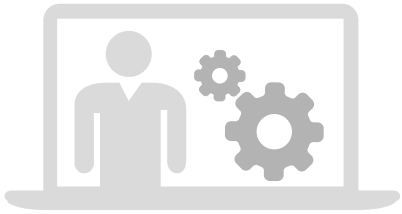
Protecting organizations against cyber threats becomes significantly more challenging when the threats come from within the organization, from trusted and authorized users. It can be difficult to determine when users are simply doing their job function or actually doing something malicious or negligent.

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?

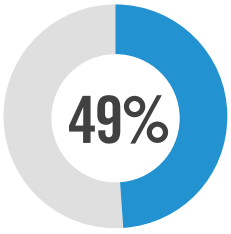
59%

Privileged IT users/admins

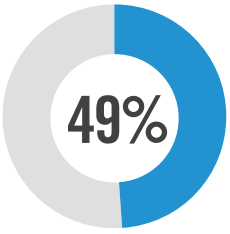


52%

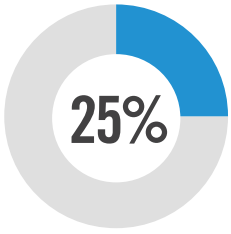
Contractors/ service providers/ temporary workers



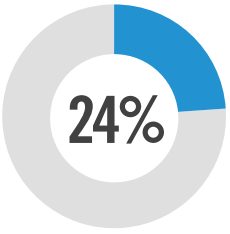
Regular employees



Privileged business users/ executives



Other IT staff



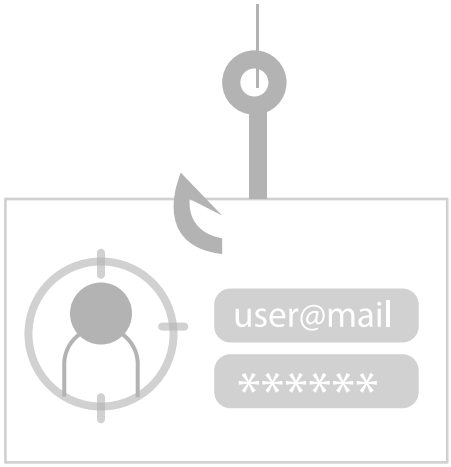
Executive managers

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

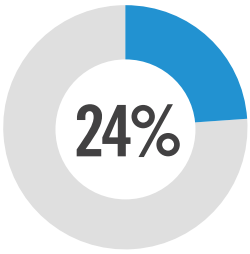
ACCIDENTAL INSIDERS

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.

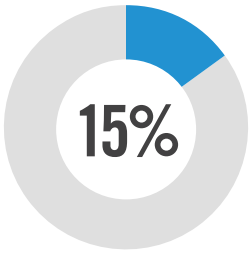
What are the most common accidental insider threats you are most concerned about?



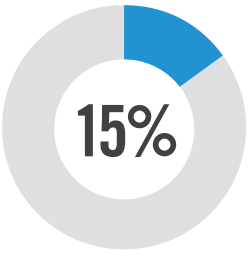
43% Phishing attempts



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%

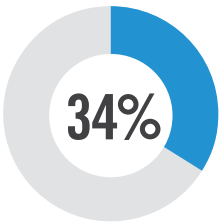
Collaboration & communication

(email, messaging, etc.)

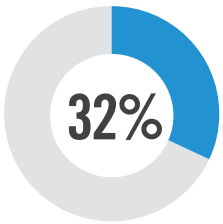
35%

Productivity

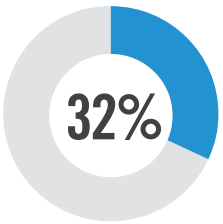
(Office 365, word processing, spreadsheets, etc.)



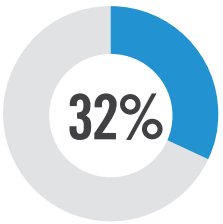
Website



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%

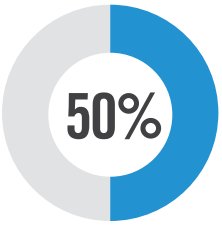
Customer data

55%

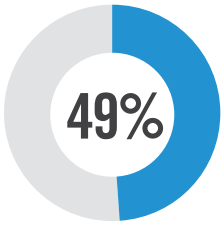
Intellectual property

52%

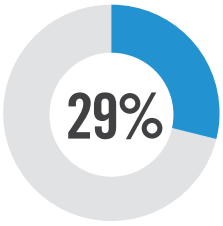
Financial data



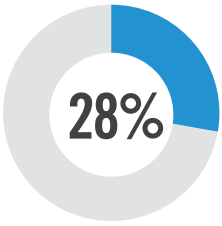
Employee data



Company data



Sales and marketing data



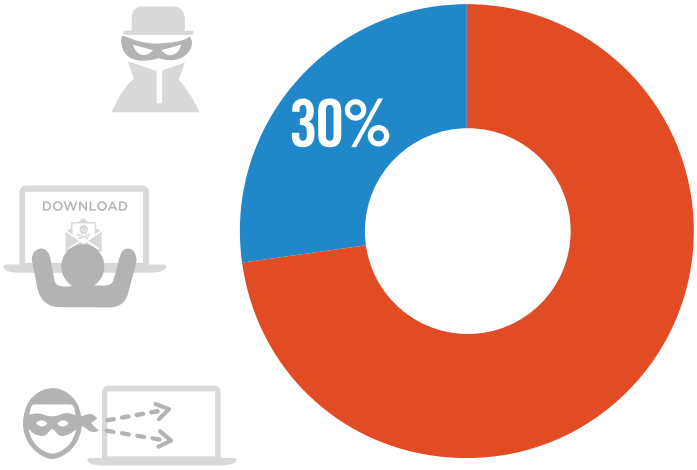
Healthcare data

Not sure/other 4%

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?

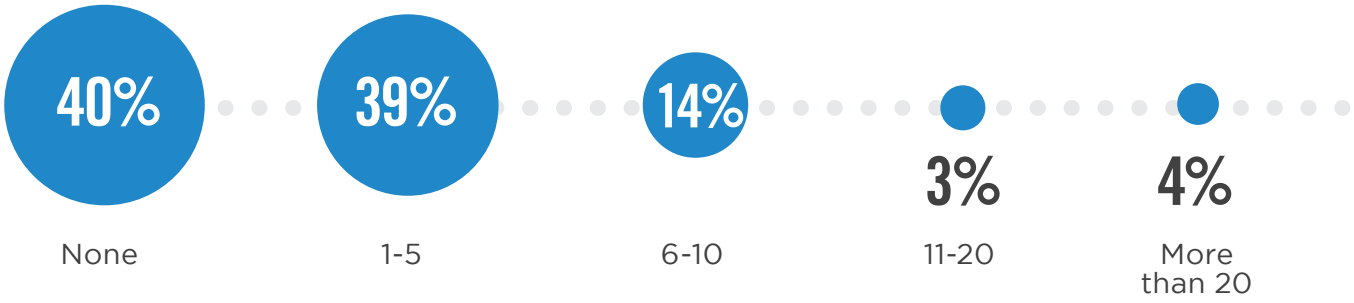


70%

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?



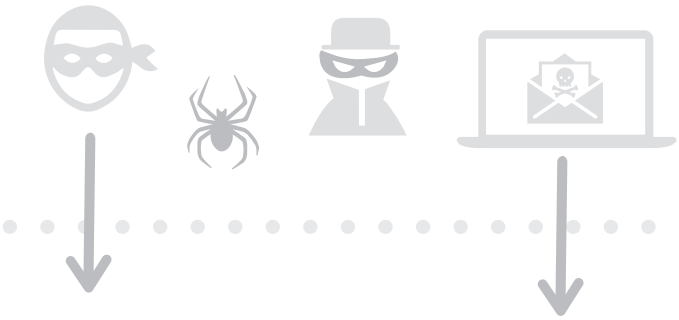
INSIDER VULNERABILITY

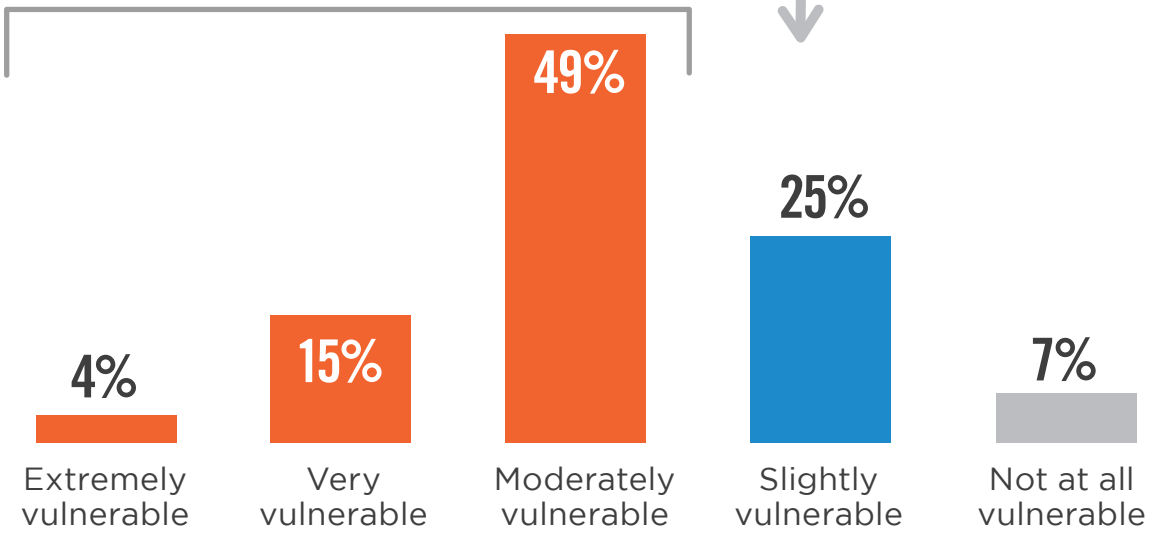
We asked cybersecurity professionals to assess their organization's vulnerability to insider threats. An overwhelming 68% of organizations feel moderately to extremely vulnerable. Only 7% say they are not at all vulnerable to an insider attack. Insider threats present another layer of complexity for 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?

DETECTION AND PREVENTION

Because insiders often have elevated access privileges to sensitive data and applications, it becomes increasingly difficult to detect malicious activity (56%). Combined with the proliferation of data sharing apps (46%) and more data leaving the traditional network perimeter (45%), 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?

56%

Insiders already have credentialed access to the network and services

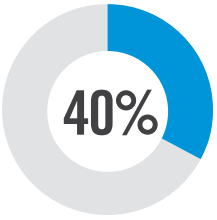
46%

Increased use of applications that can leak data

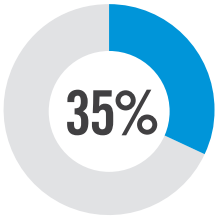
(e.g., Web email, DropBox, social media)

45%

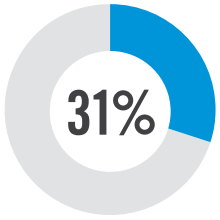
Increased amount of data that leaves protected boundary/perimeter



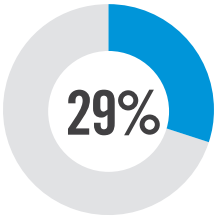
More end-user devices capable of theft



Migration of sensitive data to the cloud along with adoption of cloud apps



Insiders are more sophisticated



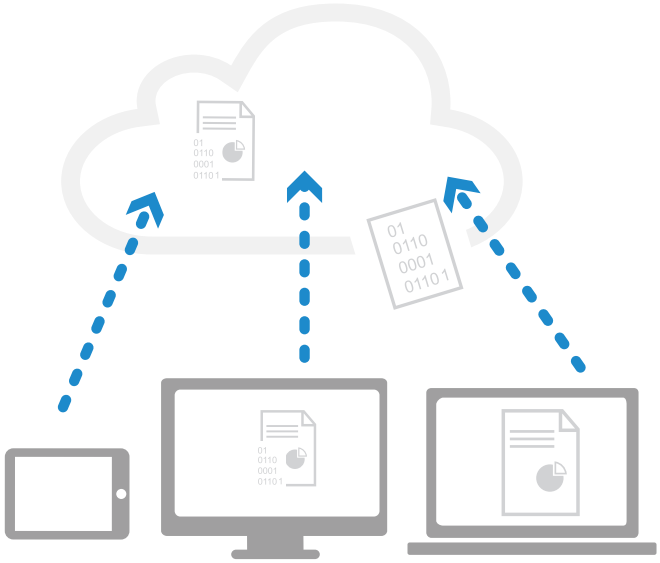
Difficulty in detecting rogue devices introduced into the network or systems

Absence of an Information Security Governance Program 21% | Not sure/other 10%

INSIDER ATTACKS IN THE CLOUD

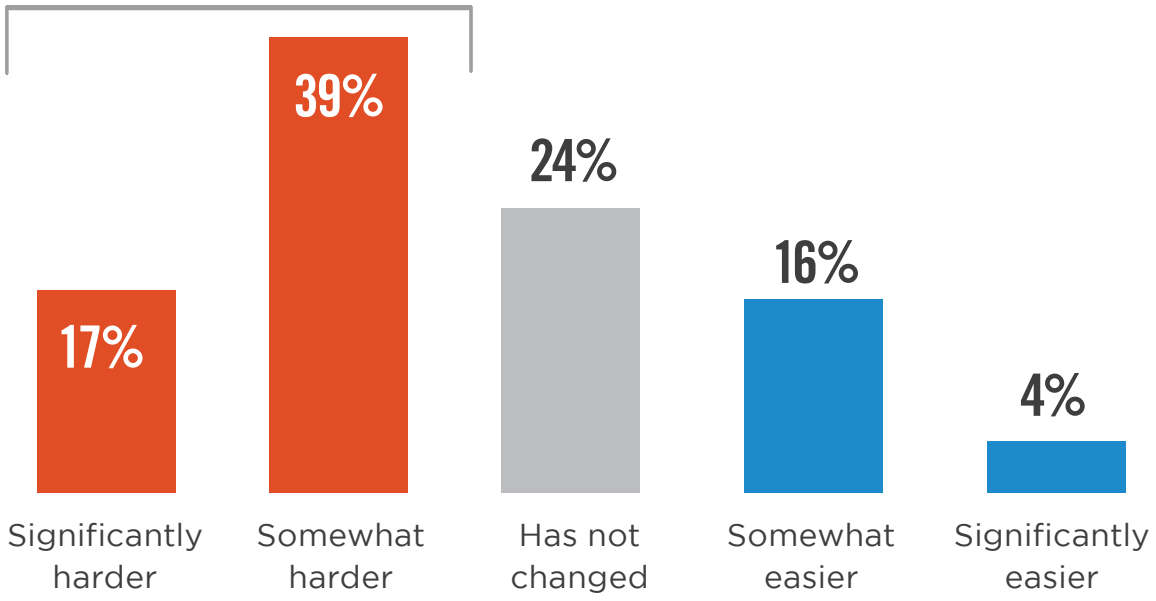
The shift to cloud computing is making the detection of insider attacks more difficult, as confirmed by 56% of cybersecurity professionals.

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



56%

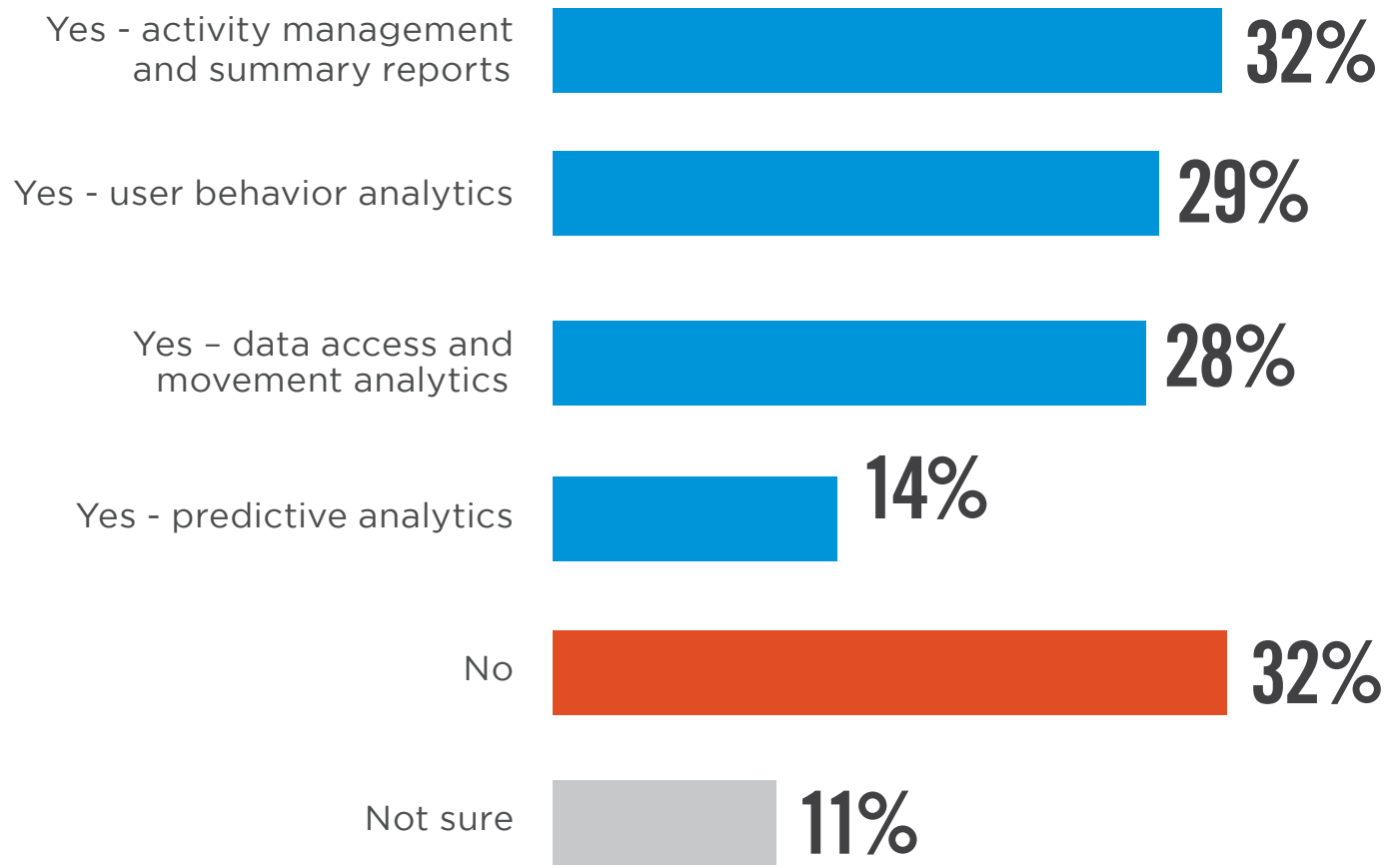
Believe that detecting insider attacks has become significantly to somewhat harder.



INSIDER THREAT ANALYTICS

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

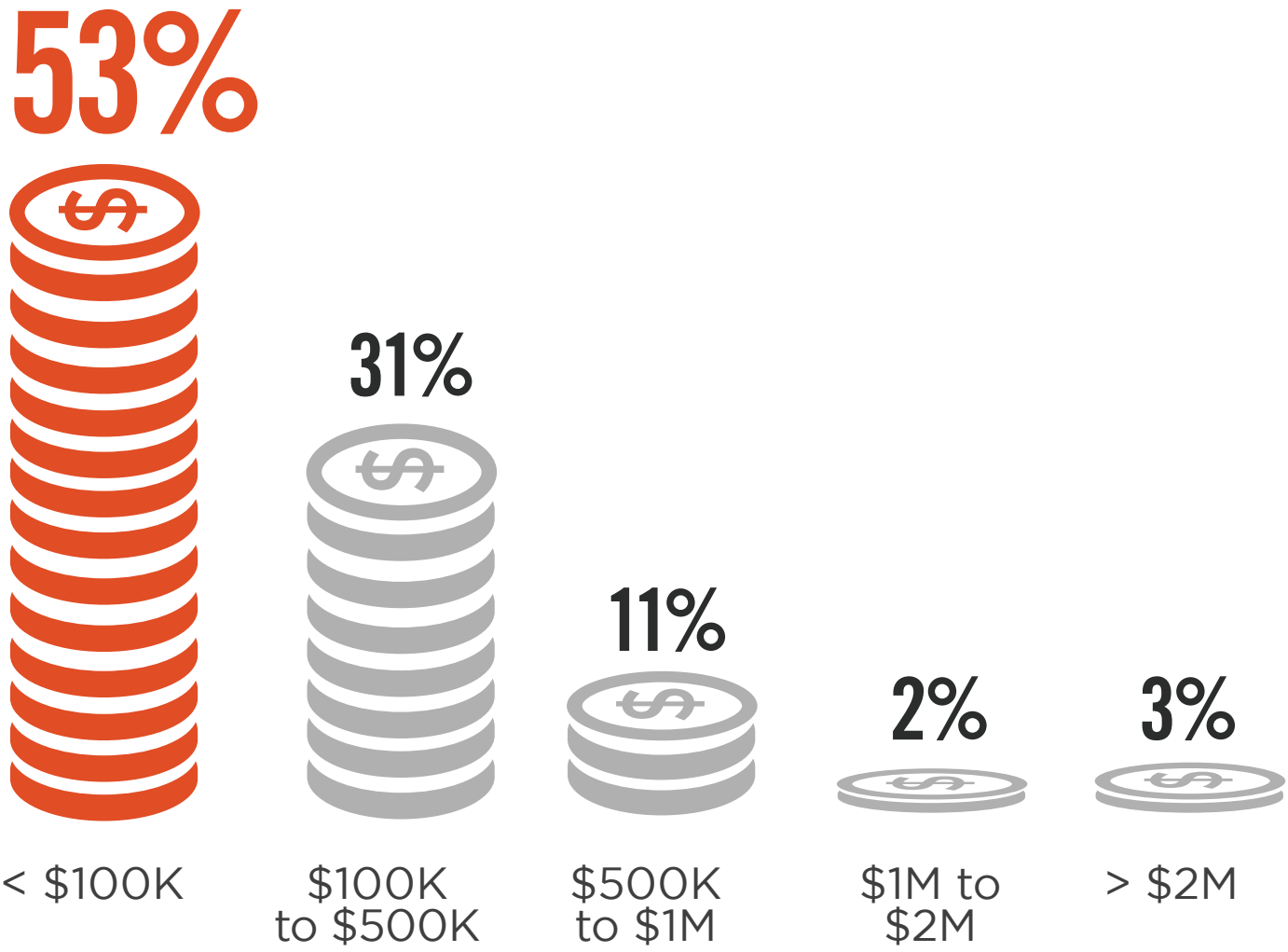
Does your organization leverage analytics to determine insider threats?



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.

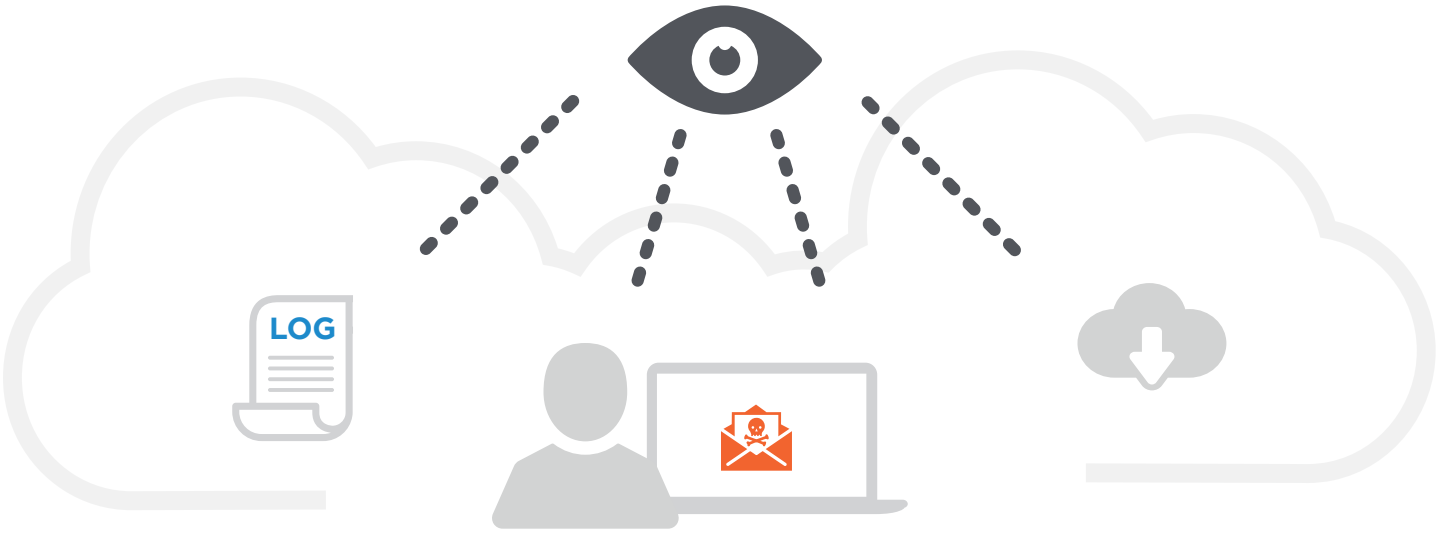
What is the estimated average cost of remediation after an insider attack?

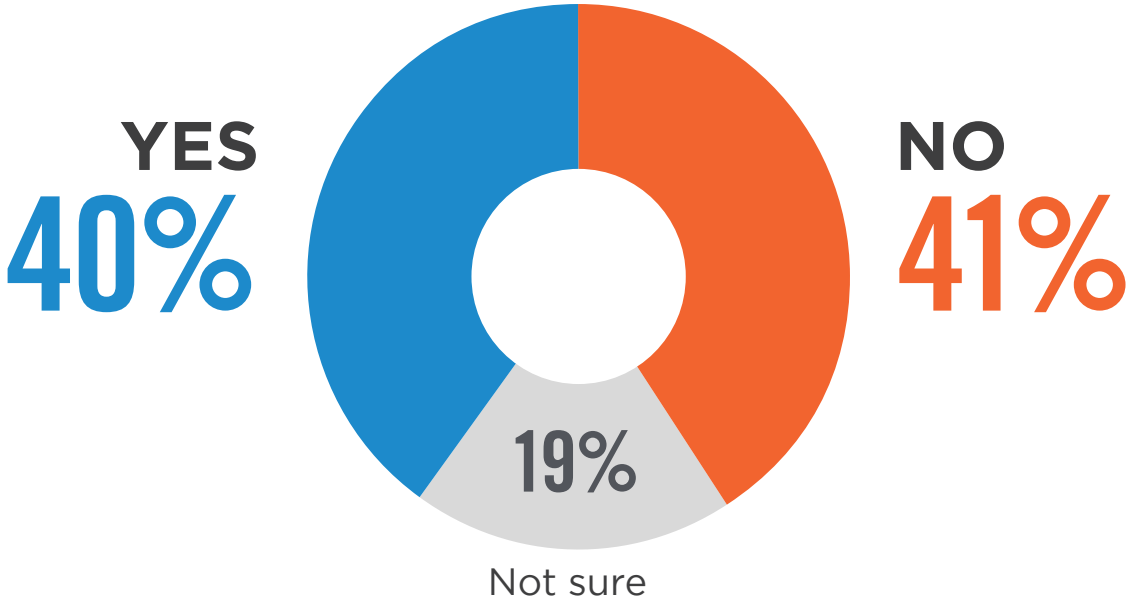


MONITOR ABNORMAL USER BEHAVIOR

Only 40% of organizations monitor user behavior across their cloud footprint.

Do you monitor abnormal user behavior across your cloud footprint (SaaS, IaaS, PaaS)?

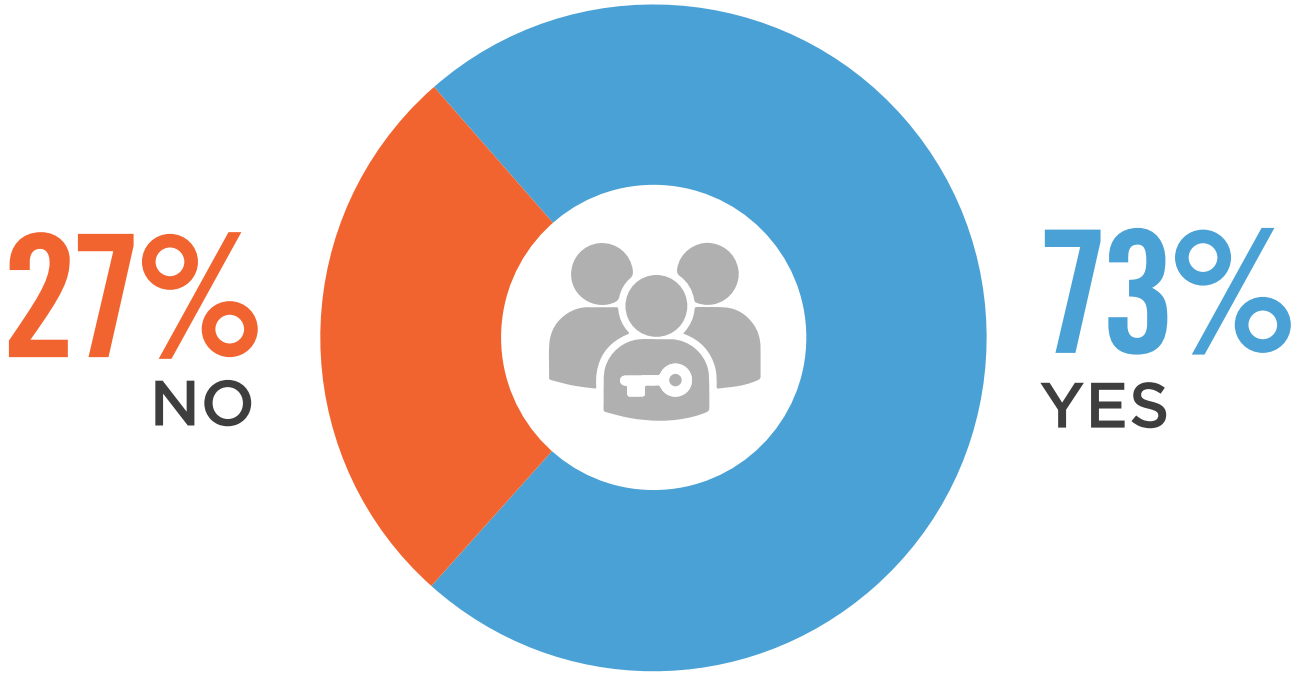




USER PRIVACY

User privacy is a significant concern in the context of insider threat monitoring for seven out of ten organizations we surveyed.

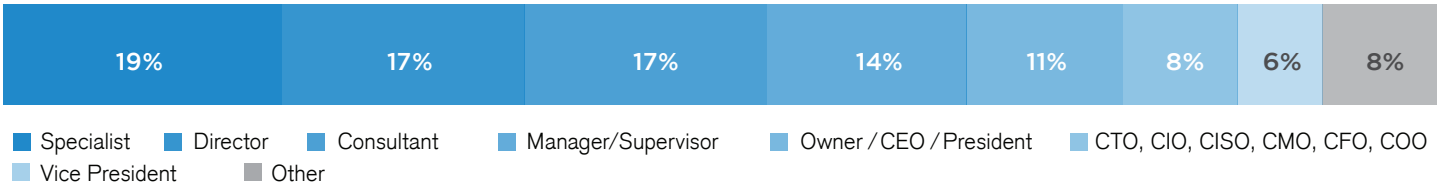
Is user privacy a concern when monitoring insider threats?



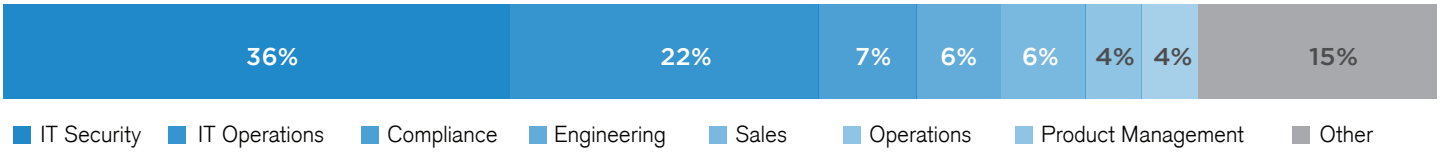
METHODOLOGY & DEMOGRAPHICS

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.

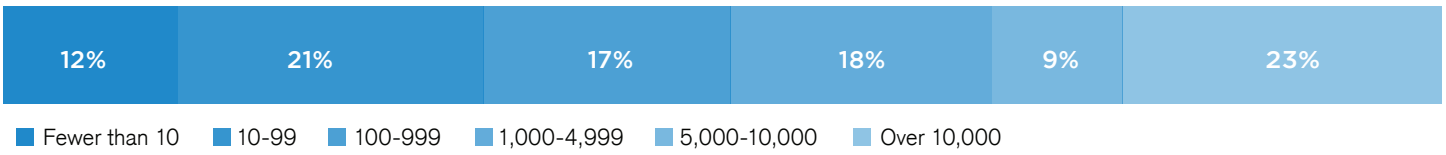
CAREER LEVEL



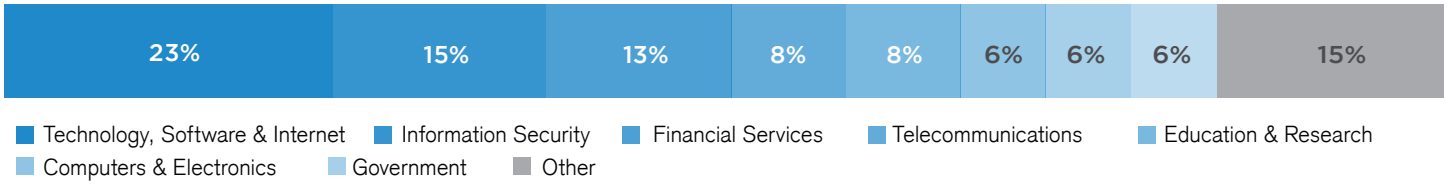
DEPARTMENT



COMPANY SIZE



INDUSTRY



ABOUT US

Securonix | www.securonix.com

Securonix is redefining SIEM using the power of big data and machine learning. Built on an open Hadoop platform, Securonix Next-Gen SIEM provides unlimited scalability and log management, behavior analytics-based advanced threat detection, and automated incident response on a single platform. Globally, customers use Securonix to address their insider threat, cyber threat, cloud security, and application security monitoring requirements.

RESOURCES

Keep up to date on the latest developments in cybersecurity. Securonix cybersecurity experts regularly publish content on emerging security threats and security and compliance best practices.

Webinars – Features topics including security operations center (SOC) best practices, threat hunting guidance, and how to secure your cloud. Provides CISOs, SOC analysts, incident responders, compliance professionals, and other cybersecurity professionals with the knowledge to make critical security decisions.

https://www.securonix.com/resource-type/webinars/

White Papers – Written by cybersecurity experts from our development, implementation, and field teams Securonix white papers include real-world scenarios, use cases, and customer stories.

https://www.securonix.com/resource-type/white-papers/

Blog – Includes articles on a wide range of cybersecurity and compliance topics, including technical commentary on key trends and the latest developments in behavior analytics, insider threats, ransomware, social engineering, incident response, threat hunting, and more.

https://www.securonix.com/blog/