2020

Cybersecurity
INSIDERS

INSIDER THREAT REPORT

GURUCUL

INTRODUCTION

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

The 2020 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
- 68% of organizations confirm insider attacks are becoming more frequent
- 53% of organizations believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud
- 63% of organizations think that privileged IT users pose the biggest insider security risk to organizations

This 2020 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 Gurucul 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

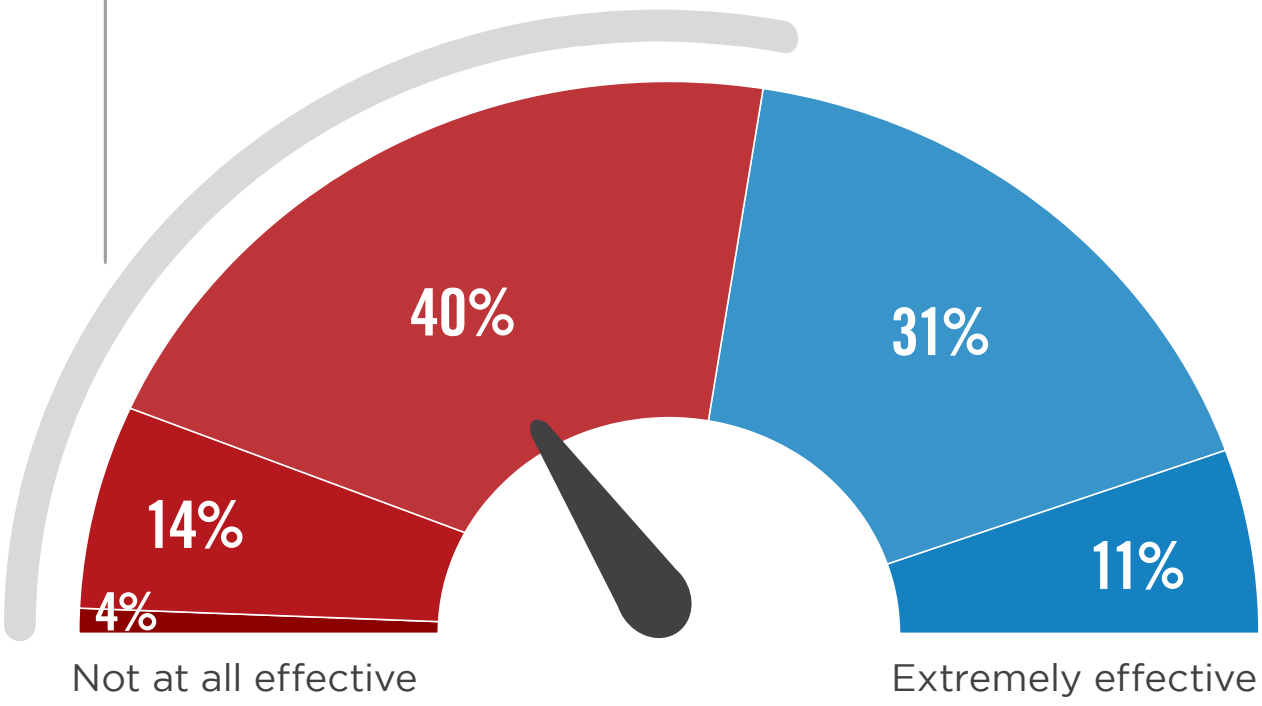
Cybersecurity
INSIDERS

INSIDER THREAT DISCOVERY AND RESPONSE

A majority of organizations consider themselves only somewhat effective or worse (58%) 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?

58% 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 (63%) pose the biggest insider security risk to organizations.

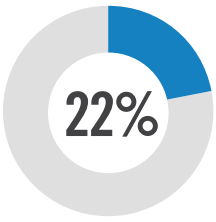
What type(s) of insiders pose the biggest security risk to organizations?

63% Privileged IT users/admins

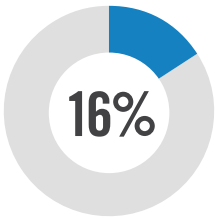
51%
Regular employees

50%
Contractors/ service providers/ temporary workers

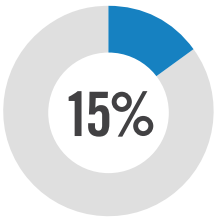
50%
Privileged business users/executives



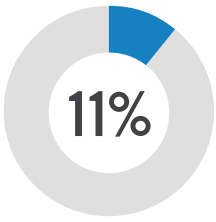
Other IT staff



Executive managers



Customers/ clients



Business partners

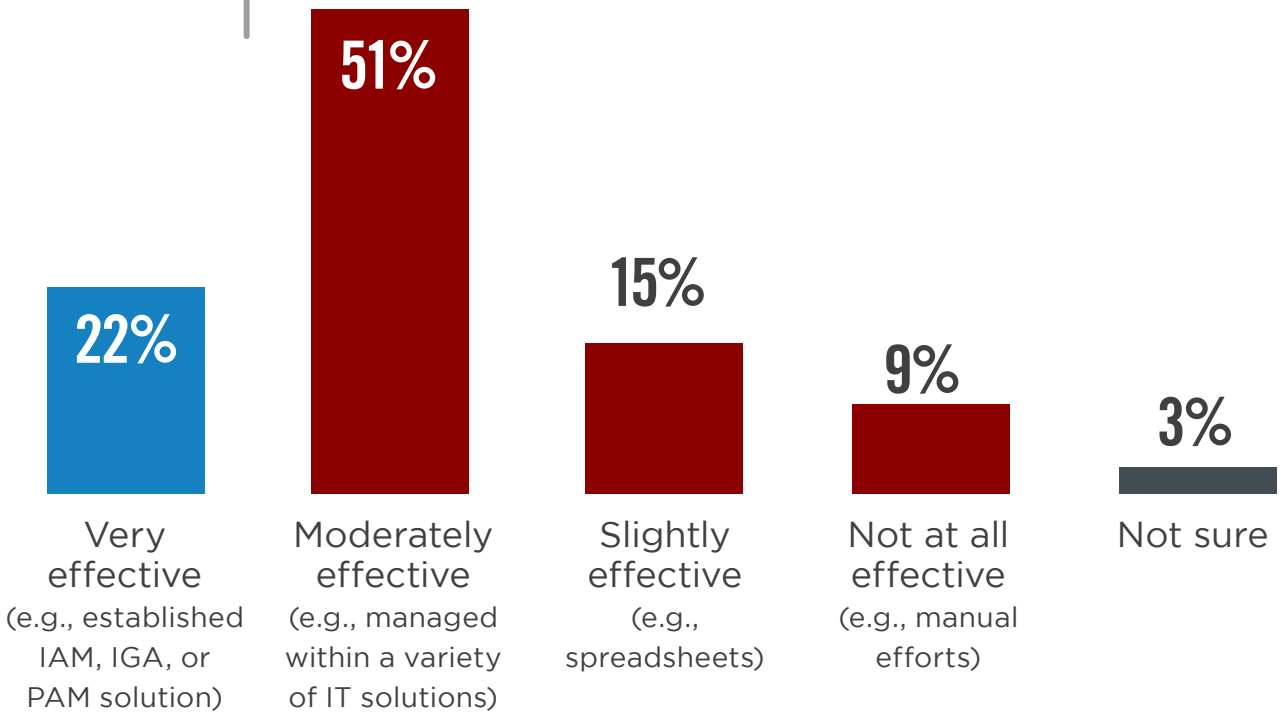
Interns 4% | Not sure/other 3%

USER PRIVILEGES

Privileged IT users and admins have been identified as posing the biggest security risk - however only a small proportion (22%) of organizations feel that they are very effective in managing user privileges. This suggests that privilege management should become a higher organizational priority.

How effective is your organization at managing user privileges?

78% Don't believe that they have very effective management of user privileges



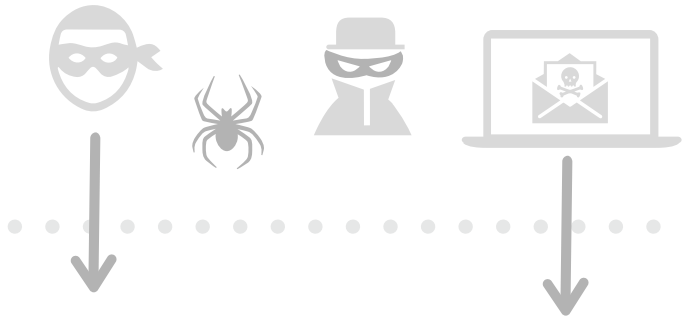
INSIDER VULNERABILITY

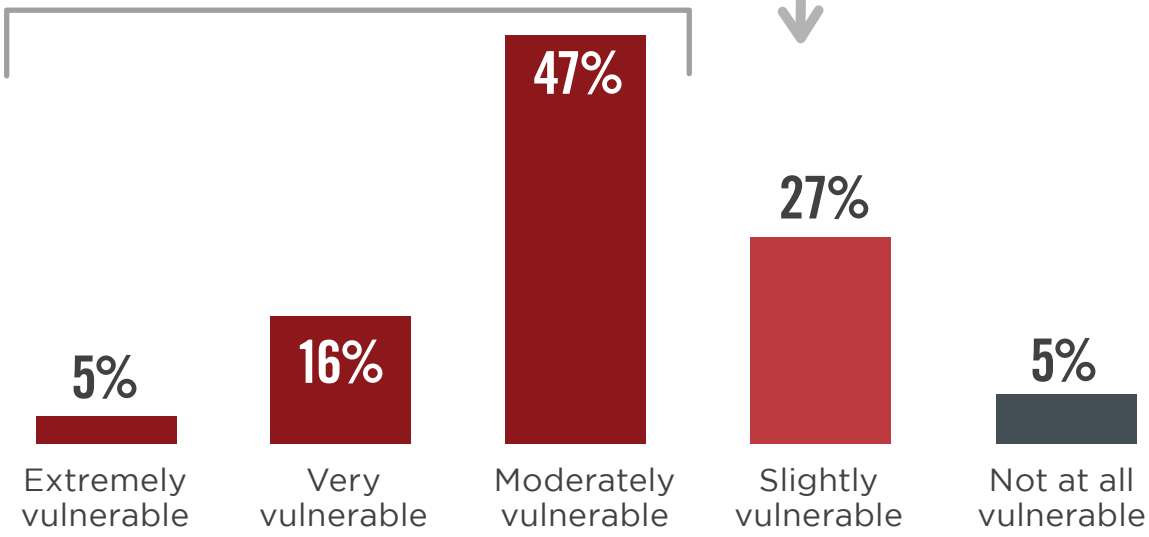
We asked cybersecurity professionals to assess their organization's vulnerability to insider threats. An overwhelming 68% of organizations feel moderately to extremely vulnerable. Only 5% say they are not at all vulnerable to an insider attack. Insider threats present another layer of complexity for 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.





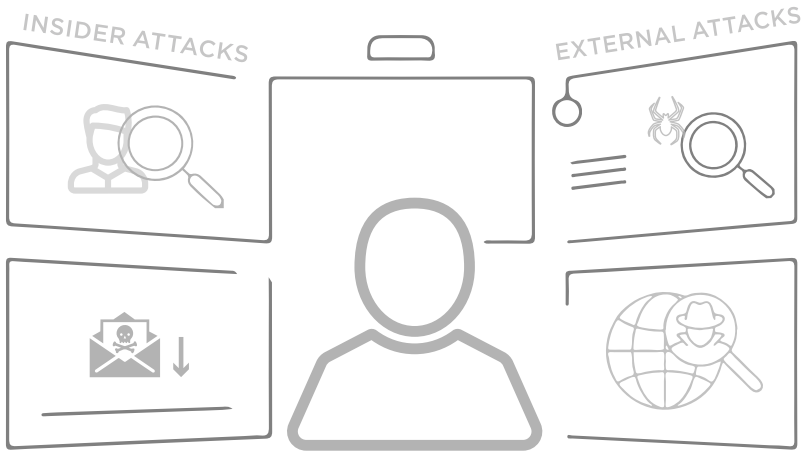
An alarming 29% of organizations said they do not have adequate controls in place (just as alarming, another 23% are not sure). The good news is security practitioners realize that advanced detection and prevention of insider threats is key; 48% of respondents have already implemented security controls and policies to deal with insider threats.

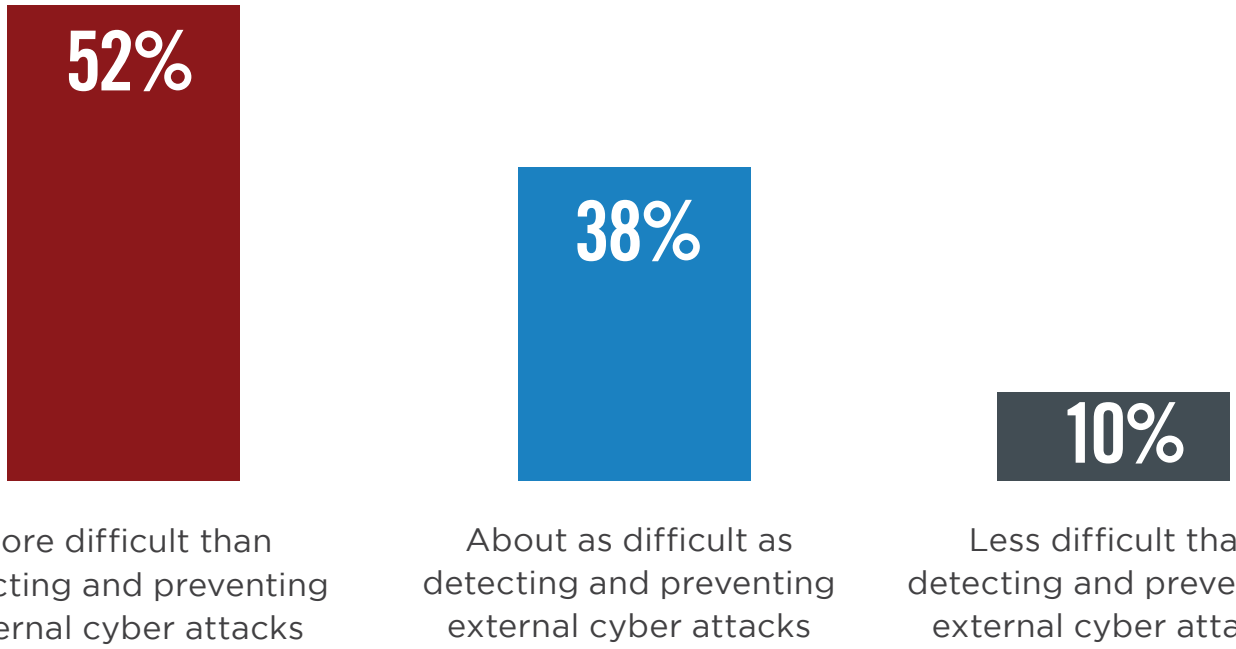
Does your organization have the appropriate controls to prevent an insider attack?

INTERNAL VS. EXTERNAL ATTACKS

When comparing internal attacks to external cybersecurity attacks, a majority (52%) 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?





More difficult than detecting and preventing external cyber attacks

About as difficult as detecting and preventing external cyber attacks

Less difficult than detecting and preventing external cyber attacks

DETECTION AND PREVENTION

Because insiders often have elevated access privileges to sensitive data and applications, it becomes increasingly difficult to detect malicious activity (59%). Combined with the proliferation of data sharing apps (50%) 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?

59%

Insiders already have credentialed access to the network and services

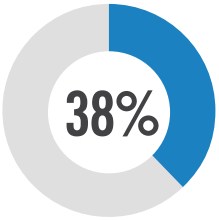
50%

Increased use of applications that can leak data

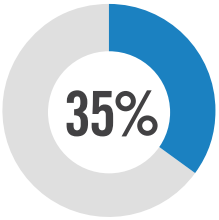
(e.g., Web email, DropBox, social media)

47%

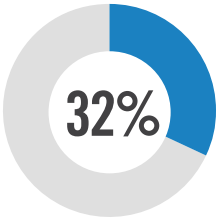
Increased amount of data that leaves protected boundary/perimeter



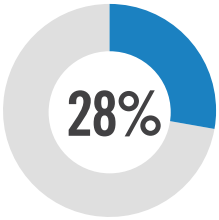
More end-user devices capable of theft



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



Insiders are more sophisticated



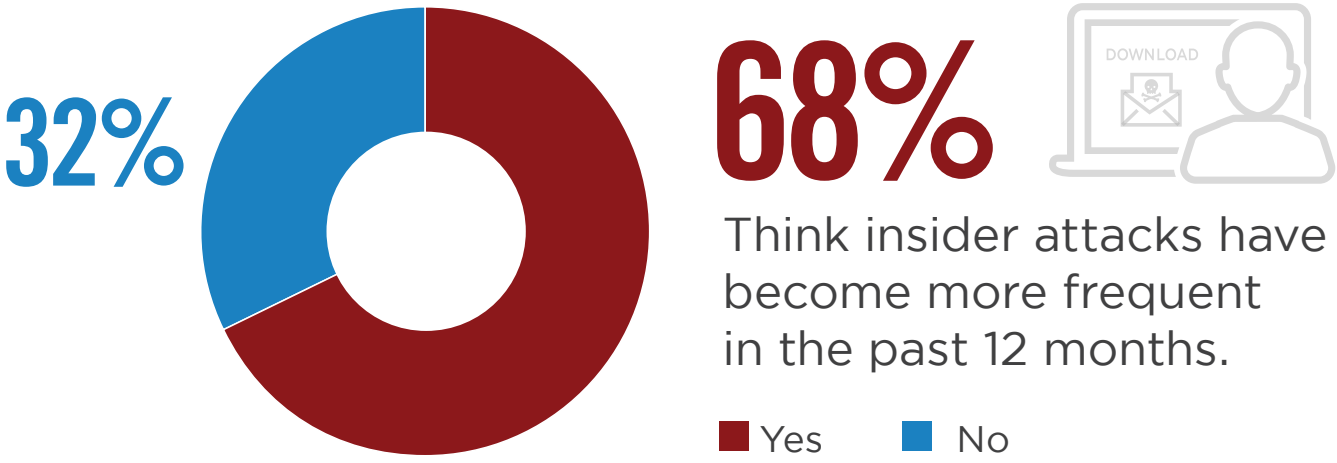
Difficulty in detecting rogue devices introduced into the network or systems

Absence of an Information Security Governance Program 22% | Not sure/other 7%

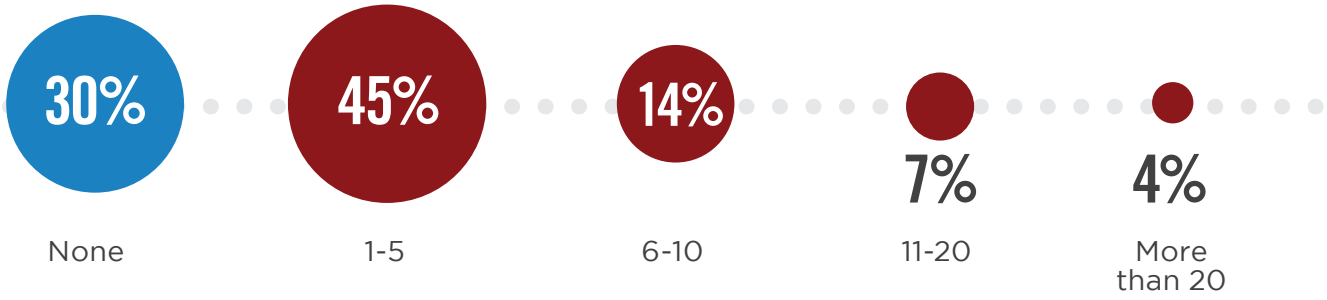
RISE OF INSIDER ATTACKS

A significant majority of organizations (68%) observed that insider attacks have become more frequent over the last 12 months. In fact, 70% 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?



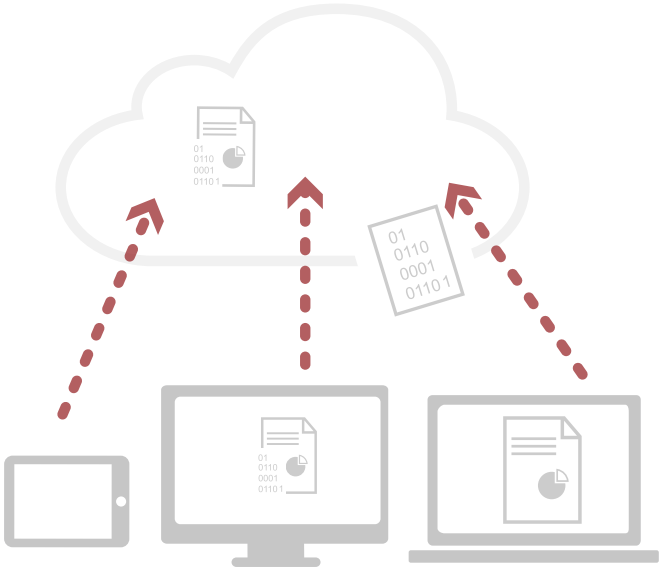
How many insider attacks did your organization experience in the last 12 months?



INSIDER ATTACKS IN THE CLOUD

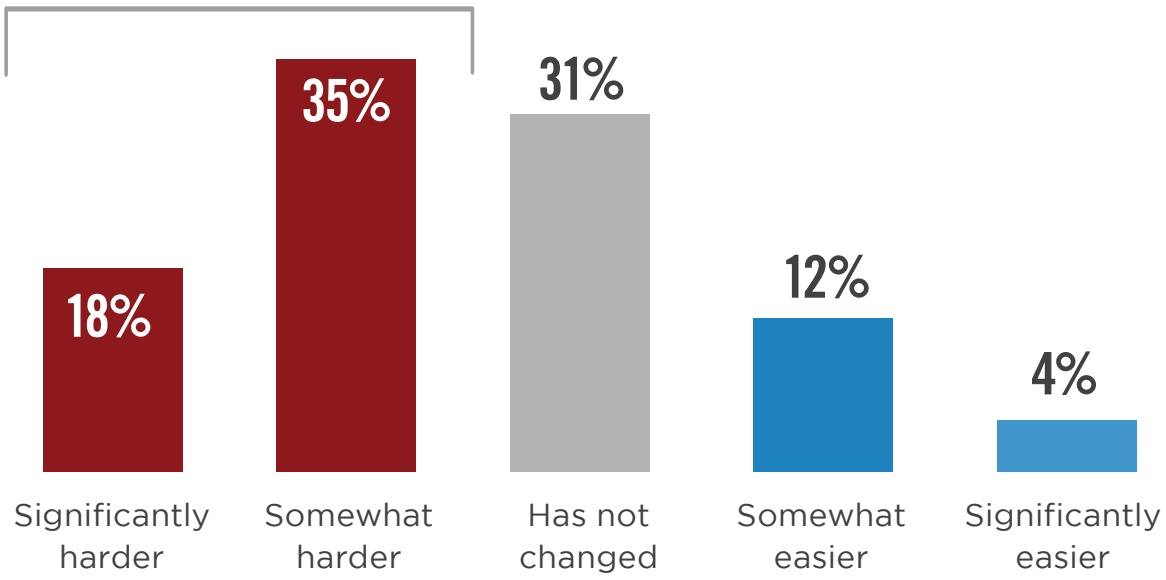
The shift to cloud computing is making the detection of insider attacks more difficult, as confirmed by 53% of cybersecurity professionals.

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



53%

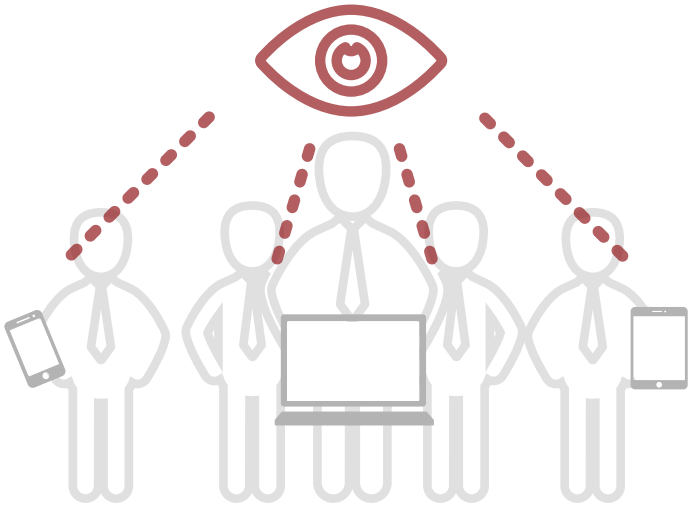
Believe that detecting insider attacks has become significantly to somewhat harder.

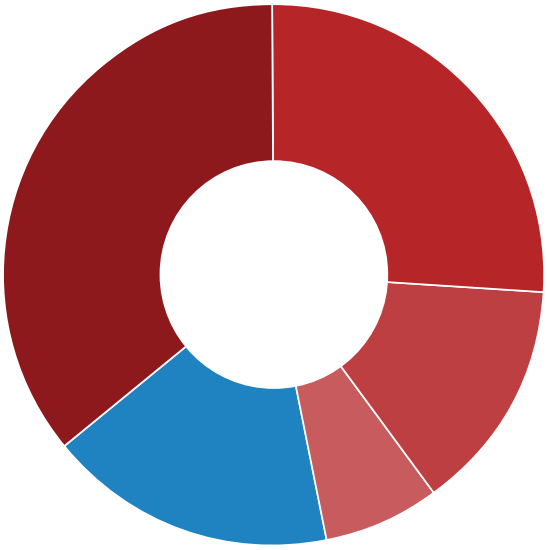


USER BEHAVIOR MONITORING

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-three percent of organizations monitor user behavior in one way or another, most commonly utilizing access logging (36%) and automated user behavior monitoring (26%).

Do you monitor user behavior?





36%
YES, but access logging only

26%
YES, we use automated tools to monitor user behavior 24x7

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

17%
NO, we don't monitor user behavior at all

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

ANOMALOUS BEHAVIOR DETECTION

There is significant variance in the capacity to detect anomalous behavior across multiple categories. The level of visibility into privileged accounts is high (70%), whereas visibility into cloud is low (30%). This variance may very well be indicative of different degrees of perceived risk and the corresponding degree of scrutiny.

Are you able to detect anomalous behavior of any of the following?

70%

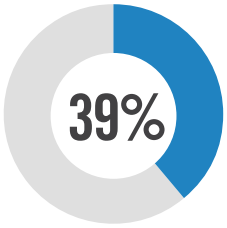
Privileged accounts

57%

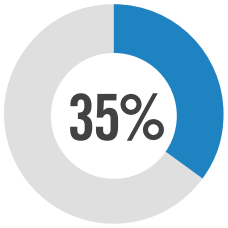
Documents/ document repositories

43%

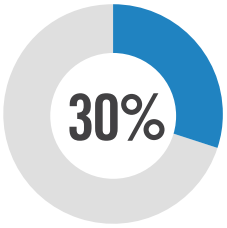
Entities (e.g., Devices)



Service accounts



NetFlow/ packet data



Cloud applications & infrastructure

VISIBILITY INTO USER BEHAVIOR

Organizations rely most commonly on server logs to track user behavior (46%), followed by having deployed user activity monitoring (33%), and in-app audit system/feature (31%).

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

46%

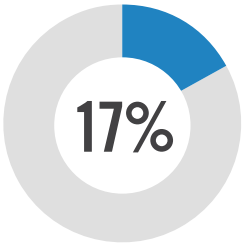
Rely on server logs

33%

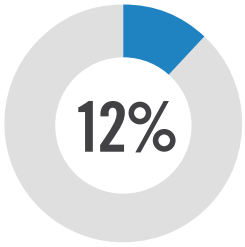
Have deployed user activity monitoring

31%

In-app audit system/feature



No visibility at all



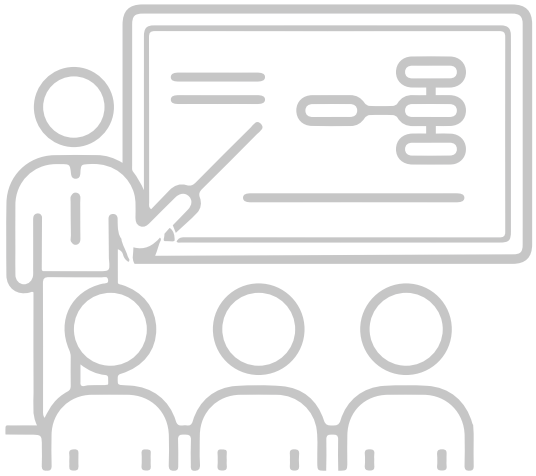
Have deployed keylogging

Not sure/other 14%

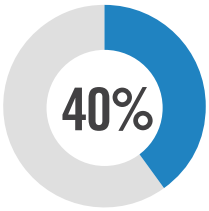
COMBATING INSIDER THREATS

The most utilized tactic in combating insider threats is user training (49%) 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 (40%) and user activity monitoring (36%).

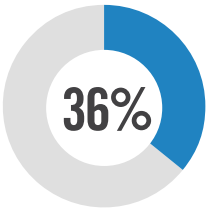
How does your organization combat insider threats today?



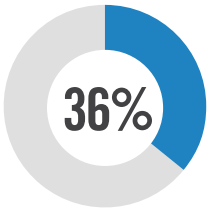
49%
User training



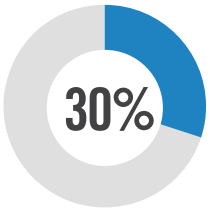
Information security governance program



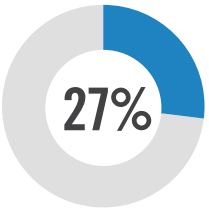
User activity monitoring



Background checks



Database activity monitoring



Secondary authentication

Specialized third-party applications and devices 19% | Native security features of underlying OS 19% | Managed Security Service Provider 14% | Custom tools and applications developed in-house 13% | We do not use anything 6% Not sure/other 2%

SIEM HURDLES

Not enough resources to operate SIEM is the single biggest bottleneck to more effective use of the platform (31%). This is followed by being overwhelmed by too many false positive alerts (22%) and not being able to detect unknown threats (18%).

What is your biggest hurdle in maximizing the value of your SIEM?

31%

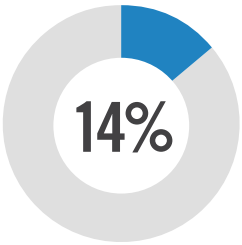
Not enough resources

22%

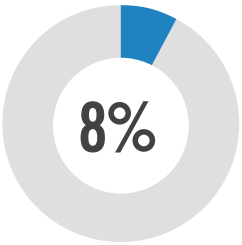
Too many false positives

18%

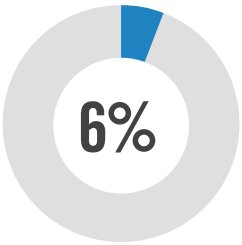
Can't detect unknown threats



Inability to prioritize risk



Not logging the right data

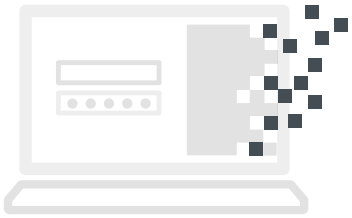


Can't import all the data needed

FOCUS ON DETERRENCE

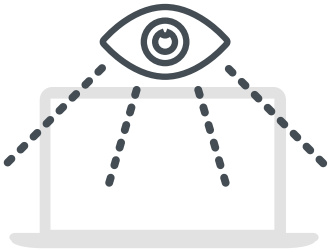
While all methods of countering insider threats are important, organizations are shifting their focus towards deterrence (61%) and detection of internal threats (60%), while analysis and post breach forensics (45%) and deception (11%) follow.

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



61%

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

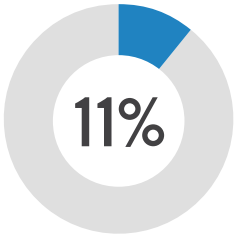


60%

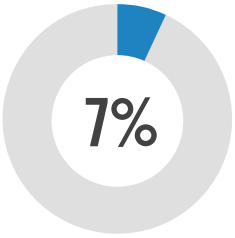
Detection
(e.g., user monitoring, IDS, etc.)

45%

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



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



None

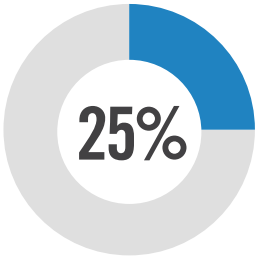
Other 2%

SPEED OF REMEDIATION

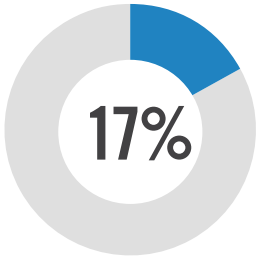
The overwhelming majority of organizations (83%) believe that they can remediate insider threats. However, what may be a major concern is that a significant proportion of companies can only remediate after data loss occurred (42%) – where business impact is much larger.

How quickly can you remediate Insider Threats?

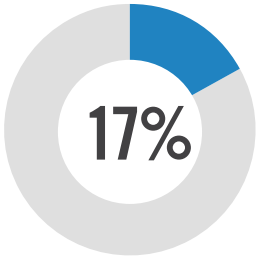
42% After the data has left my organization



In real-time



Before data exfiltration

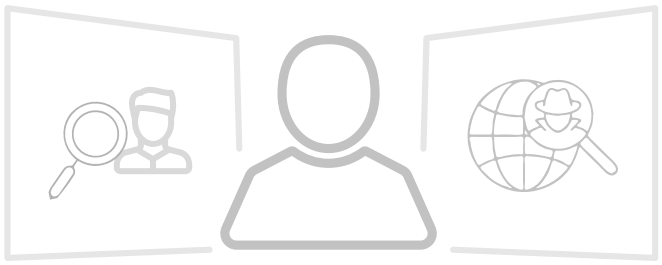


Can't detect insider threats

DETECTION AND RECOVERY

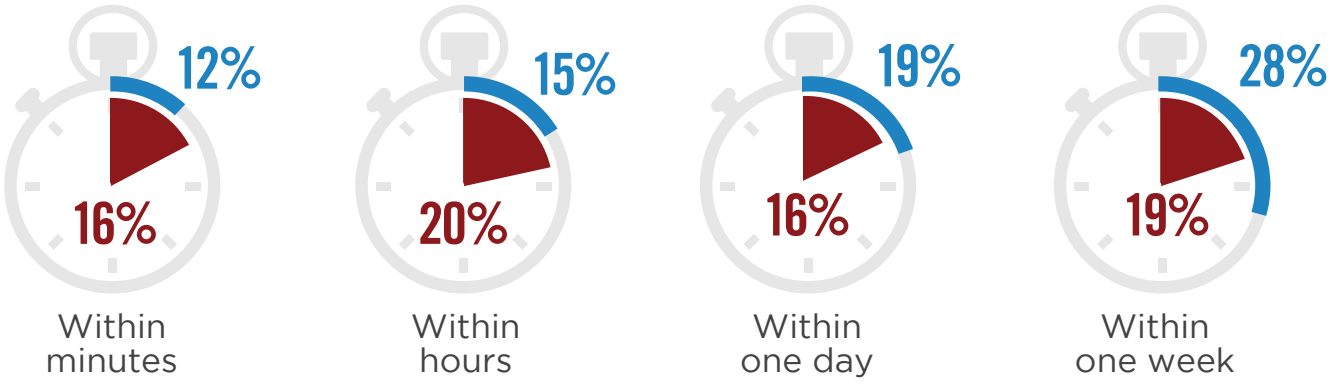
When faced with insider attacks, organizations have a range of detection and recovery speeds. While some are able to detect and respond rapidly (36% claim detection and 27% recovery within hours) – the timeframe for others is substantial (24% detection and 26% recovery times over a month). In general, detection and recovery time periods are correlated, indicating organizations place equal emphasis on detection and recovery.

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



Detect

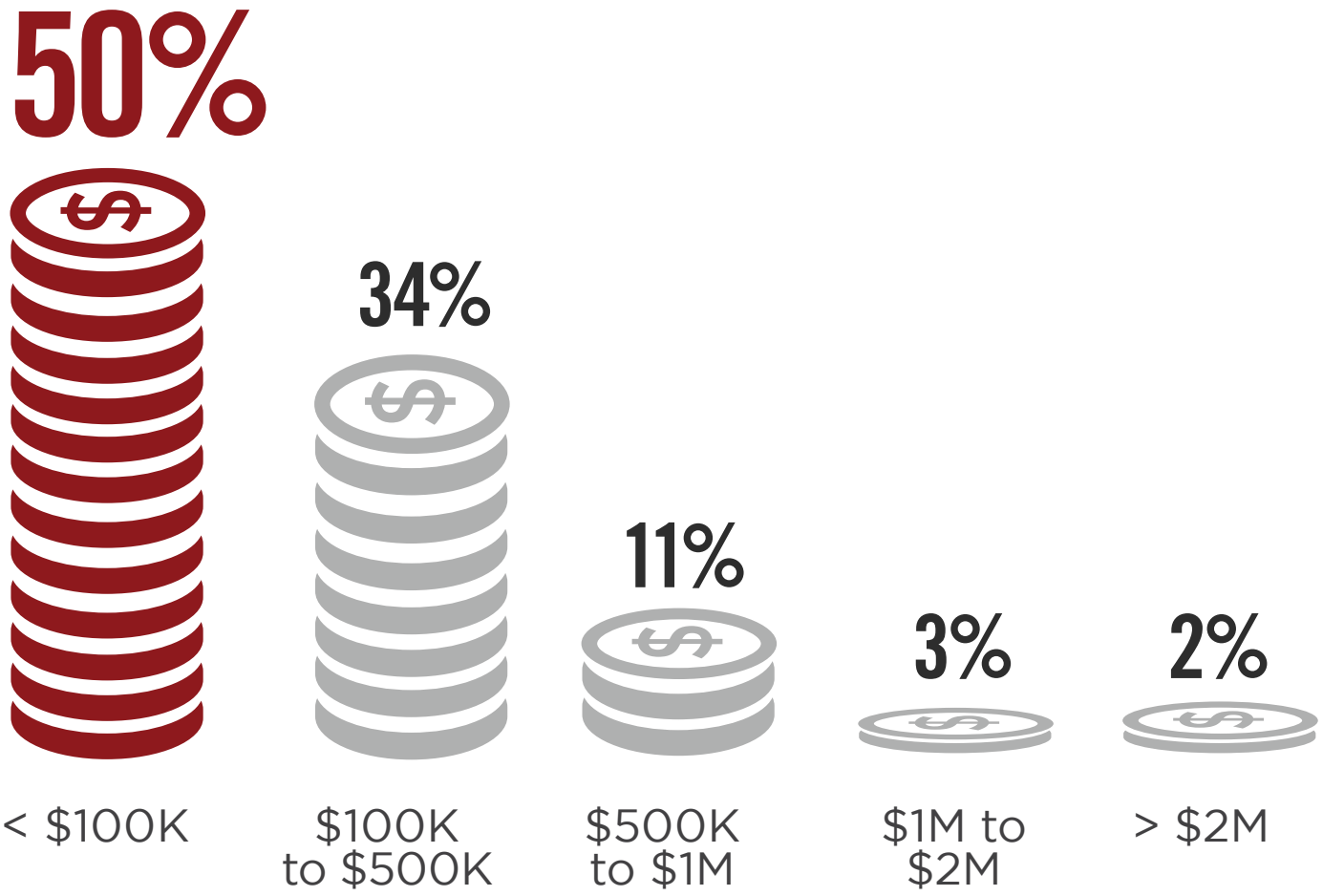
Recover



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 (50%). Thirty-four percent expect damages between $100,000 to $500,000.

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

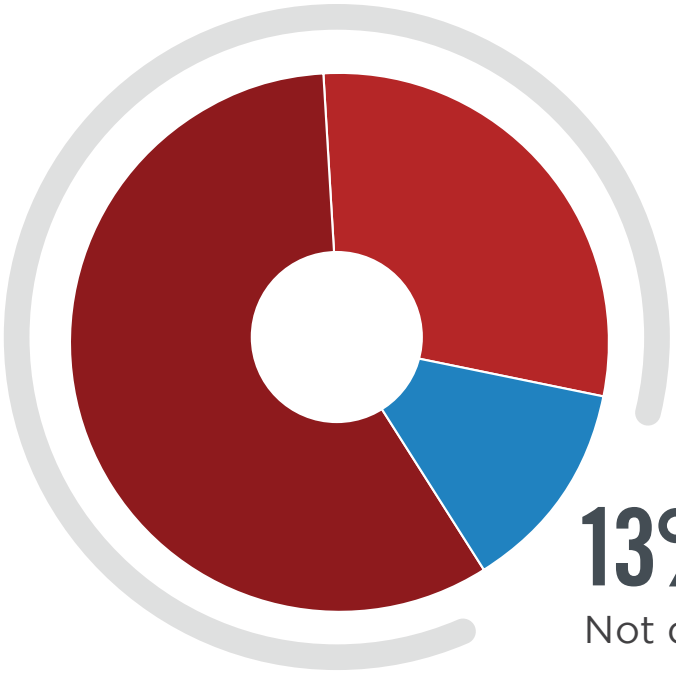


DAMAGES FROM INSIDER ATTACKS

Eighty-seven 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?

87% Find it moderately difficult to very difficult to determine the actual damage of an insider attack.



58% Moderately difficult

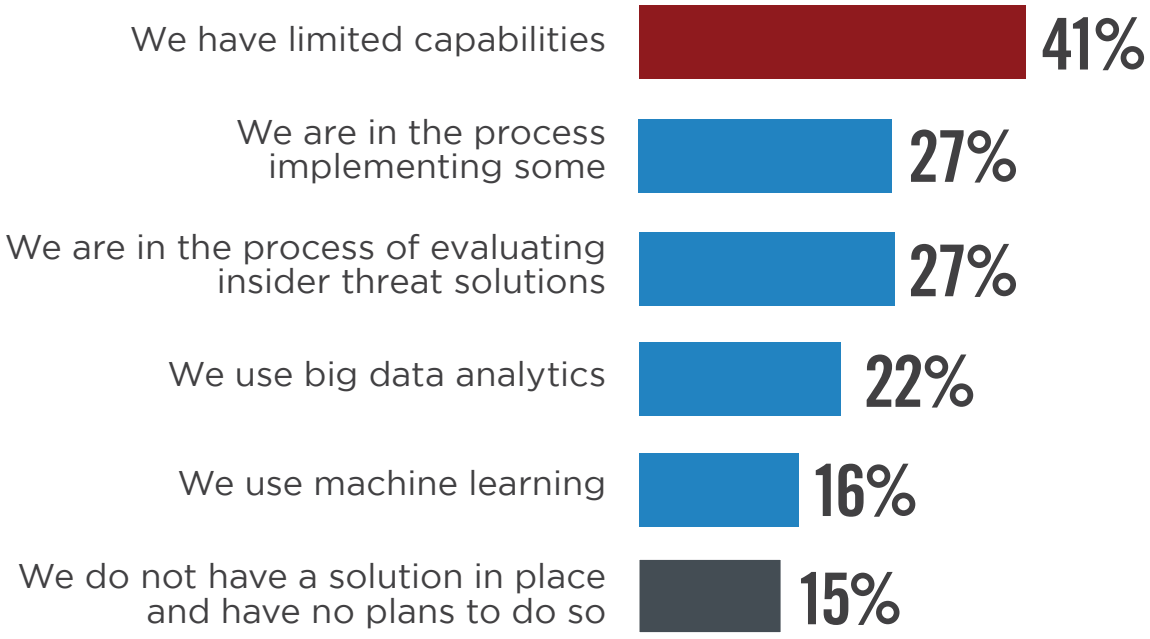
29% Very difficult

13% Not difficult

INSIDER THREAT SOLUTIONS

When asked about insider threat solutions, a majority of organizations still have limited capabilities (41%), while other organizations are in the process of implementing and evaluating solutions (tied at 27%). Only a small fraction of 15% say they have no solutions in place and no plans to implement them.

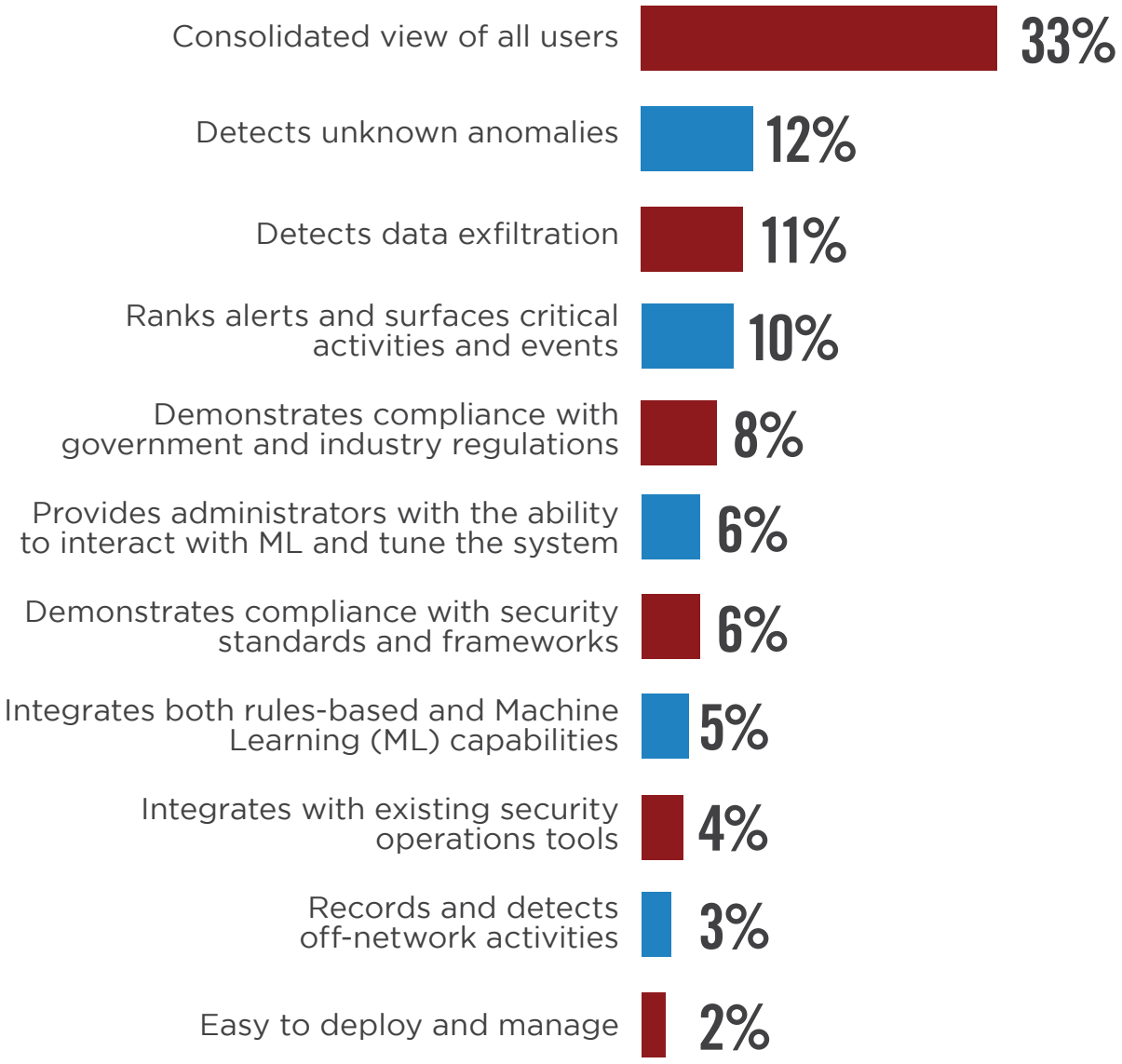
In what ways are you currently using insider threat capabilities?



IMPORTANT CAPABILITIES

When asked to rank insider threat capabilities in terms of importance, organizations selected a consolidated view of all users as the single highest priority capability.

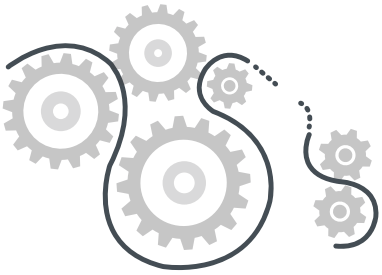
Rank the following insider threat capabilities in terms of importance



INSIDER THREAT IMPACT

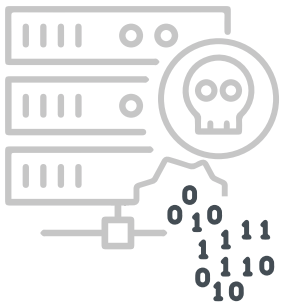
Insider threats have a range of organizational impact, ranging from operational disruption (54%) to loss of critical data (50%) to brand damage (38%).

What impact have insider threats had on your organization?



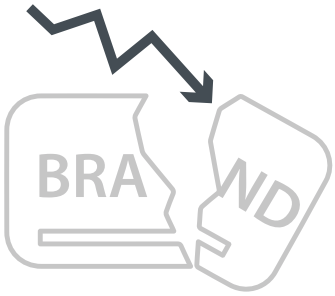
54%

Operational disruption or outage



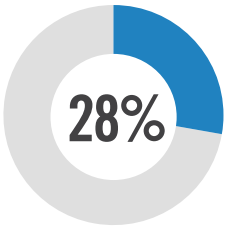
50%

Loss of critical data

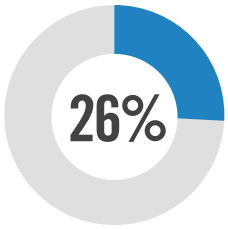


38%

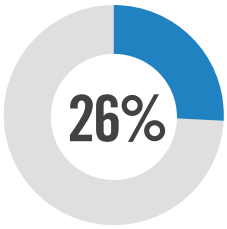
Brand damage



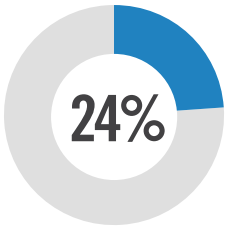
Legal liabilities



Loss in competitive edge



Expenditure remediating successful intrusions



Loss in revenue

Loss in market valuation 20% | No impact 14%

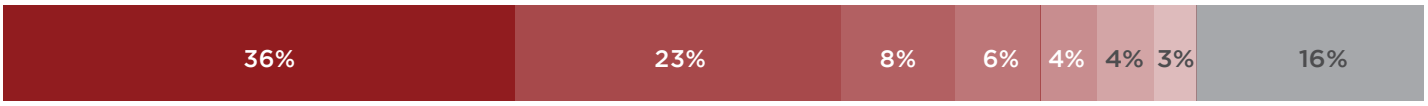
METHODOLOGY & DEMOGRAPHICS

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

Director · Specialist · Manager/Supervisor · Consultant · Owner / CEO / President · CTO, CIO, CISO, CMO, CFO, COO · Vice President · Other

DEPARTMENT

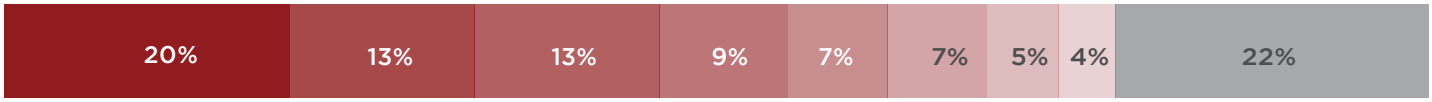


IT Security · IT Operations · Compliance · Operations · Product Management · Engineering · Sales · Other

COMPANY SIZE

Fewer than 10 · 10-99 · 100-999 · 1,000-4,999 · 5,000-10,000 · Over 10,000

INDUSTRY



Technology, Software & Internet · Information Security · Financial Services · Education & Research · Government · Professional Services · Telecommunications · Manufacturing · Other

IT SECURITY TEAM SIZE

No dedicated resources · 1 dedicated security resource · 2 – 5 security resources · More than 5 security resources · Security resources are outsourced · Other