# INSIDER THREAT

## SPOTLIGHT REPORT

Presented by

LinkedIn Group Partner

Information Security

bitglass | DELL Software | Fasoo | LIGHTCYBER CLOSING THE BREACH DETECTION GAP | Lumension A HEAT Software Company | observe it

palerra | RES software | SergeantLaboratories | SpectorSoft | VECTRA Security that thinks | Watchful Keep IT secret.

# INSIDER THREAT
## SPOTLIGHT REPORT

# TABLE OF CONTENTS

# OVERVIEW

Highly publicized insider data theft, such as the recent Morgan Stanley breach or Edward Snowden incident, highlight the increasing need for better security practices and solutions to reduce the risks posed by insider threats.

This report is the result of comprehensive crowd-based research in cooperation with the 260,000+ member Information Security Community on LinkedIn and Crowd Research Partners to gain more insight into the state of insider threats and solutions to prevent them.

Many thanks to our sponsors for supporting this unique research project:

Bitglass | Dell Software | Fasoo | LightCyber | HEAT Software | ObserveIT | Palerra | RES Software | Sergeant Laboratories | SpectorSoft | Vectra Networks | Watchful Software

Thanks to everyone who participated in the survey.
I hope you will enjoy this report.

Holger Schulze

**Holger Schulze**
Group Founder
Information Security
Community on LinkedIn

hhschulze@gmail.com

LinkedIn Group Partner
Information Security

# KEY SURVEY FINDINGS

## The 5 Key Trends for Insider Threats

1. Privileged users, such as managers with access to sensitive information, pose the biggest insider threat to organizations (59 percent). This is followed by contractors and consultants (48 percent), and regular employees (46 percent).

2. 62 percent of security professionals say insider threats have become more frequent in the last 12 months. But only 34 percent expect additional budget to address the problem.

3. Less than 50 percent of organizations have appropriate controls to prevent insider attacks.

4. 62 percent of respondents say that insider attacks are far more difficult to detect and prevent than external attacks.

5. 38 percent of survey respondents estimate remediation costs to reach up to $500,000 per insider attack. 64 percent of respondents find it difficult to estimate the damage of a successful insider attack.


INSIDER THREATS
& VULNERABILITY

# TOP INSIDER THREATS

Data leaks stemming from insider attacks are most concerning to the survey respondents (63 percent). Respondents are slightly more concerned about inadvertent data breaches (57 percent) than malicious breaches (53 percent).

**63%**
Data Leaks


**57%**
Inadvertent Data Breach (careless user)

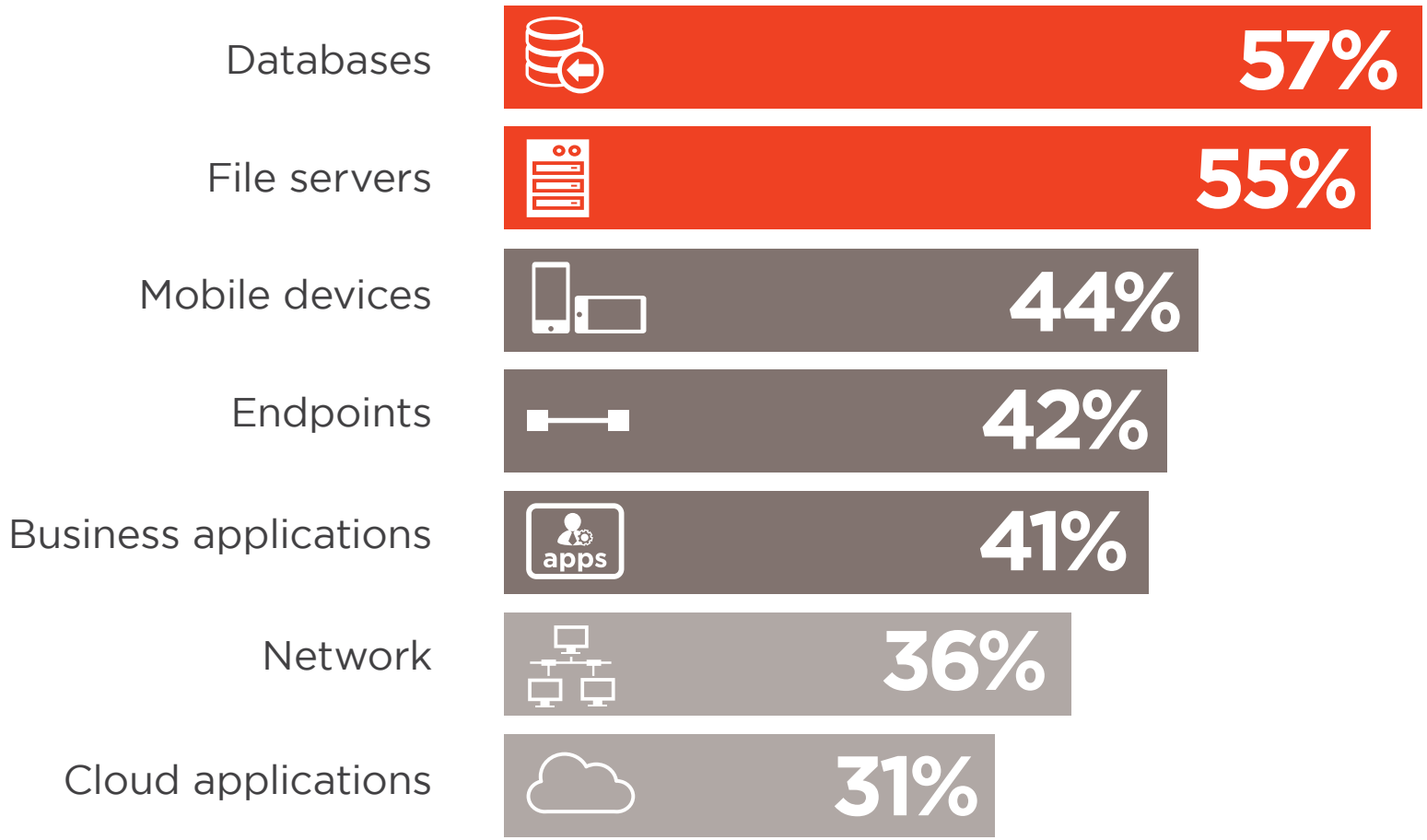
**53%**
Malicious Data Breach

| 36% | 29% | 23% | 20% | 4% |
|---|---|---|---|---|
| Fraud | IP Theft | Espionage | Sabotage | Not Sure/Other |

Q: What type of insider threats are you most concerned about?

# IT ASSETS AT RISK

Databases (57 percent) and file servers (55 percent) are considered most vulnerable to insider attacks. After all, this is where the majority of sensitive data resides.




Q: What IT assets are most vulnerable to insider attacks?

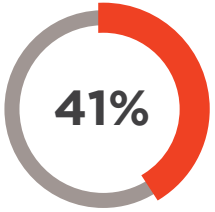
# RISKY USERS

Privileged users, such as managers with access to sensitive information, pose the biggest insider threat (59 percent). This is followed by contractors and consultants (48 percent), and regular employees (46 percent).

**59%**
Privileged Users

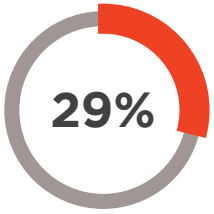
**48%**
Contractors/Consultants Temporary Workers

**46%**
Regular Employees

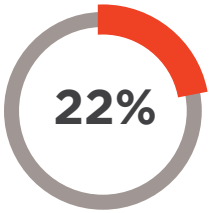



IT administrators & staff

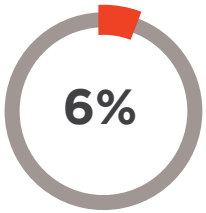

3rd party service providers




Executive management




Business partners, customers, suppliers

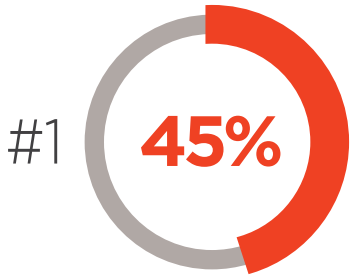



Not Sure Other

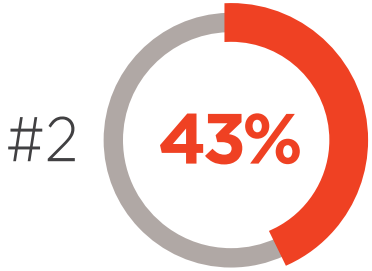
Q: What user groups do you believe pose the biggest security risk?

# MOST VULNERABLE APPS

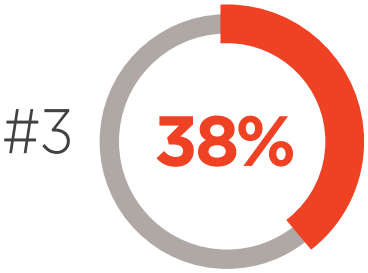
Collaboration & communication apps, such as email, are most vulnerable to insider attacks (45 percent), followed by cloud storage & file sharing apps such as Dropbox (43 percent). Finance and accounting apps come in third with 38 percent.



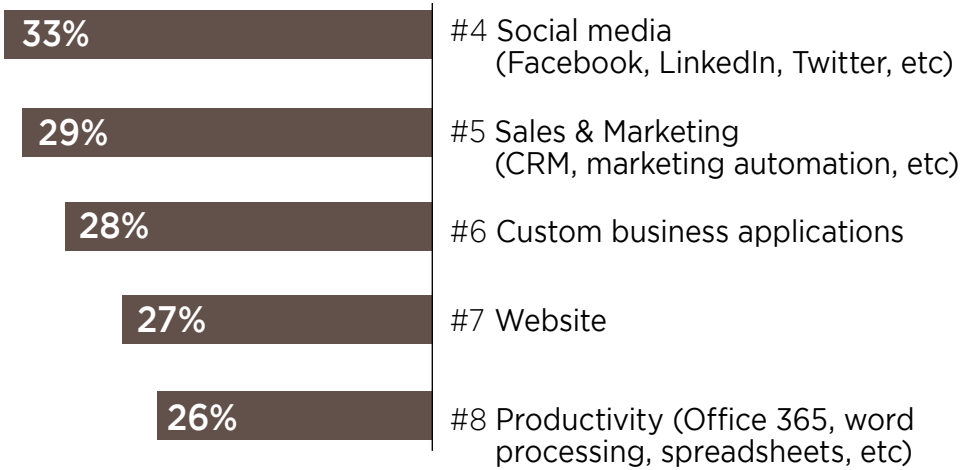

Collaboration & communication




Cloud storage & file sharing apps




3 Finance & accounting

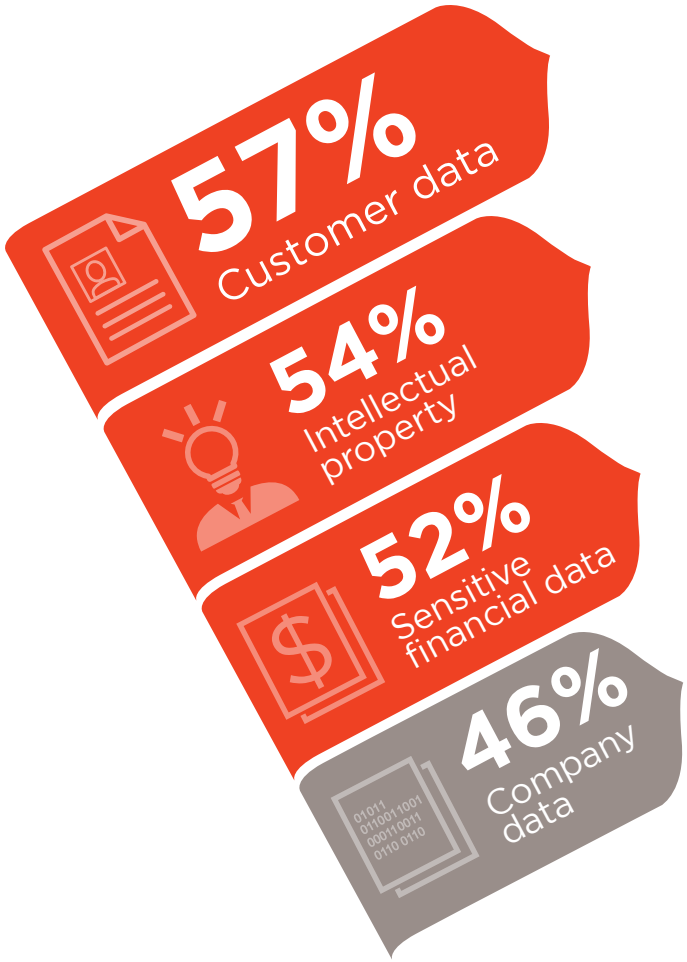



IT Operations 25% | Application development & testing 24% | Business intelligence / Analytics 23% | Cloud applications 22% | HR 21% | Content management 18% | Disaster recovery / Storage / Archiving 14% | Supply chain management 12% | Project management 9% | Not sure / Other 6%

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

# DATA MOST VULNERABLE TO INSIDER ATTACKS

Due to its value to attackers, customer data is most vulnerable to insider attacks (57 percent), closely followed by intellectual property (54 percent), and financial data (52 percent).




## MOST VULNERABLE DATA TO INSIDER ATTACKS

**45%** Employee data

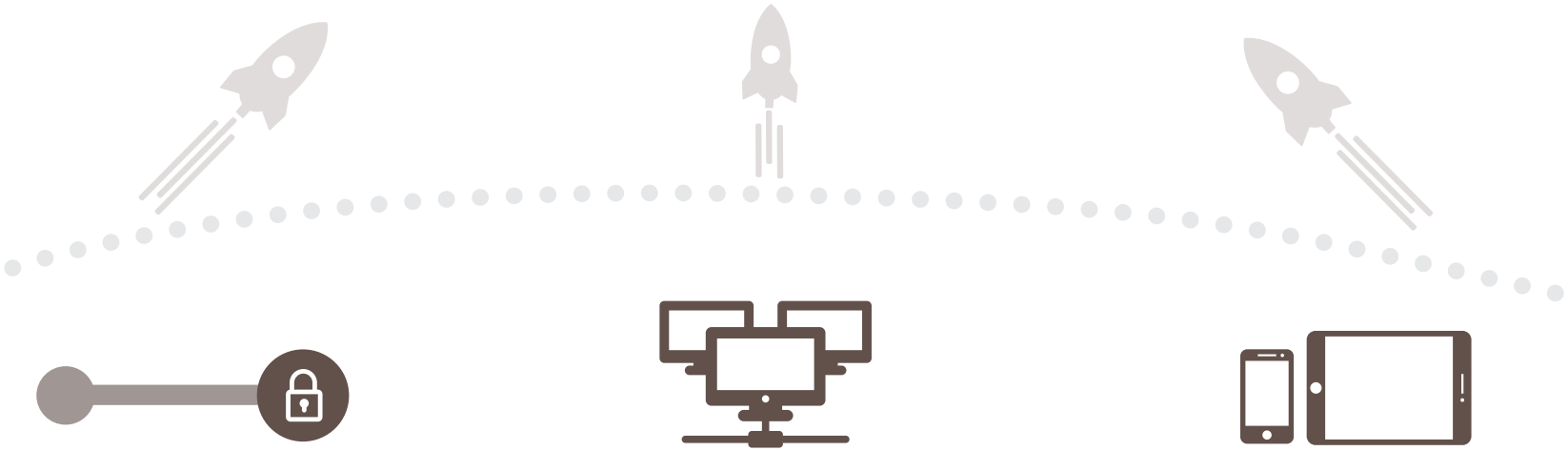
**30%** Sales & marketing data

**20%** Healthcare data

Q: What types of data are most vulnerable to insider attacks?

# LAUNCH POINTS FOR INSIDER ATTACKS

Endpoints are by far the most common launch point for insider attacks (56 percent), highlighting the need for robust endpoint security and policies. This is followed by networks (43 percent) and mobile devices (42 percent) as starting points of insider attacks.



**56%**
Endpoints

**43%**
Network

**42%**
Mobile devices

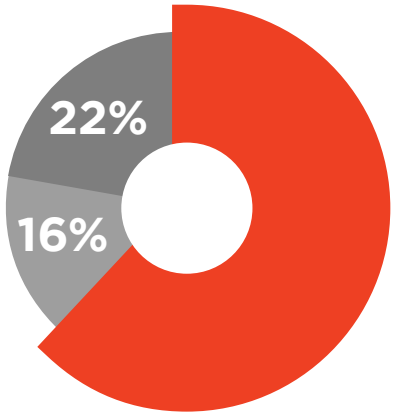
File servers 35% | Cloud applications 22% | Databases 22% | Business applications 22% | Not sure / Other 14%

Q: What IT assets are most commonly used to launch insider attacks from?

# THE RISE OF INSIDER ATTACKS

A majority of security professionals (62 percent) saw a rise in insider attacks over the last 12 months.

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




**62%**

think there were more insider attacks in the past 12 months.

Yes No Not sure

This rise in insider attacks is mostly due to a combination of three factors: insufficient data protection strategies and solutions (53 percent), the proliferation of sensitive data moving outside the firewall on mobile devices (50 percent), and lack of employee training and awareness (50 percent).


Insufficient data protection strategies or solutions


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

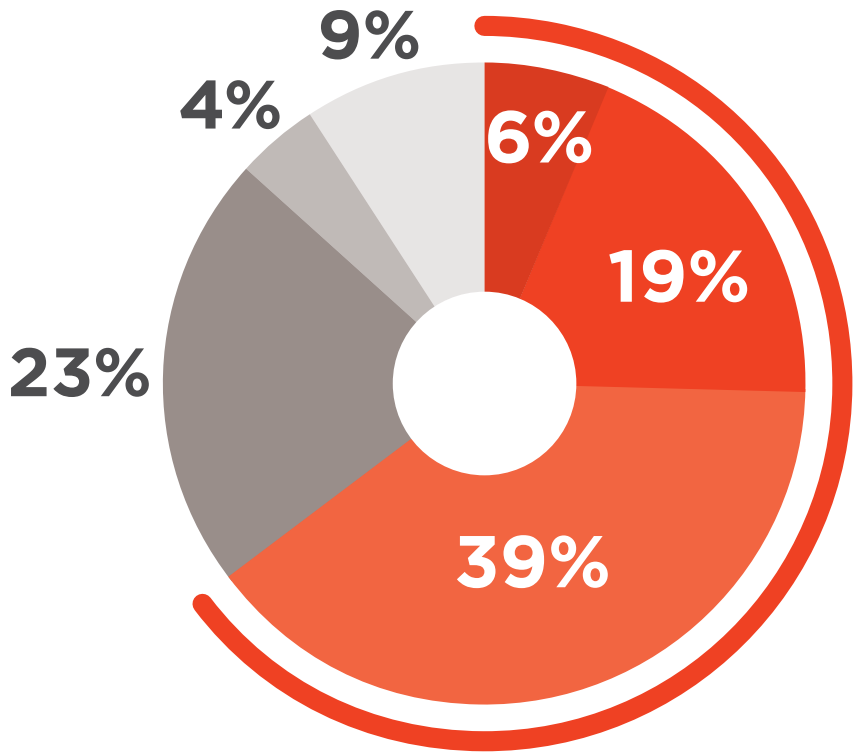

Lack of employee training / awareness

Increasing number of devices with access to sensitive data 50% |
More employees, contactors, partners accessing the network 34% |
Increased public knowledge or visibility of insider threats that were previously undisclosed 27% |
Increasing amount of sensitive data 27% | Technology is becoming more complex 25% |
Not sure / Other 7%

Q: What do you believe are the main reasons why insider threats are rising?

# VULNERABILITY

64 percent feel extremely, very or moderately vulnerable to insider threats.




**64%**

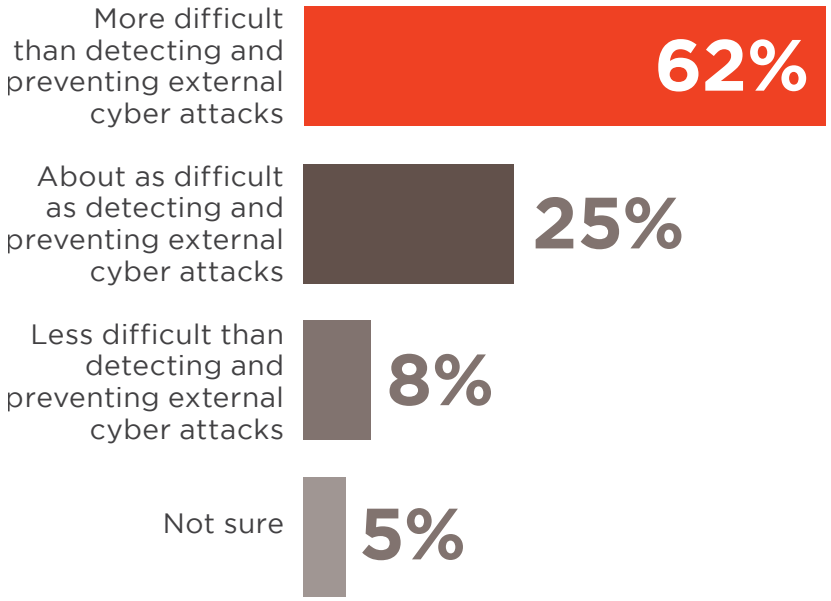
vulnerable to insider threats

- Extremely vulnerable
- Very vulnerable
- Moderately vulnerable
- Slightly vulnerable
- Not at all vulnerable
- Not sure

Q: How vulnerable is your organization to insider threats?

# INTERNAL VS EXTERNAL ATTACKS

A majority of respondents (62 percent) say that insider attacks are more difficult to detect and prevent than external attacks.




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

The key reasons for the difficulty in detecting and preventing insider attacks are that insiders often already have access to systems and sensitive information (66 percent), the increased use of cloud based apps (58 percent), and the rise in the amount of data that is leaving the protected network perimeter (42 percent).

**66%** Insiders already have credentialed access to the network and services

**58%** Increased use of applications that can leak data (e.g., Web email, DropBox, social media)

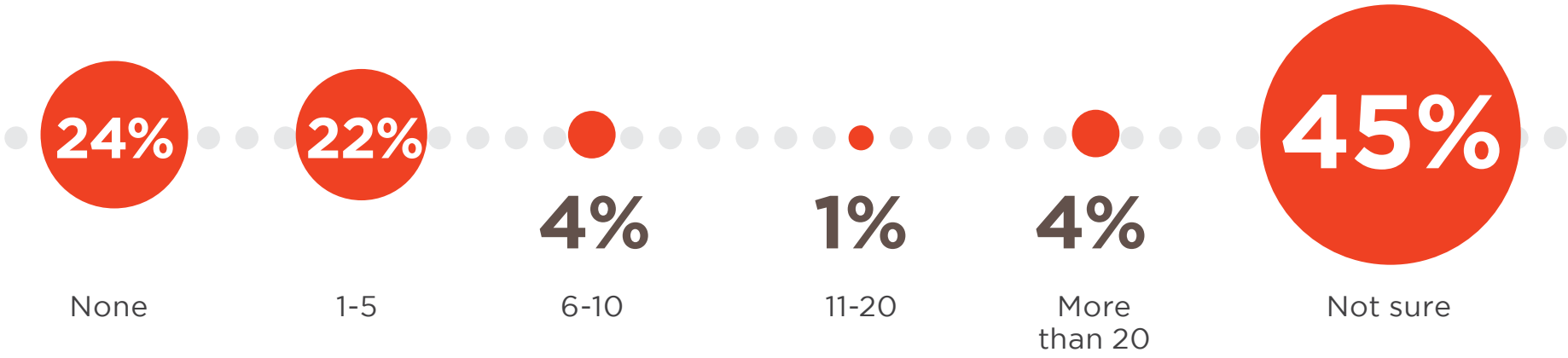

**42%** Increased amount of data that leaves protected boundary / perimeter

More end user devices capable of theft 39% | Difficulty in detecting rogue devices introduced into the network or systems 27% | Insiders are more sophisticated 26% | Not sure / Other 8%

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

# FREQUENCY OF INSIDER ATTACKS

45 percent of respondents can't determine whether their organizations experienced insider attacks in the last 12 months. 22 percent experienced between one and five attacks. About a quarter of organizations believe they experienced no attacks at all. The average number of known insider attacks is 3.8 incidents per organization per year.

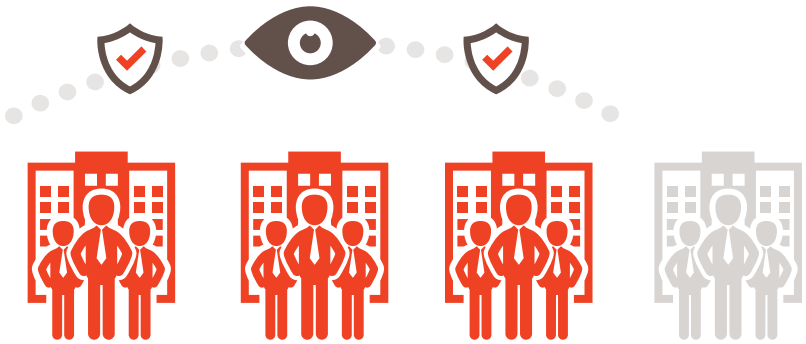



Q: How many insider attacks did your organization experience in the last 12 months?

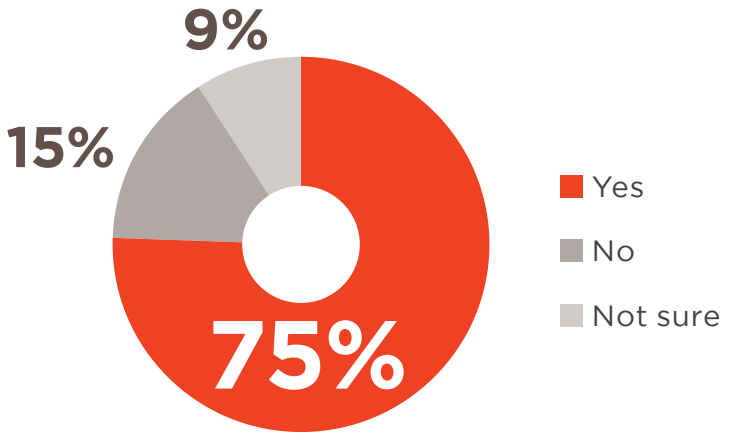

THREAT
DETECTION

# MONITORING OF APPLICATIONS

Three in four companies monitor the security controls of their applications.

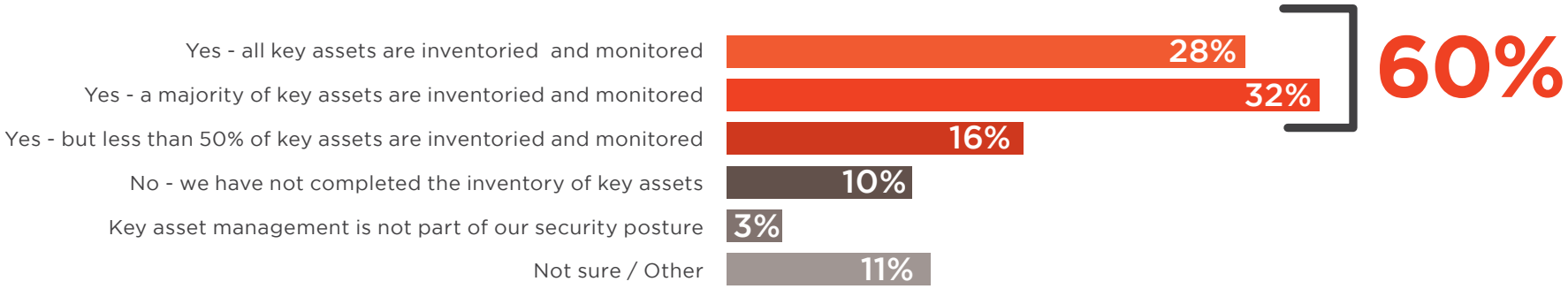


Q: Does your organization monitor security configurations / controls of your applications?




## MONITORING OF KEY IT ASSETS

60 percent of organizations monitor a majority or all of their key IT assets.

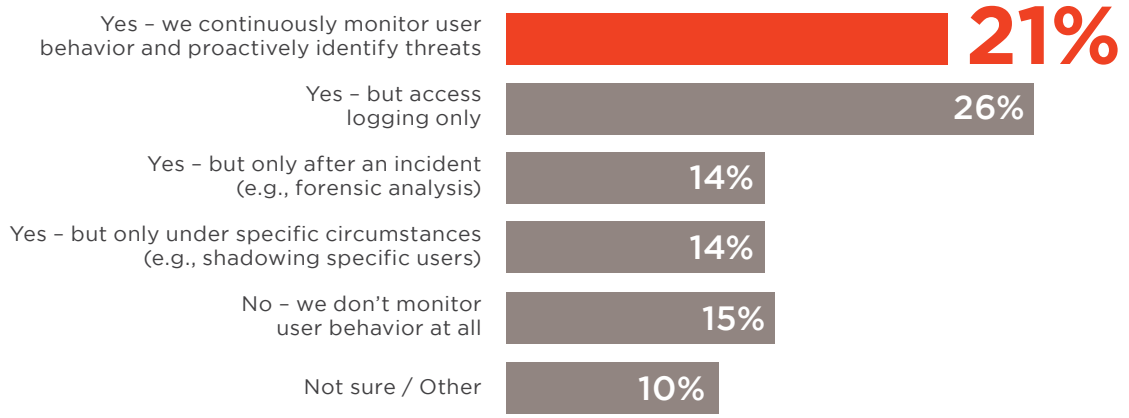



Q: Do you monitor key assets and system resources?

# USER BEHAVIOR MONITORING

Only 21 percent of organizations continuously monitor user behavior taking place on their network. While most organizations' emphasis is on assets, it is important to monitor both the IT assets and user behavior for more effective protection against insider threats.

Q: Do you monitor user behavior?




## VISIBILITY INTO USER BEHAVIOR

Most organizations (48 percent) rely on server logs to review user behavior. Only 28 percent have deployed dedicated user activity monitoring solutions.


**48%**
Server Logs

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

In-app audit system / Feature 31% | Have deployed user activity monitoring 28% | No visibility at all 17% | Have deployed keylogging 7% | Not sure / Other 18%

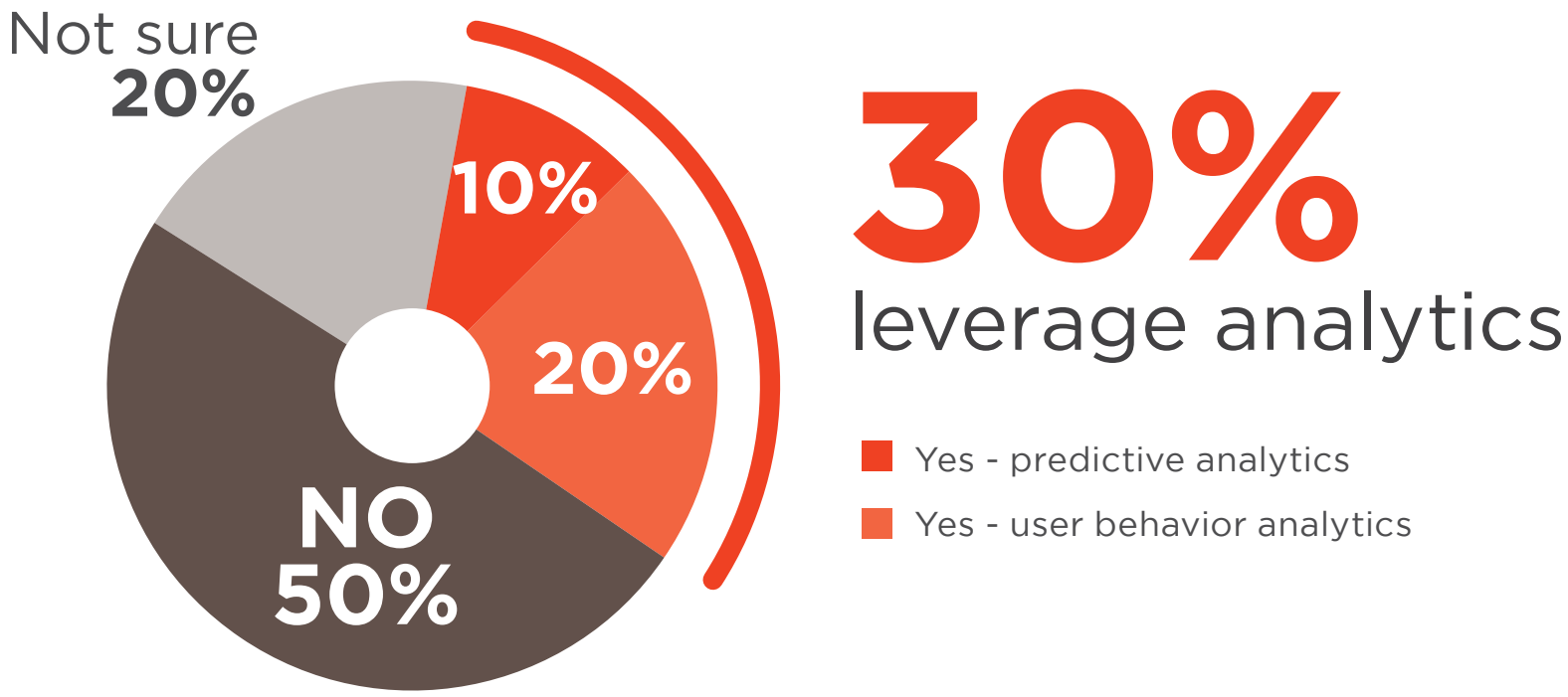
## USER MONITORING IN THE CLOUD

While 75 percent of organizations deploy user monitoring for on-premise applications, only 25 percent monitor user behavior within their cloud footprint.

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

# INSIDER THREAT ANALYTICS

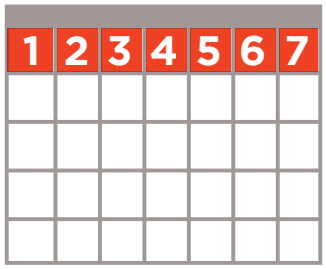
50 percent of organizations do not use analytics to determine insider threats. Of the 30 percent of organizations that leverage analytics, one third uses predictive analytics and two thirds deploy behavior analytics.



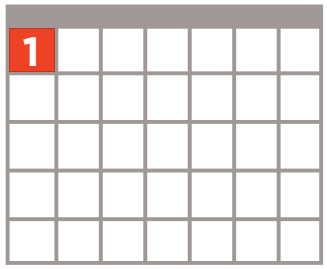

Q: Does your organization leverage analytics to determine insider threats?

# SPEED OF DETECTION

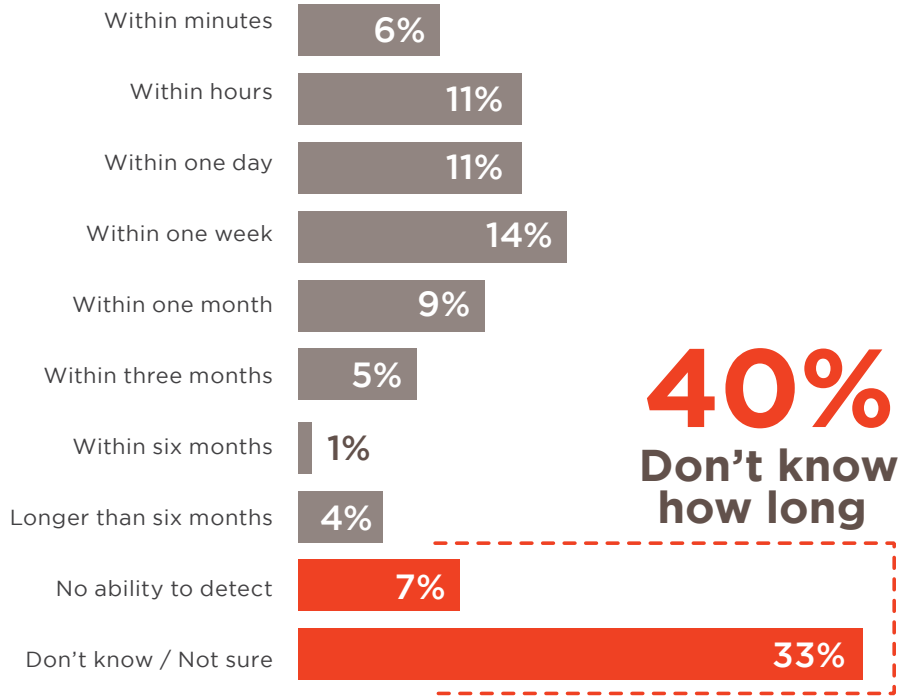
Among the IT professionals who have an opinion on the speed of detecting an insider attack, the most frequent response times are a week or less (42 percent), and for 28 percent of respondents typically within the same day or faster. Perhaps most worrisome is that 40 percent of respondents simply don't know how long detection of an insider attack against their organization would take or have no ability to detect insider attacks at all.




**42%**
**in a week or less**




**28%**
**within the same day or faster**



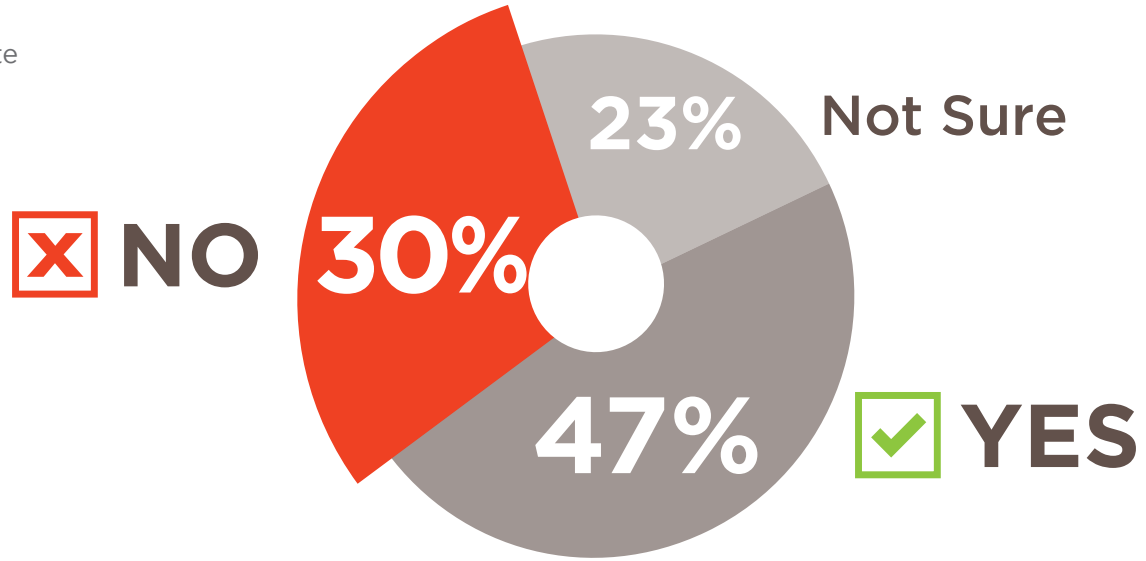

Q: How long would it typically take your organization to detect an insider attack?


SECURITY TOOLS
& PROCESSES

# CONTROLS TO COMBAT INSIDER THREATS

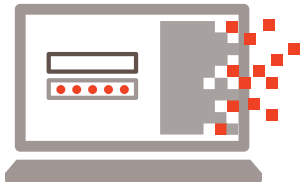
30 percent of organizations today do not have the appropriate controls to prevent an insider attack.

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



# FOCUS ON DETERRENCE

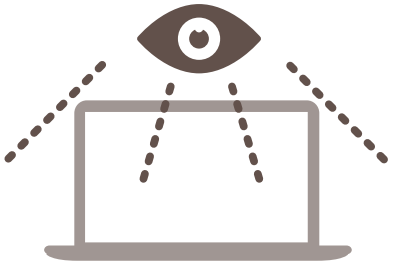
Most organizations place their insider threat management focus and resources on deterrence tactics (63 percent), followed by detection (51 percent) and analysis & forensics (41 percent).



**63%**

## Deterrence

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



**51%**

## Detection

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


**41%**

## Analysis & Forensics

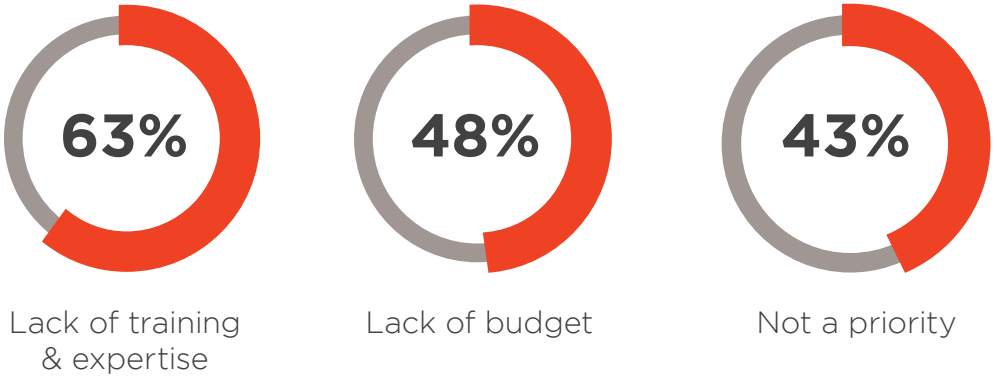
(e.g., SIEM, user monitoring, etc.)

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

# BARRIERS TO BETTER INSIDER THREAT MANAGEMENT

The biggest perceived barriers to better insider threat management are all organizational, starting with a lack of training and expertise (63 percent). Rounding out the top three are insufficient budgets (48 percent) and lack of making insider threat defense a priority (43 percent). Surprisingly, technology related barriers only come in at 29 percent.

Q: What are the biggest barriers to better insider threat management?




Lack of collaboration between separate departments 40% |
Lack of suitable technology 29% | Lack of staff 23% | Not sure / Other 9%

## BUDGET PRIORITIES

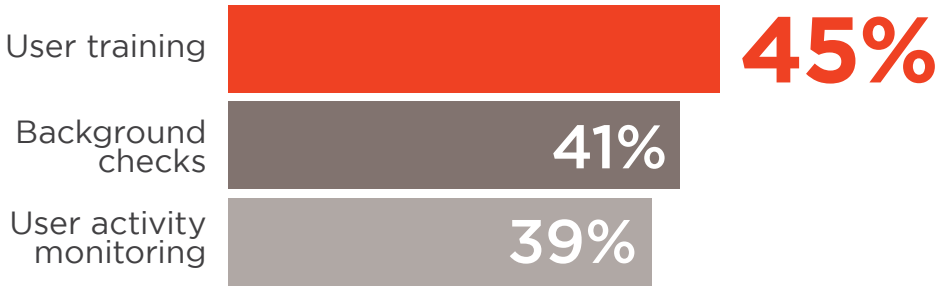
One of the best indicators of changing priorities is the budgeting process. For the respondents who have visibility into the budgets allocated to insider threat management, over a third expect budgets to increase. For 55 percent of respondents budgets will stay flat, and only 11 percent expect a decline.


Q: How is your budget changing in the next 12 months to better detect and prevent insider attacks?

# INSIDER THREAT APPROACH

User training is the most popular tactic to combat insider threats (45 percent) followed by background checks (41 percent) and user activity monitoring (39 percent).


Q: How does your organization combat insider threats today?

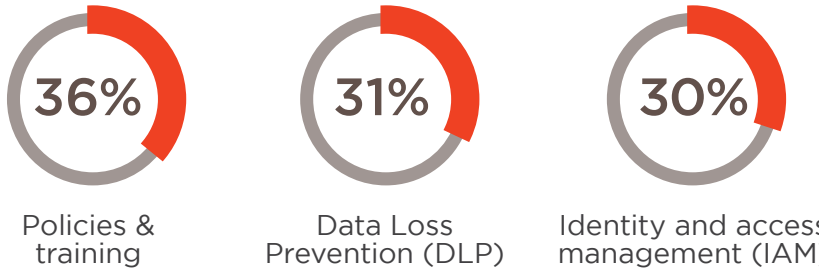



Native security features of underlying OS 28% | Secondary authentication 21% | Password vault 18% | Specialized third party applications and devices 18% | Custom tools and applications developed in house 16% | Managed Security Service provider 11% | We do not use anything 7% | Not sure / Other 14%

## MOST EFFECTIVE TOOLS

Policies and training (36 percent) are considered the most effective tools in protecting against insider threats. Data loss prevention (DLP) tools (31 percent) and identity and access management (IAM) (30 percent) round out the top three.

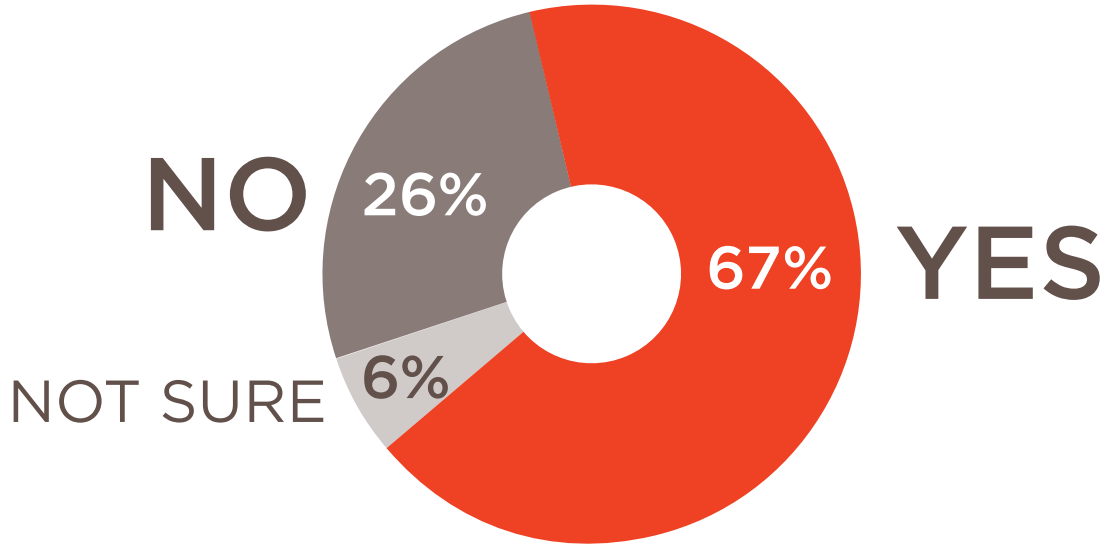
Q: What security tools are most effective in protecting against insider attacks?




User monitoring 28% | User behavior anomaly detection 28% | Encryption of data at rest, in motion, in use 28% | Log analysis 26% | Security information and event – management (SIEM) 26% | Data Access Monitoring 24% | Intrusion Detection and Prevention (IDS/IPS) 23% | Security analytics & intelligence 21% | Multifactor authentication 20% | Endpoint and mobile security 20% | Network defenses (firewalls) 16% | Password vault 11% | Enterprise Digital Rights Management solutions (EDRM) 6% | Cloud Security Gateway 5% | Not sure / Other 8%

# KEEPING TRACK OF SECURITY INCIDENTS

Two thirds of companies keep track of security incidents using a centralized helpdesk and ticketing system.




**67%**

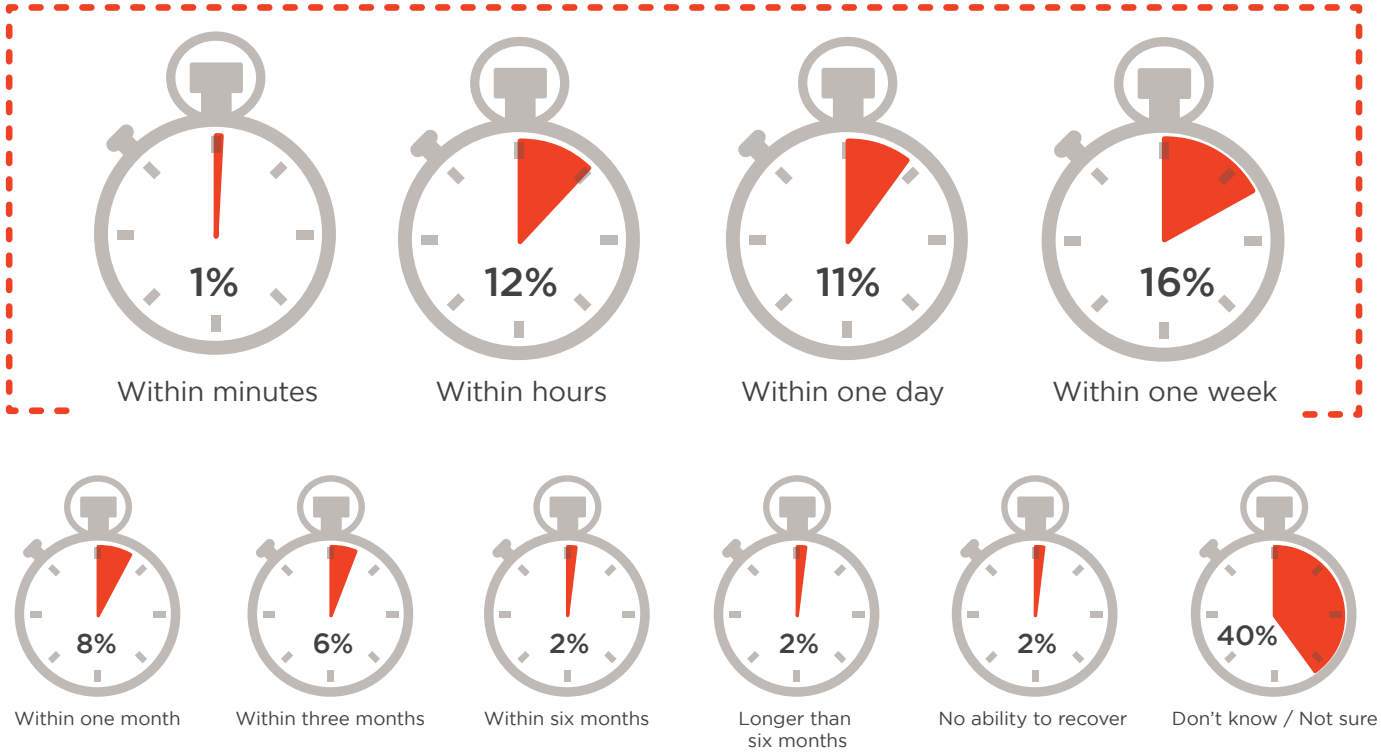
Use central help desk / ticketing system

Q: Do you use a central help desk / ticketing system for security incidents?


RECOVERY &
REMEDIATION

# SPEED OF RECOVERY

The expected speed of recovery from an insider attack follows the same pattern we are seeing for speed of detection. The most common recovery times are a week or less (40 percent). In this context, recovery is defined as closing down the attack vector, considering that a successful attack can result in long lasting economic and reputation damage to the organization. 40 percent of respondents simply don't know how fast their organization would recover from an insider attack.




**40%**

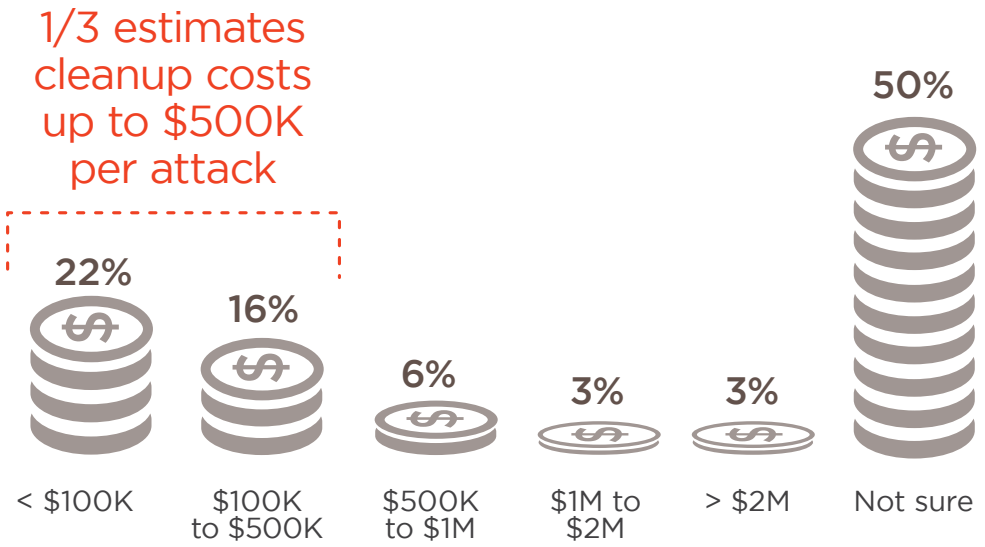
recovery time of a week or less

Q: How long would it typically take your organization to recover from an insider attack?

# COST OF REMEDIATION

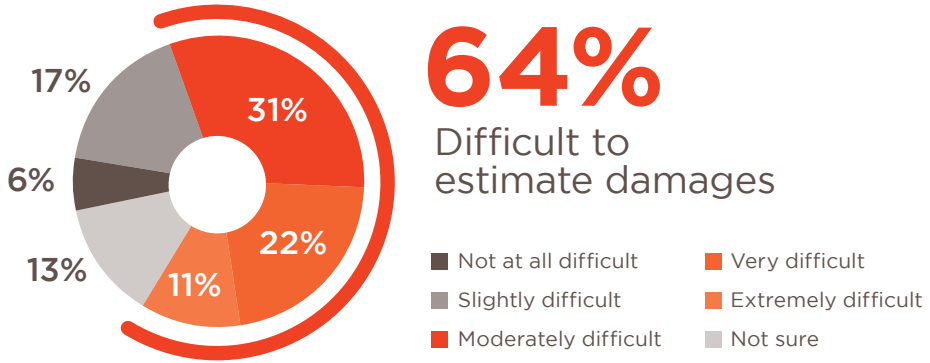
Successful insider attacks can be costly to organizations, from immediate economic impact to long term damages in reputation and customer trust. Over a third of survey respondents estimate remediation costs to reach up to $500,000 per attack. Of those that are able to estimate the average cost of remediation, 24 percent believe the cost exceeds $500,000 and can reach in the millions. The overall estimated cost of remediating a successful insider attack is around $445,000. With an average risk of 3.8 insider attacks per year, the total remediation cost of insider attacks can quickly run into the millions of dollars.

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




## DAMAGES FROM INSIDER ATTACKS ARE HARD TO ESTIMATE

64 percent of respondents find it difficult to estimate the damage of a successful insider attack.



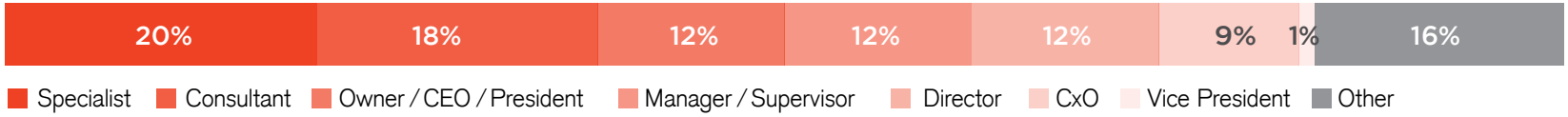

Q: Within your organization, how difficult is it to determine the actual damage of an occurred insider threat?

# METHODOLOGY & DEMOGRAPHICS

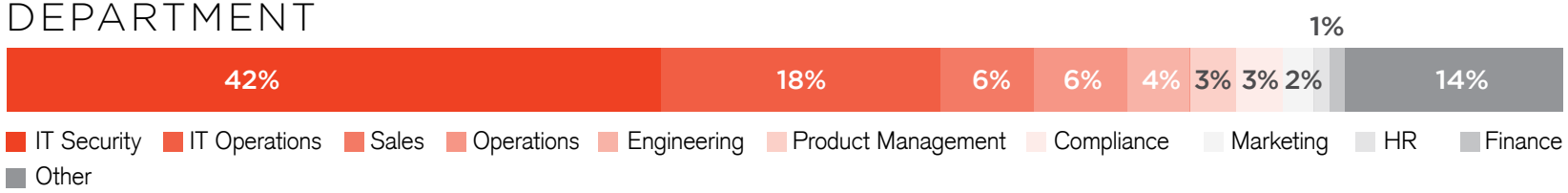
The Insider Threat Spotlight Report is based on the results of a comprehensive survey of over 500 cybersecurity professionals to gain more insight into the state of insider threats and solutions to prevent them.

The respondents range from technical executives to managers and IT security practitioners, and they represent organizations of varying sizes across many industries. Their answers provide a comprehensive perspective on the state of cloud security today.

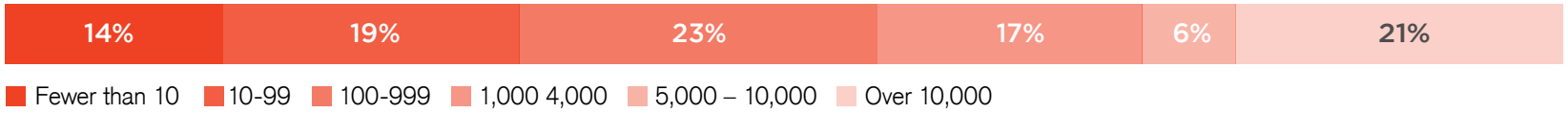
## CAREER LEVEL



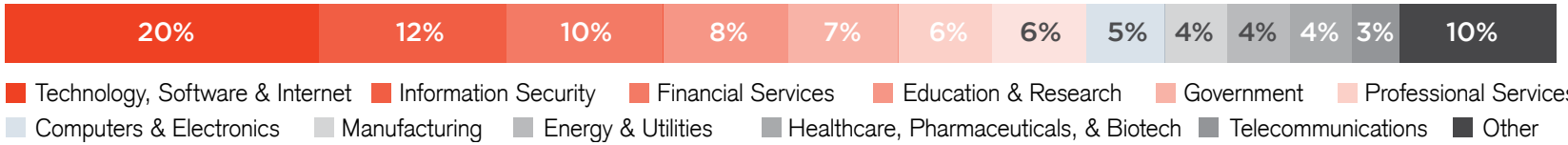

## DEPARTMENT




## COMPANY SIZE




## INDUSTRY



# SPONSORS

We would like to thank our sponsors for supporting the **Insider Threat Spotlight Report.**

## Bitglass | www.bitglass.com

In a world of cloud applications and mobile devices, IT must secure corporate data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are not suited to solving this task, since they were developed to secure the corporate network perimeter. Bitglass is a Cloud Access Security Broker that delivers innovative technologies that transcend the network perimeter to deliver total data protection for the enterprise - in the cloud, on mobile devices and anywhere on the Internet. Founded in 2013 by industry veterans with a proven track record of innovation, Bitglass is based in Silicon Valley and backed by venture capital from NEA and Norwest.

---

## Dell Software | www.dellsoftware.com

Dell Software empowers organizations of all sizes to experience Dell's "power to do more" by delivering scalable yet simple-to-use solutions that can increase productivity, responsiveness and efficiency. Dell Software is uniquely positioned to address today's most pressing business and IT challenges with holistic, connected software offerings across five core solution areas, encompassing data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, helps customers simplify IT, mitigate risk and accelerate business results.

---

## Fasoo | www.fasoo.com

The Fasoo data security framework helps organizations to facilitate and enhance their information security framework based on a data-centric security model with people-centric policies in multi-layered approaches in complex enterprise IT environments. The Fasoo data security framework is ideal for a diversified collaboration environment in cloud and mobile, effective for insider threat management and a last resort against possible APT. Fasoo has successfully retained its leadership in the data-centric security market by deploying solutions for more than 1,200 organizations in enterprise-wide level, securing more than 2.5 million users.

# SPONSORS

We would like to thank our sponsors for supporting the **Insider Threat Spotlight Report.**

## LightCyber | www.lightcyber.com

LightCyber is a leading provider of Active Breach Detection solutions that accurately detect active cyber attacks that have circumvented traditional threat prevention systems. The LightCyber Magna™ platform is the first security product to simultaneously profile both network traffic and endpoint state in order to accurately detect compromised user accounts and devices early in the attack lifecycle, and to enable security operators to remediate breaches and stop attacks before real damage is done. Founded in 2011 and led by world-class cyber security experts, the company's products have been successfully deployed by top-tier customers around the world in the financial, legal, telecom, government, media and technology sectors.

## HEAT Software | www.heatsoftware.com

HEAT Software is a leading provider of Hybrid Service Management (SM) and Unified Endpoint Management (UEM) software solutions for organizations of all sizes. Our UEM solution includes security software which help businesses protect vital information and manage critical endpoint risk, including Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance.

## ObserveIT | www.observeit.com

ObserveIT is the world's leading provider of user activity monitoring software. Founded in 2006, ObserveIT is the only security software company that provides user behavior analytics, alerting and visual forensics to know when users put your business at risk. With ObserveIT, information security teams are able to detect data misuse within core applications, see exactly what's happening in live sessions and act in real time. To do this, ObserveIT provides screen-recording technology to capture all user activity regardless of the environment and converts screenshots into user activity logs that makes it easy to search, analyze, audit and act upon alerts. ObserveIT has more than 1,200 customers in over 70 countries.

# SPONSORS

We would like to thank our sponsors for supporting the **Insider Threat Spotlight Report.**

## Palerra | www.palerra.com

Palerra designed LORIC™ to provide continuous compliance, threat visibility, and automated incident response for an organization's entire cloud footprint (SaaS, PaaS, and IaaS) in a single platform. It automates all steps of the security lifecycle to enable organizations to keep pace with the rapidly increasing volume of cloud usage as well as the velocity of change in the threat landscape. LORIC does so without any hardware or software, and does not impact the native user experience for cloud usage. Today enterprises across financial services, consumer hospitality, hi-technology and more use LORIC from Palerra, to secure their Cloud footprint.

## RES Software | www.ressoftware.com

RES Software, the leader in digital workspace technology, helps organizations achieve better business results with reduced security risks and improved regulatory compliance -- without disrupting the employee experience with technology. Our people-centric approach to services and security enables the enterprise to empower the digital workforce far beyond the capabilities of simple antivirus and firewall technologies. By making technology access secure, even in multiple device/multiple location scenarios, RES enhances internal threat protection, IT control, and secure employee engagement. RES boasts numerous patented technologies, faster time to value, and superior customer support for more than 3,000 companies around the world.For more information, visit www.ressoftware.com or follow updates on Twitter @ressoftware.

## Sergeant Laboratories | www.sgtlabs.com

Sergeant Laboratories' premier solution, AristotleInsight, brings quant management to information security. See which users have privileged access, when privileges are elevated, and what data each user touches. See when RDP and VPN connections are made, who made them, what data was accessed, and exactly what occurred during the connection. See every change in your Active Directory; including what the change was, who made it, and which device the change was made from. AristotleInsight provides these insights and more within a practical solution that is immediately useful, installs seamlessly, and 'just runs' without oversight.

# SPONSORS

We would like to thank our sponsors for supporting the **Insider Threat Spotlight Report.**

## SpectorSoft | www.SpectorSoft.com

SpectorSoft is the leader in user activity monitoring and an innovator in user behavior analysis software. SpectorSoft has helped more than 36,000 businesses, government organizations, schools and law enforcement agencies improve how they address security and achieve compliance. SpectorSoft award-winning solutions include enterprise-grade insider threat detection software, a powerful user activity monitoring solution deployed by thousands of companies in more than 110 countries, robust Event and Security Log Management, and the world's leading employee investigation tool.

---

## Vectra Networks | www.vectranetworks.com

Vectra Networks is the leader of real-time detection of cyber attacks in progress. The Vectra X-series breach detection platform continuously monitors network traffic to automatically detect any phase of an ongoing cyber attack. The platform provides visually intuitive reports of hosts under attack and context about what the attacker is doing. Vectra automatically prioritizes attacks that pose the greatest business risk, enabling organizations to quickly make decisions on where to focus their time and resources. Vectra Networks' investors include Khosla Ventures, IA Ventures and AME Cloud Ventures. The company's headquarters are in San Jose, California.

---

## Watchful Software | www.watchfulsoftware.com

Watchful Software provides advanced persistent security solutions that keep sensitive information safe from security breaches resulting from accidental or malicious disclosure. Watchful was formed to protect an organization's most critical asset after its people – its information. The company addresses the growing need for protecting sensitive and proprietary information against accidental or malicious theft, leakage, or loss. Leveraging key technologies including advanced encryption algorithms, digital rights management, and eBiometrics, Watchful has developed a suite of solutions that ensure only authorized personnel have access to enterprise systems and information, protecting against potentially massive economic and competitive damage from cyberterrorists and information thieves.

# CONTACT US

## Interested in co-sponsoring the next security research report?

Contact us to learn more.

info@crowdresearchpartners.com




LinkedIn Group Partner
Information Security