INSIDER THREAT

SPOTLIGHT REPORT

LinkedIn Group Partner

Information Security

Presented by

bitglass

OVERVIEW

Highly publicized insider data theft, such as the recent Morgan Stanley breach and Edward Snowden incidents, highlights the increasing need for better security practices and solutions to counter insider threats. With the rapid adoption of cloud and mobile, the difficulty of preventing such attacks rises substantially.

This report is the result of comprehensive research in cooperation with 500 security professionals, uncovering the hard facts on insider threats and what we as an industry are doing to prevent and detect them.

KEY FINDINGS

1. **Insider Threats on the Rise**
   62% of IT Security professionals say insider threats have become more frequent in the past 12 months.

2. **Cloud and Mobile Drive Increased Insider Threat Concerns**
   Insufficient data protection (54 percent), more data leaving the network (50 percent) and more devices with sensitive data (50 percent) are the top sources of insider threats.

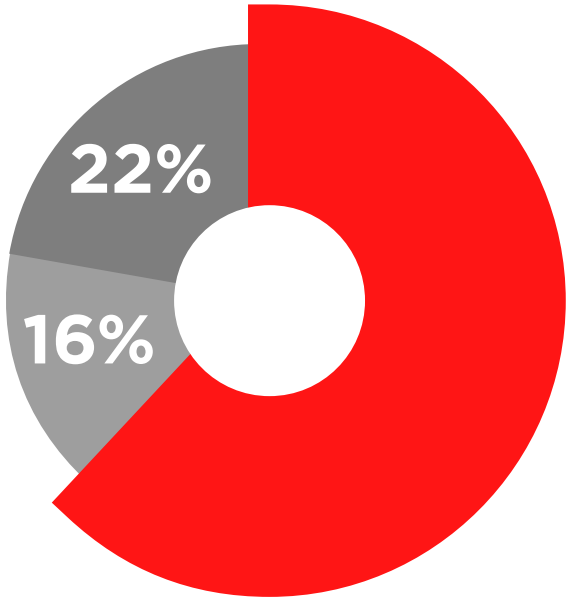
3. **Major Differences Between Threat Detection Confidence and Threat Detection Reality**
   The average data breach lasts 205 days (nearly 7 months), yet only 11 percent of organizations believe it would take even 6 months to detect an insider threat.

4. **What Insider Threats?**
   45 percent of enterprises had no idea how many insider threats actually occurred in their organization during the last year.

5. **Collaboration and Cloud File Sharing Apps are Most Vulnerable**
   Applications most vulnerable to insider threats include collaboration and communication applications (45 percent), cloud storage and file sharing (43 percent) and finance and accounting applications (38 percent).

THE RISE OF INSIDER ATTACKS

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



62%

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

Yes No Not sure

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

CLOUD AND CONSUMERIZATION THE BIG FACTORS

Beyond insufficient security practices, the rise in cloud apps and mobile devices are driving the increase in insider threats.

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?

RISKY USERS

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

59%

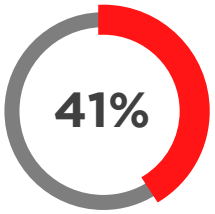
Privileged Users

48%

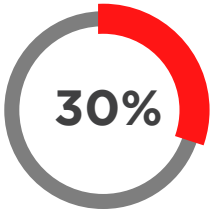
Contractors/Consultants Temporary Workers

46%

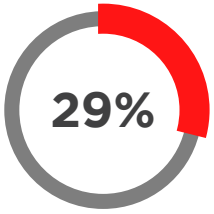
Regular Employees



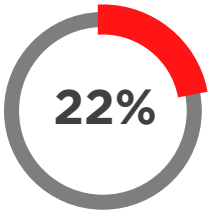
IT administrators & staff



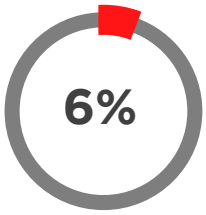
3rd party service providers



Executive management



Business partners, customers, suppliers

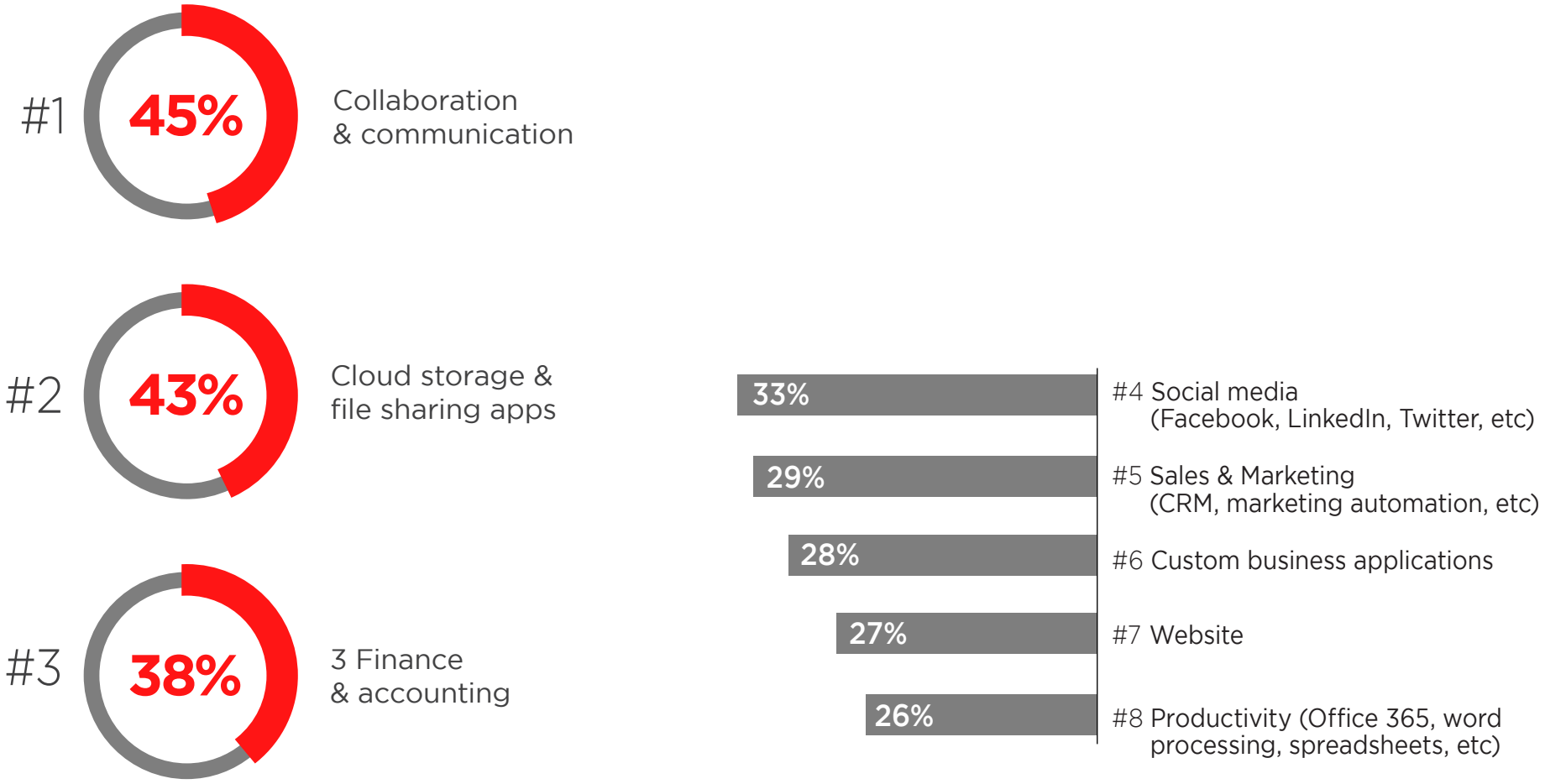


Not Sure Other

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.

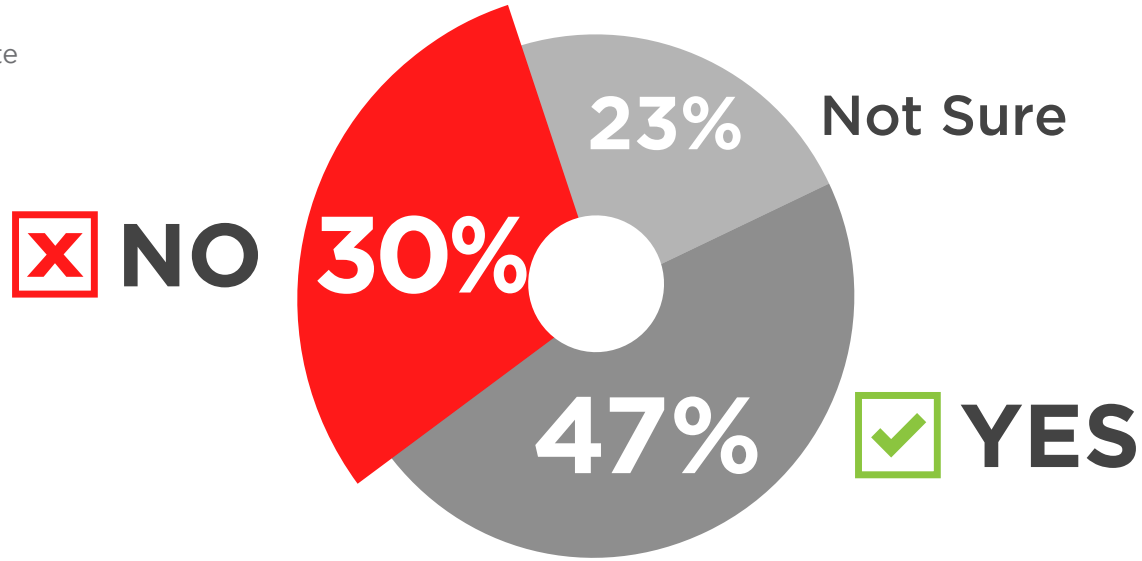


Q: In your opinion, what types of applications are most vulnerable to insider attacks?

CONTROLS TO COMBAT INSIDER THREATS

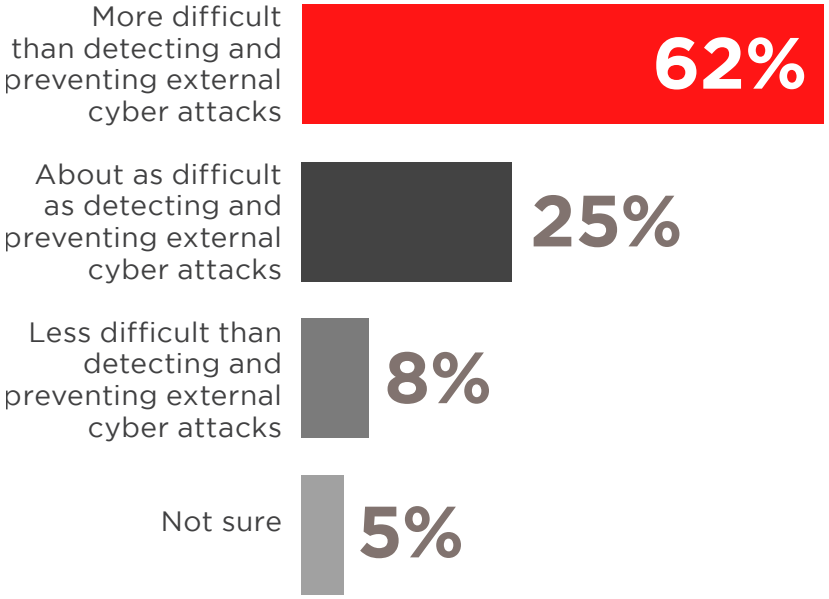
30 percent of organizations today do not have the appropriate controls to prevent an insider attack.

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



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?

Insider threats are becoming more difficult to detect due to increased use of applications that can leak data and an increase in the amount of data leaving the perimeter.

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

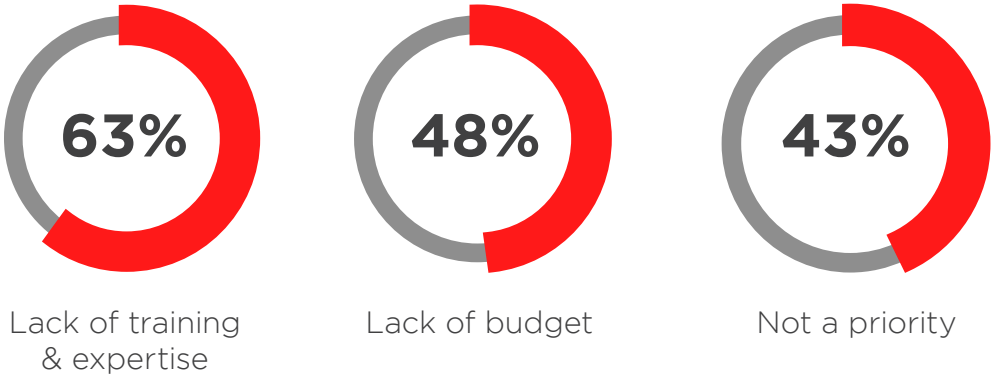
More end user devices capable of theft 39% | Difficulty in detecting rogue devices introduced into the network or systems 27% | Insiders are more sophisticated 26% | Not sure / Other 8%

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

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.

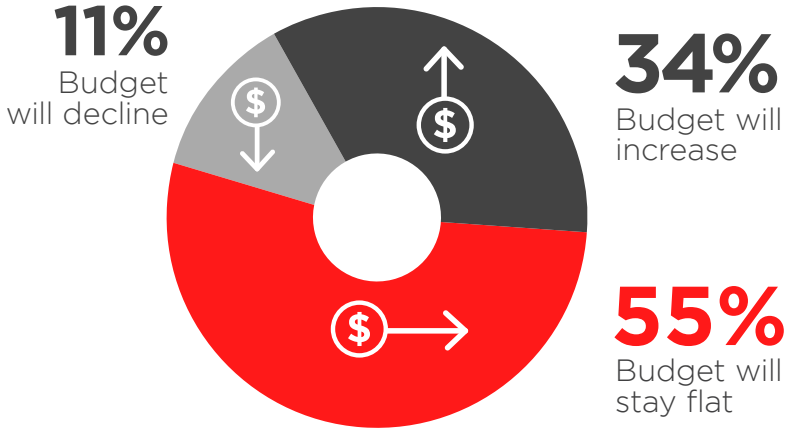
Q: What are the biggest barriers to better insider threat management?



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

BUDGET PRIORITIES

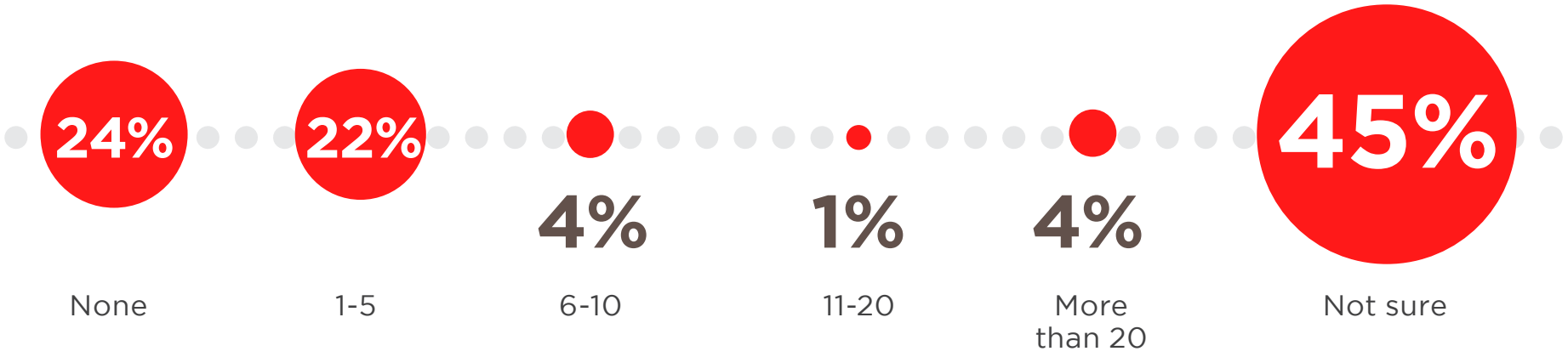
One of the best indicators of changing priorities is the budgeting process. For the respondents who have visibility into the budgets allocated to insider threat management, over a third expect budgets to increase. For 55 percent of respondents budgets will stay flat, and only 11 percent expect a decline.



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

FREQUENCY OF INSIDER ATTACKS

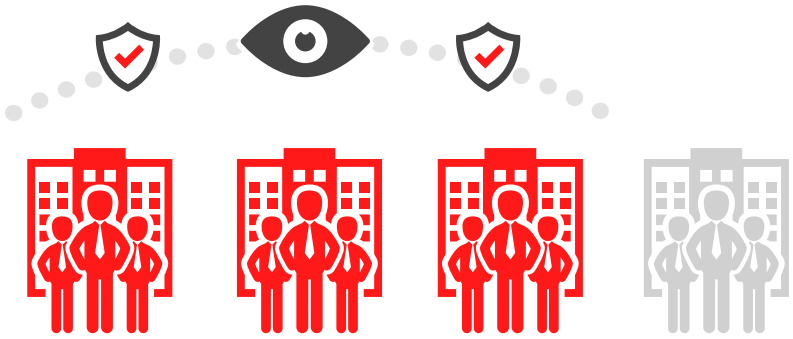
45 percent of respondents can't determine whether their organizations experienced insider attacks in the last 12 months. 22 percent experienced between one and five attacks. About a quarter of organizations believe they experienced no attacks at all. The average number of known insider attacks is 3.8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



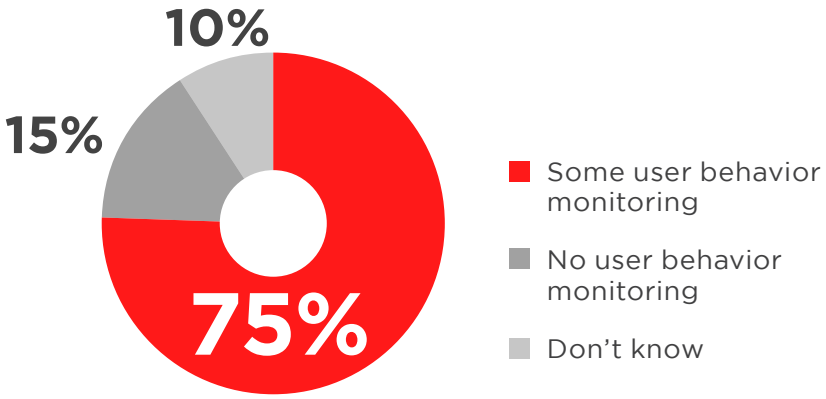
Q: How many insider attacks did your organization experience in the last 12 months?

MONITORING OF APPLICATIONS

75% of organizations perform some sort of user behavior monitoring on their network.

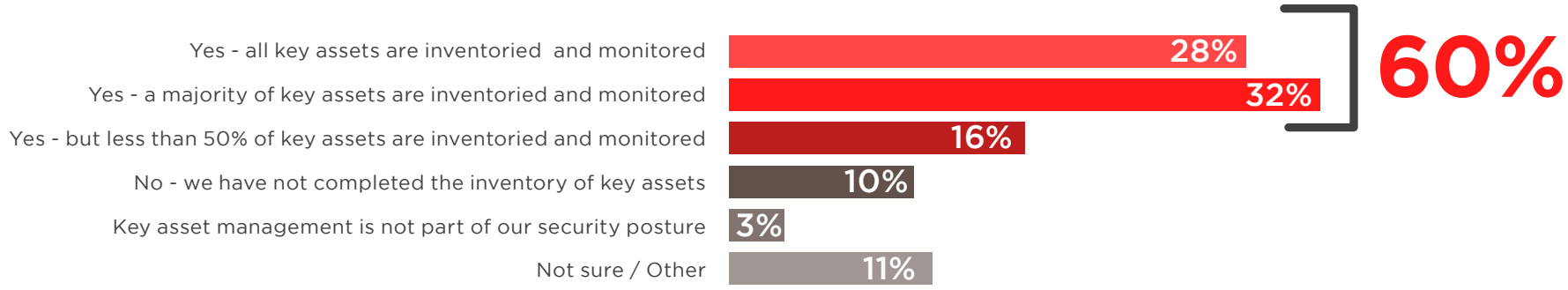


Q: Does your organization monitor security configurations / controls of your applications?



MONITORING OF KEY IT ASSETS

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

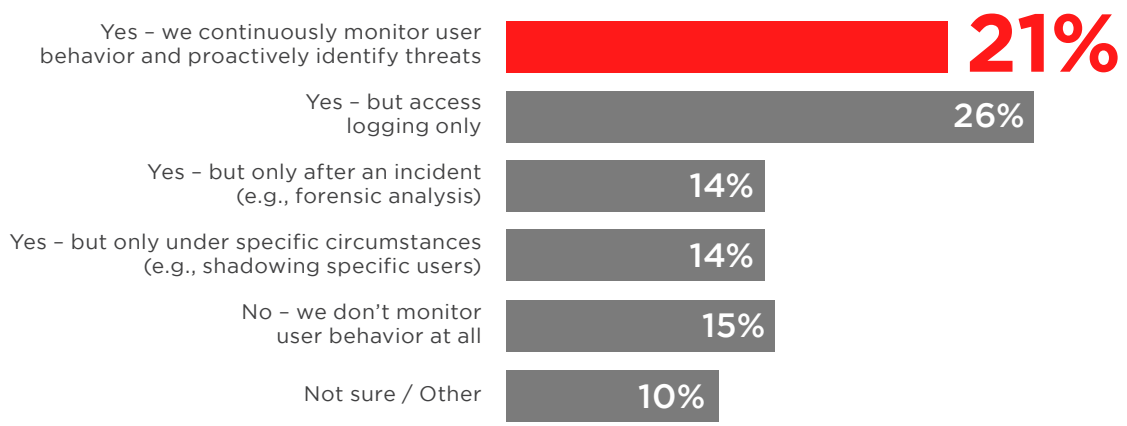


Q: Do you monitor key assets and system resources?

USER BEHAVIOR MONITORING

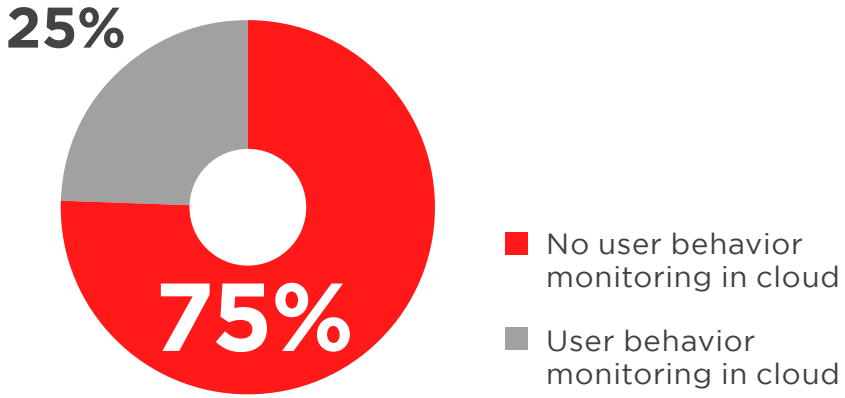
Only 21 percent of organizations continuously monitor user behavior taking place on their network. While most organizations' emphasis is on assets, it is important to monitor both the IT assets and user behavior for more effective protection against insider threats.

Q: Do you monitor user behavior?



USER MONITORING IN THE CLOUD

Only 25% of organizations monitor abnormal user behavior across their cloud footprint.

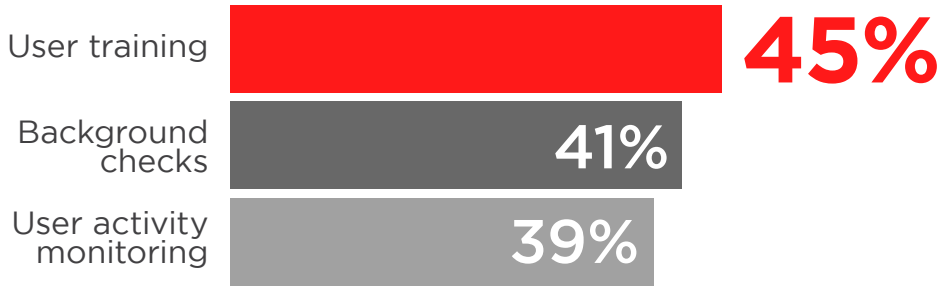


Q: Do you monitor abnormal user behavior across your cloud footprint (SaaS, IaaS, PaaS)?

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?

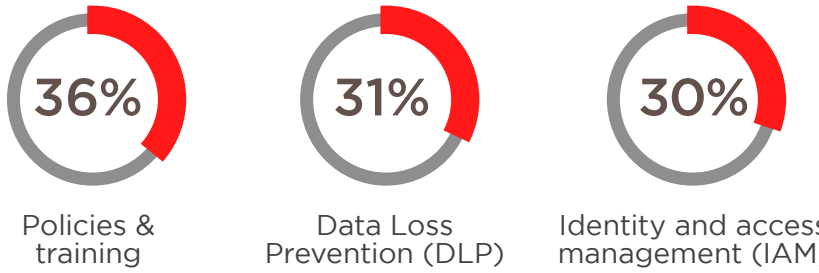


Native security features of underlying OS 28% | Secondary authentication 21% | Password vault 18% | We do not use anything 7% | Not sure / Other 14%

MOST EFFECTIVE TOOLS

Policies and training (36 percent) are considered the most effective tool 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.

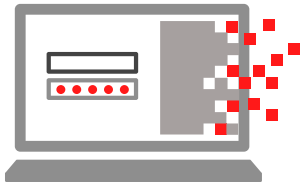
Q: What security tools are most effective in protecting against insider attacks?



User monitoring 28% | User behavior anomaly detection 28% | Encryption of data at rest, in motion, in use 28% | Not sure / Other 8%

FOCUS ON DETERRENCE

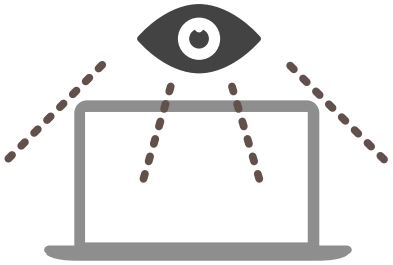
Most organizations place their insider threat management focus and resources on deterrence tactics (63 percent), followed by detection (51 percent) and analysis & forensics (41 percent).



63%

Deterrence

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



51%

Detection

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

41%

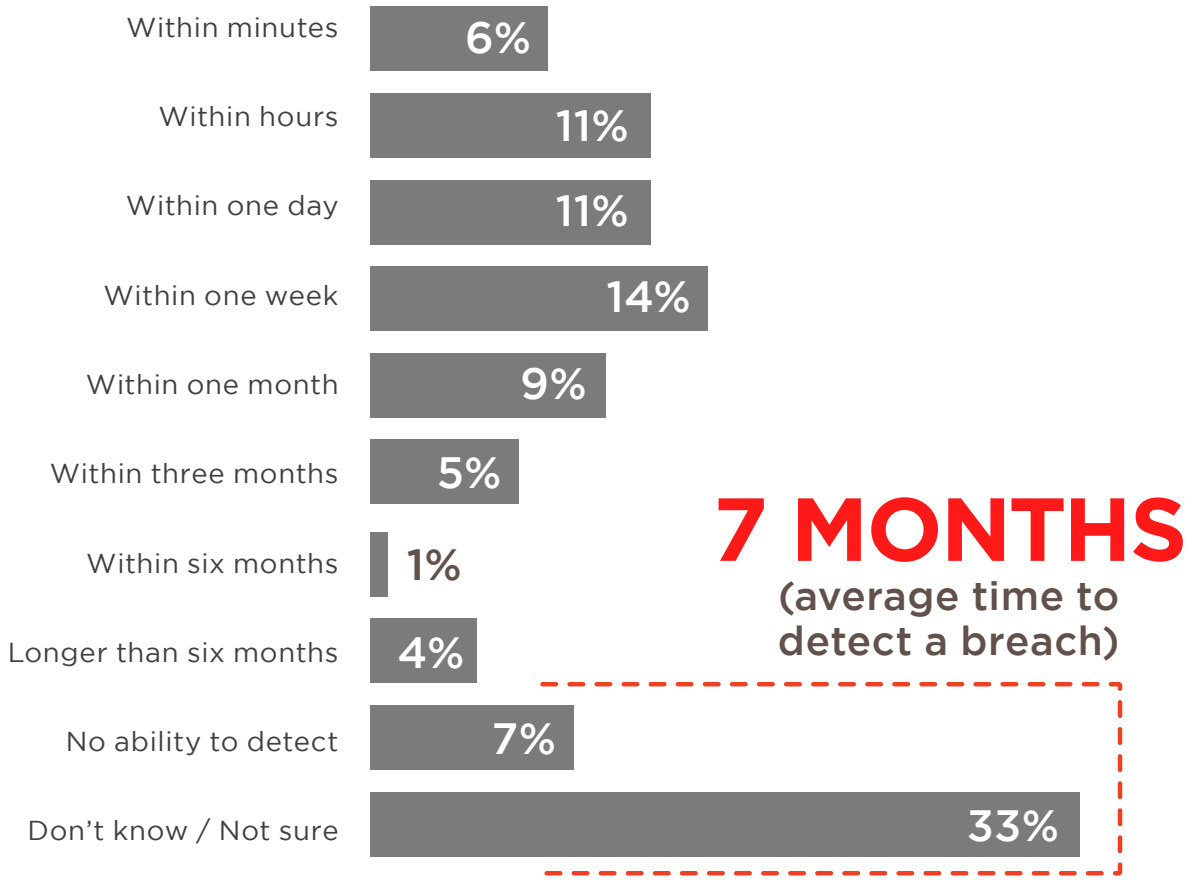
Analysis & Forensics

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

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

SPEED OF DETECTION

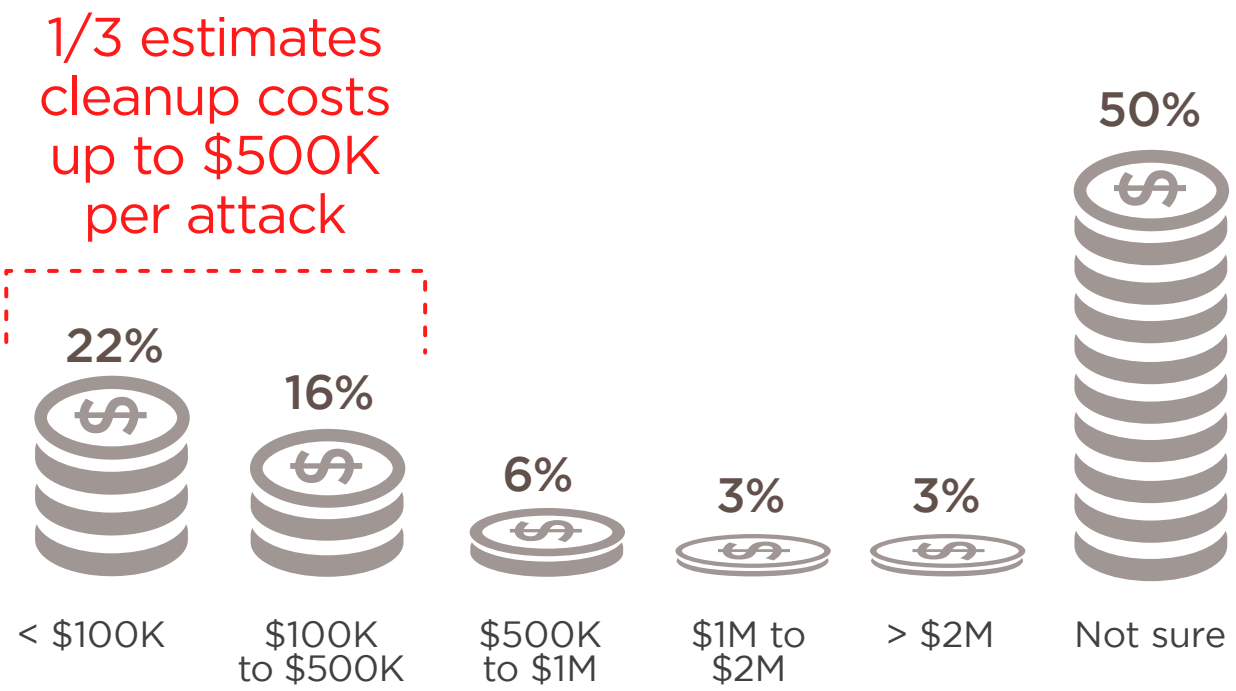
The average data breach lasts 205 days (nearly 7 months), yet of those that can estimate detection time, only 11 percent of organizations believe it would take even 6 months to detect an insider threat.



Q: How long would it typically take your organization to detect 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.



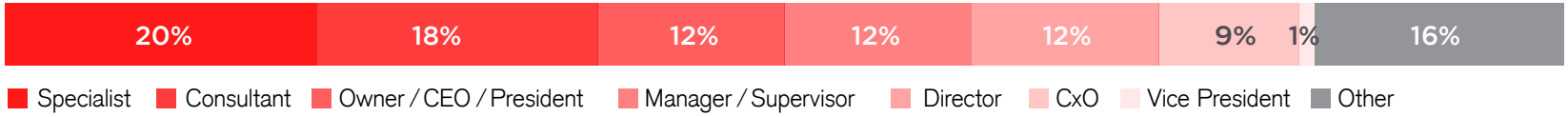
Q: What is the estimated, average cost of remediation after an insider attack?

METHODOLOGY & DEMOGRAPHICS

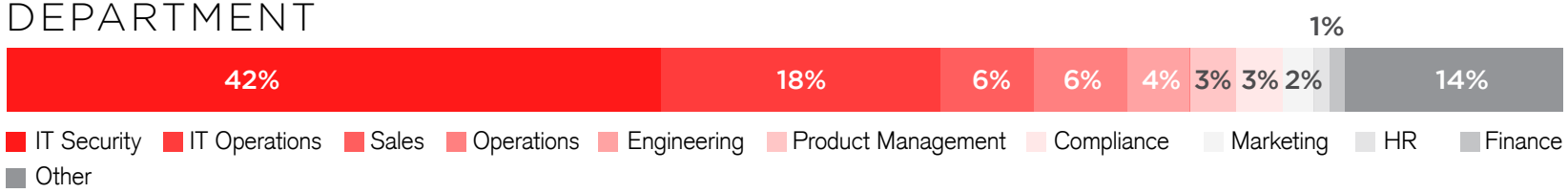
The Insider Threat Spotlight Report is based on the results of a comprehensive survey of over 500 cybersecurity professionals to gain more insight into the state of insider threats and solutions to prevent them.

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.

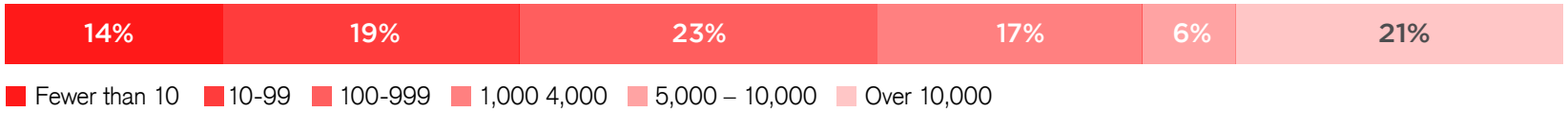
CAREER LEVEL



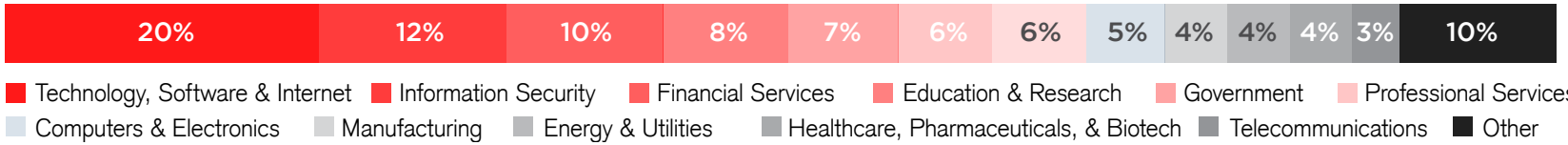
DEPARTMENT



COMPANY SIZE



INDUSTRY



CONTACT US

In a world of applications and mobile devices, IT must secure data that resides on third-party servers and travels over third-party networks to employee-owned mobile devices. Existing security technologies are simply not suited to solving this task, since they are 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.

Bitglass was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. Bitglass is based in Silicon Valley and backed by venture capital from NEA, Norwest and Singtel Innov8.

bitglass

To learn more visit

www.bitglass.com