Insider Attacks

Industry Survey

Haystax TECHNOLOGY
Security Analytics **Redefined**

INSIDER ATTACKS
INDUSTRY SURVEY

TABLE OF CONTENTS

OVERVIEW

Insider threats represent some of the costliest and potentially most dangerous risks facing organizations today. A malicious insider is often too well concealed to be detected using conventional approaches, and many organizations lack the internal tools to monitor risks associated with unwitting or negligent employees.

This report is the result of comprehensive crowd-based research, in partnership with the 300,000+ members of the Information Security Community on LinkedIn and Crowd Research Partners, to gain more insight into the state of insider threats and the available solutions to predict and prevent them.

My thanks to the Information Security Community and Crowd Research Partners for conducting this survey, and especially to everyone who took the time to answer its detailed questions.

The survey makes clear that most security professionals see insider threats as a persistent challenge, but one that competes with other threats for their resources and attention. They believe better organizational policy and more resources are the key to effectively managing the problem, and that increased use of analytics is an effective deterrent against insider threats.

I hope you find this report informative, and useful to your own organization.

Bryan Ware, CEO
Haystax Technology

www.haystax.com

Haystax TECHNOLOGY
Security Analytics Redefined

LinkedIn Group Partner
Information Security

KEY SURVEY FINDINGS

1. Privileged users, such as managers with access to sensitive information, pose the biggest insider threat to organizations (60 percent). This is followed by contractors and consultants (57 percent), and regular employees (51 percent).

2. Fifty-six percent of security professionals say insider threats have become more frequent in the last 12 months. Forty-two percent of organization expect a budget increase over the next year — a strong gain of eight percentage points from the previous year.

3. Over 75 percent of organizations estimate insider breach remediation costs could reach $500,000. Twenty-five percent believe the cost exceeds $500,000 and can reach in the millions.

4. Seventy-four percent of organizations feel vulnerable to insider threats — a dramatic seven percentage point increase over last year's survey. However, less than half of all organizations (42 percent) have the appropriate controls in place to prevent an insider attack.

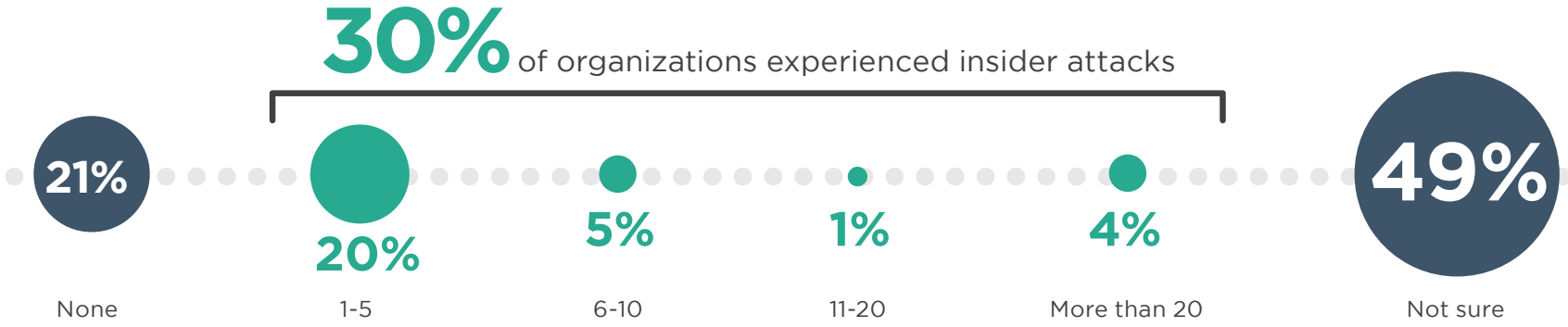
5. Fifty-six percent of organizations leverage insider threat analytics - up 20 percent compared to last year.

INSIDER ATTACKS

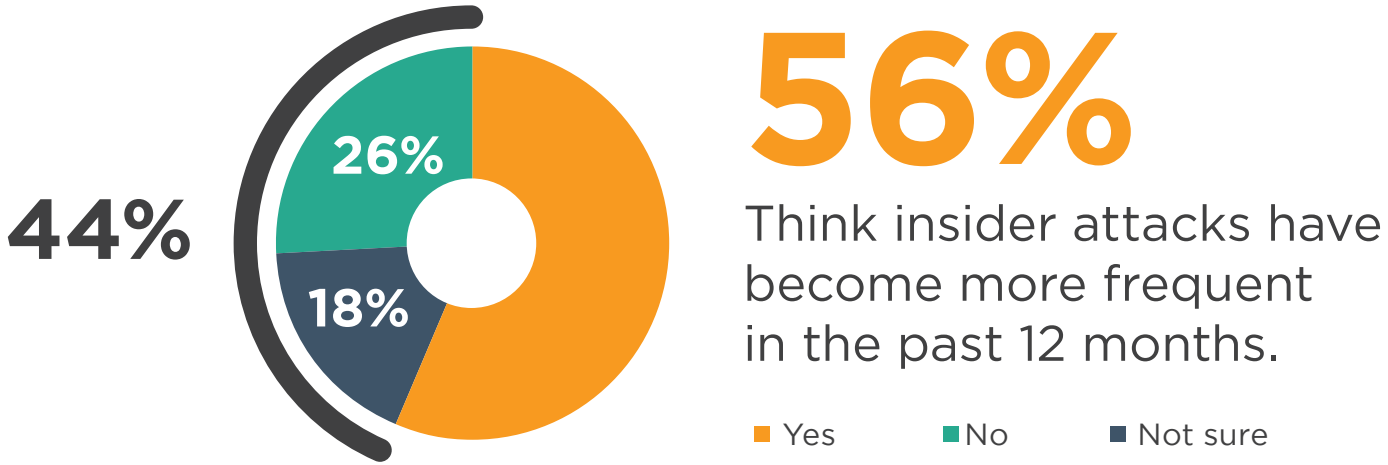
THE RISE OF INSIDER ATTACKS

Almost half of respondents have no idea if their organization experienced an insider attack in the last 12 months (49 percent). However, more people feel that insider attacks have become more frequent in the last 12 months (56 percent). Eighteen percent said they are seeing fewer breaches while 26 percent of respondents were not sure.

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



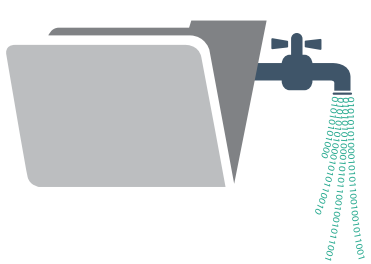
Q: Do you think insider attacks have generally become more frequent over the last 12 months?



TOP INSIDER THREATS

Malicious data breaches (61%) are among the critical insider threats organizations are most concerned about (in addition to negligent data breaches and inadvertent data breaches). Because malicious threats are premeditated, it becomes vitally important to predict and preempt these threats where possible.

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



71%

Inadvertent data breach/leak

(e.g., careless user causing accidental breach)

68%

Negligent data breach

(e.g., user willfully ignoring policy, but not malicious)

61%

Malicious data breach

(e.g., user willfully causing harm)

RISKY USERS

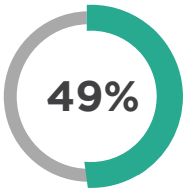
In this year's survey, privileged IT users, such as administrators with access to sensitive information, pose the biggest insider threat (60 percent). This is followed by contractors and consultants (57 percent), and regular employees (51 percent).

Q: What user groups pose the largest security risk to organizations?

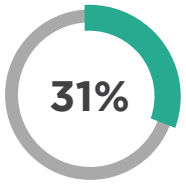
60%
Privileged IT Users / Admins

57%
Contractors/Consultants Temporary Workers

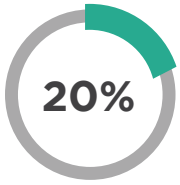
51%
Regular Employees



Privileged business users

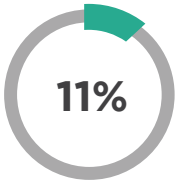


Executive managers

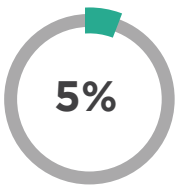


Business partners

Other IT staff



Customers



Not sure/ Other

WHAT MOTIVATES INSIDER ATTACKS

Monetizing sensitive data (55 percent), fraud (51 percent) and sabotage (42 percent) are the top motivations for malicious insider threats that companies are most concerned about. Espionage is the least concern, as highlighted by respondents (38 percent).

Q: What motivations for malicious insider threats are you most concerned about?

55%
Monetizing sensitive data

51%
Fraud

42%
Sabotage

39% IP theft

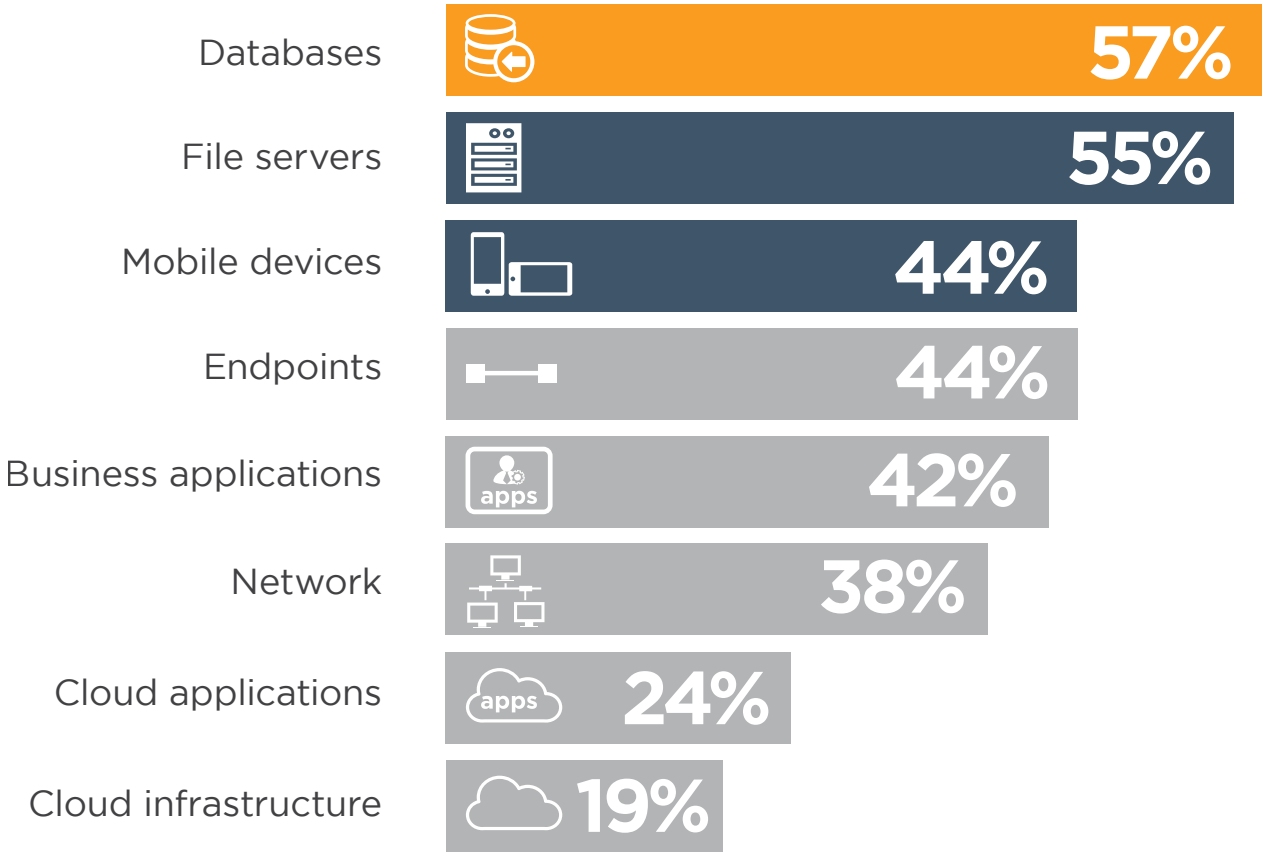
38% Espionage

10% Not sure/Other

IT ASSETS AT RISK

Given the amount of sensitive information that resides in databases, it is no surprise that similar to last year, 57 percent of companies named databases as the most vulnerable asset to an insider attack. File servers (55 percent) and mobile devices (44 percent) were named as the second and third assets that are most vulnerable. Cloud infrastructure was the least vulnerable (19 percent).

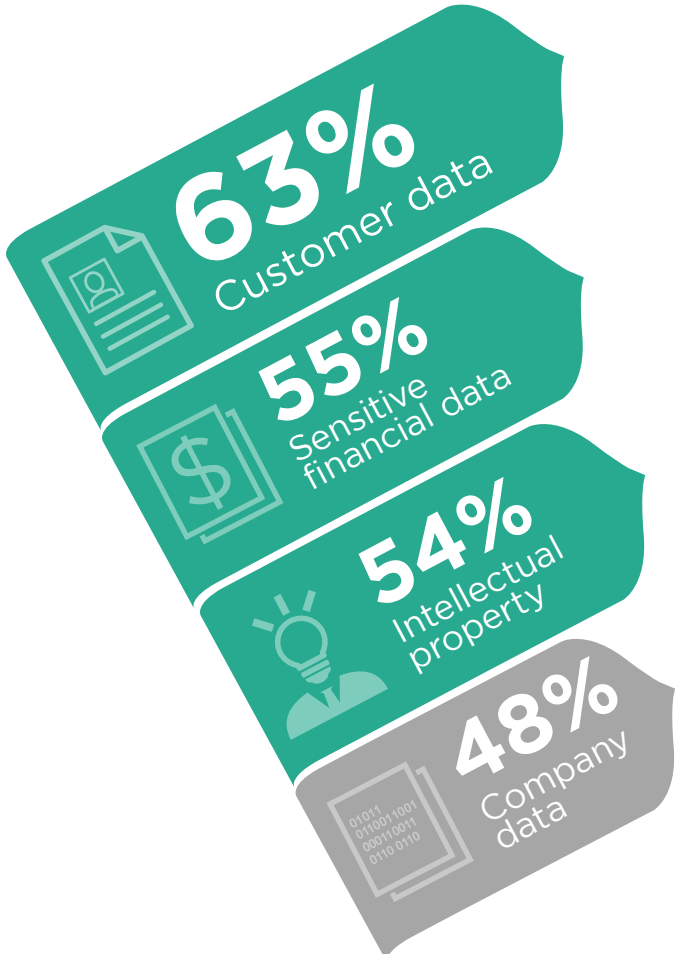
Q: What IT assets are most vulnerable to insider attacks?



DATA MOST VULNERABLE TO INSIDER ATTACKS

As expected, due to its value, customer data is most vulnerable to insider attacks (63 percent) again this year. Financial data (55 percent) and intellectual property (54 percent) marginally switch spots.

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



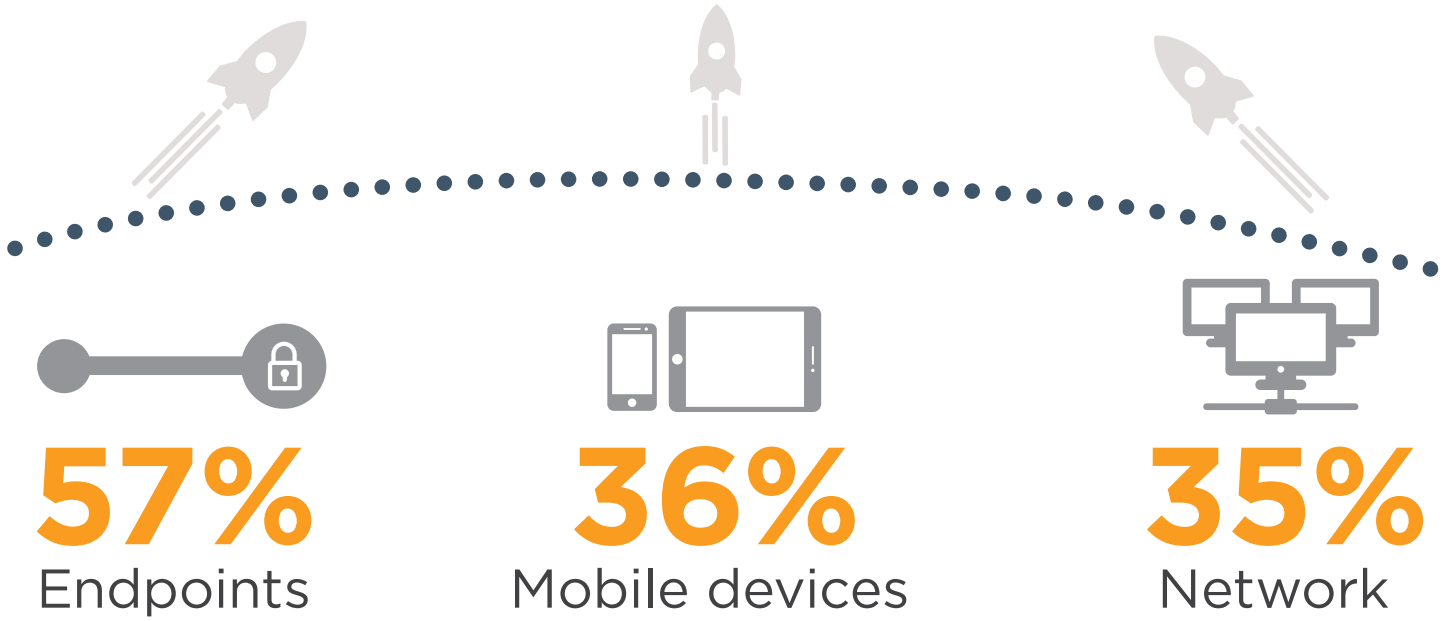
MOST VULNERABLE DATA TO INSIDER ATTACKS

Not sure / Other 6%

LAUNCH POINTS FOR INSIDER ATTACKS

Endpoints (57 percent) by far are the most common assets used to launch an insider attack. Cloud infrastructure (20 percent) is the least likely place people use to launch an attack.

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



57%
Endpoints

36%
Mobile devices

35%
Network

File servers 31% | Business applications 29% | Databases 27% | Cloud infrastructure or applications 20% | Not sure / Other 13%

WHY INSIDER ATTACKS ARE INCREASING

Insufficient data protection strategies and solutions (57 percent) and the proliferation of sensitive data moving outside the firewall on mobile devices (54 percent) are again named as reasons for why insider threats are on the rise.

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

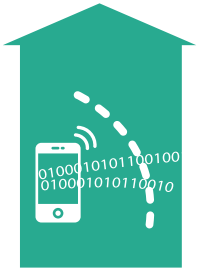
57%

Insufficient data protection strategies or solutions

54%

Increasing number of devices with access to sensitive data

48%



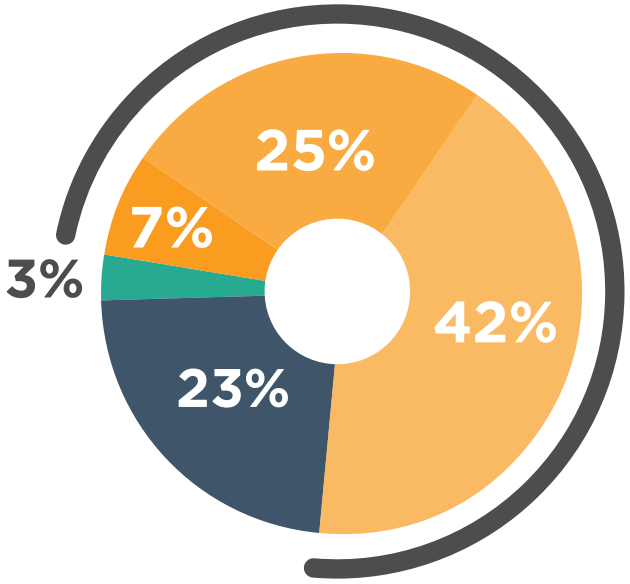
Data increasingly leaving the network perimeter via mobile devices and Web access

More employees, contractors, partners accessing the network 45% | Increasing amount of sensitive data 37% | Increased public knowledge or visibility of insider threats that were previously undisclosed 29 % | Technology is becoming more complex 27% | Increasing use of cloud apps and infrastructure 27% | Not sure / Other 10%

COMPANY VULNERABILITY

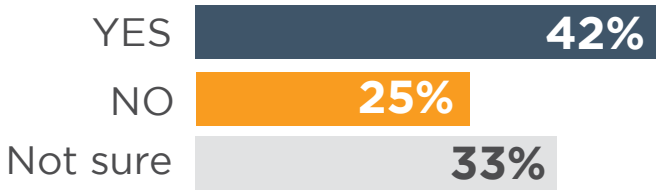
Seventy-four percent of organizations feel vulnerable to insider threats - a dramatic seven percentage point increase over last year's survey. Even though 42 percent of companies feel they have appropriate controls to prevent an insider attack, only three percent of companies feel they are not at all vulnerable to an insider attack.

Q: How vulnerable is your organization to insider threats?



74%
feel vulnerable
to insider threats

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



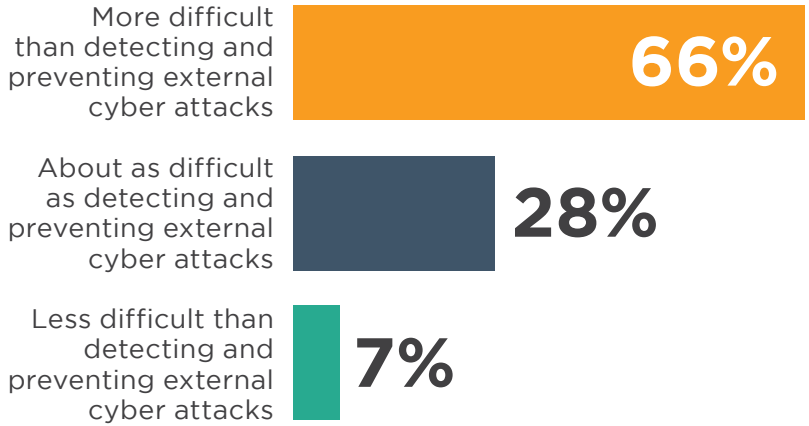
Q: Does your organization have the appropriate controls to prevent an insider attack?

THREAT DETECTION

INTERNAL VERSUS EXTERNAL ATTACKS

Similar to our previous survey, the majority of respondents (66 percent) have a harder time detecting and preventing an insider attack versus an external cyber attack.

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 (67 percent), the increased use of cloud based applications (53 percent), and the rise in the amount of data that is leaving the protected network perimeter (46 percent).

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

67% Insiders already have credentialed access to the network and services

53% Increased use of applications that can leak data (e.g., Web email, DropBox, social media)

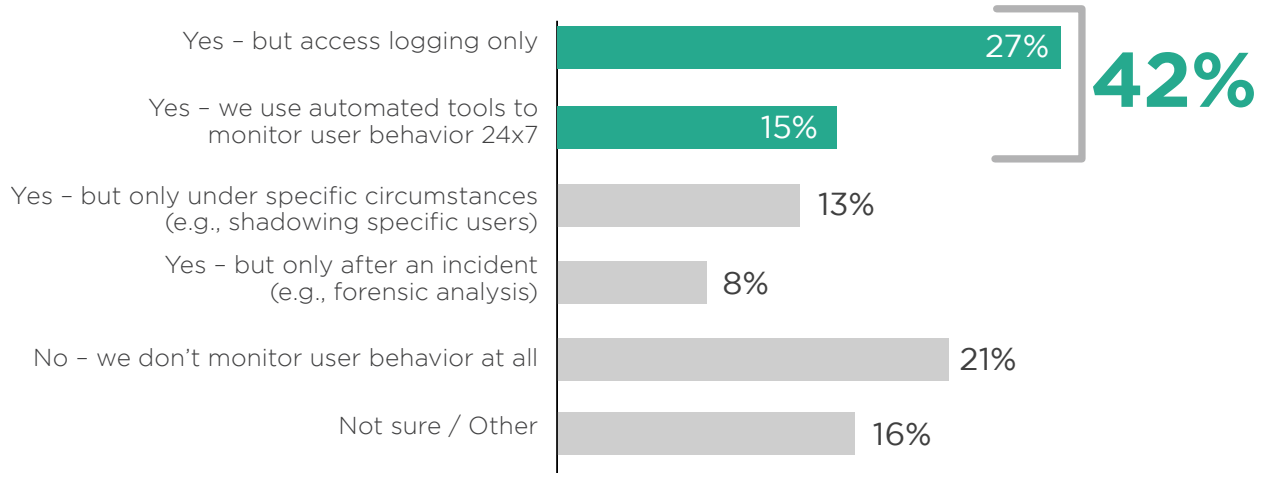
46% Increased amount of data that leaves protected boundary / perimeter

More end user devices capable of theft 33% | Difficulty in detecting rogue devices introduced into the network or systems 32% | Absence of an Information Security Governance Program 31% | Insiders are more sophisticated 28% | Migration of sensitive data to the cloud along with adoption of cloud apps 24% | Not sure / Other 10%

DATA ACCESS AND USER BEHAVIOR MONITORING

Q: Do you monitor user behavior?

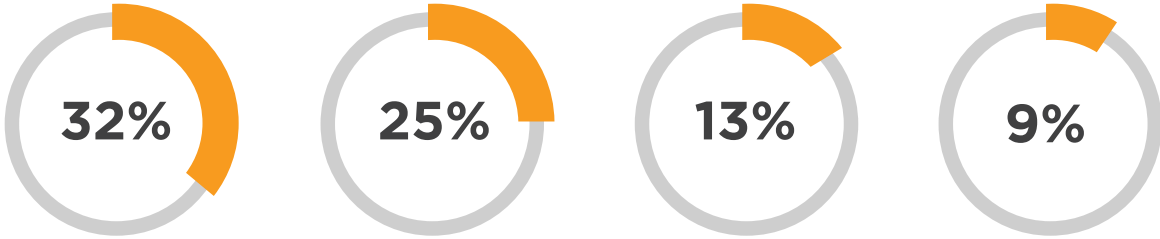
Most organizations monitor their user behavior (42 percent). Twenty one percent do not monitor user behavior.



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

Again this year, most organizations (49 percent) rely on server logs to review user behavior. Only 25 percent have deployed dedicated user activity monitoring solutions. Thirteen percent of respondents have no visibility at all.

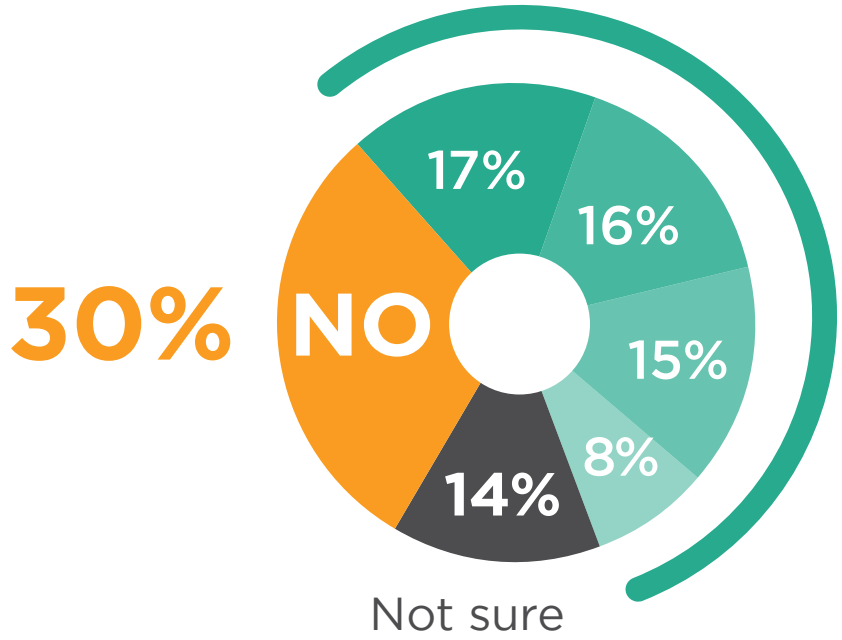
49%
Server Logs



INSIDER THREAT ANALYTICS

The number of organizations that use insider threat analytics is up 20 percent compared to last year. Of the 56 percent of organizations that are using some type of analytics, only eight percent use predictive analytics.

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



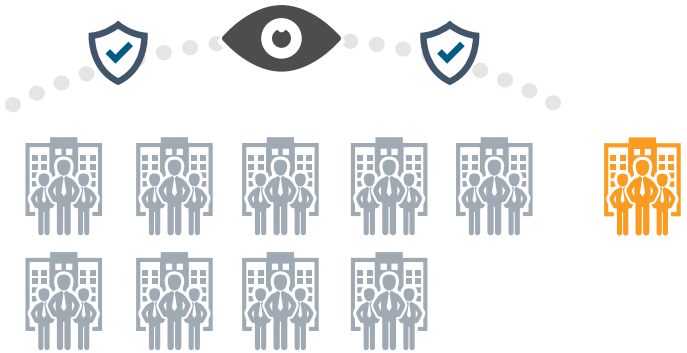
56%
leverage analytics

- Yes – activity management and summary reports
- Yes – data access and movement analytics
- Yes - user behavior analytics
- Yes - predictive analytics

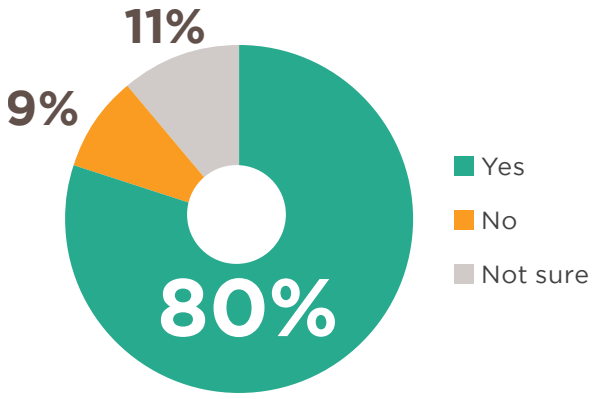
SECURITY TOOLS AND PROCESSES

CONTROLS TO COMBAT INSIDER THREATS

Organizations that proactively implement specific controls to prevent cyber attacks as part of their risk management program outnumber those that do not almost 10:1.



Q: Do you include cyber attacks in your risk management framework?



The controls that these organizations utilize include security perimeter defense tools (76 percent), database and file monitoring tools (67 percent) and security events dashboards (58 percent).

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

76% Security perimeter defense tools

67% Database and file monitoring tools

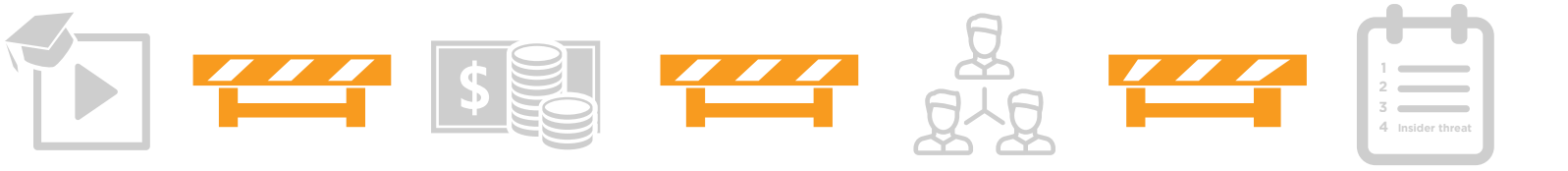
58% Security events dashboard

Access violations Key Risk Indicators by database or system 55% | Security event remediation processes 55% | Data loss and corruption Key Risk Indicators 52% | System of Record monitoring 46% | System down time Key Risk Indicators 24% | Not sure / Other 13%

BARRIERS TO BETTER INSIDER THREAT MANAGEMENT

Similar to our last survey, the biggest perceived barrier to better insider threat management is organizational, starting with a lack of training and expertise (60 percent). Rounding out the top three are insufficient budgets (50 percent) and lack of collaboration between departments (48 percent). Notably, lack of collaboration is the barrier with the highest gain since the previous survey, moving up 10 percentage points.

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



#1

60%

Lack of training & expertise

#2

50%

Lack of budget

#3

48%

Lack of collaboration between separate departments

10% p.p. from last year

#4

43%

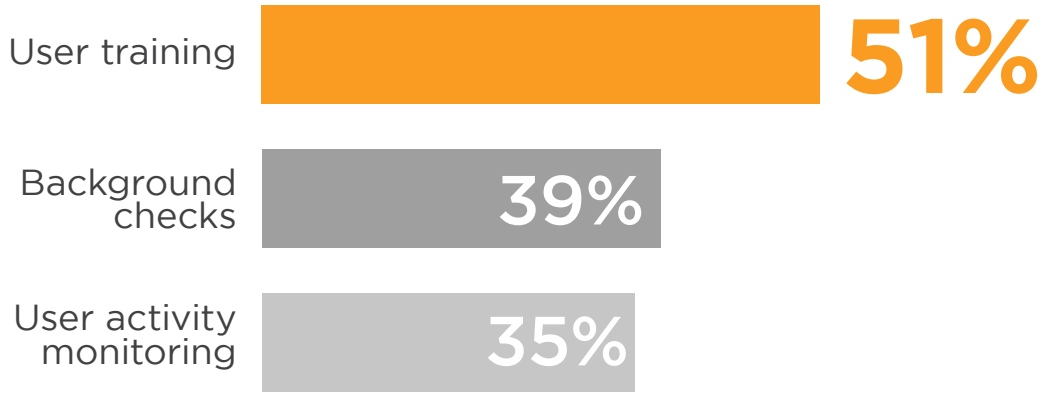
Not a priority

Lack of staff 35% | Lack of suitable technology 28% | Not sure / Other 11%

INSIDER THREAT APPROACH

User training (51 percent), background checks (39 percent) and monitoring user activity (35 percent) top the list of how organizations overcome insider threats.

Q: How does your organization combat insider threats today?



Information Security Governance Program 34% | Database Activity Monitoring 24% | Native security features of underlying OS 22% | Secondary authentication 21% | Specialized 3rd party applications and devices 15% | Custom tools and applications developed in house 11% | Managed Security Service provider 8% | We do not use anything 7% | Not sure/Other 15%

FOCUS ON DETERRENCE

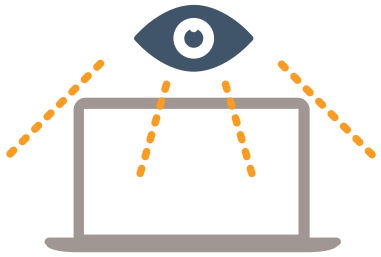
Most organizations continue to place their insider threat management focus and resources on deterrence tactics (61 percent), followed by detection (49 percent) and analysis and forensics (35 percent).

Despite the continued investments in deterrence and detection, insider threats are still on the rise.

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

61%

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



49%

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

35%

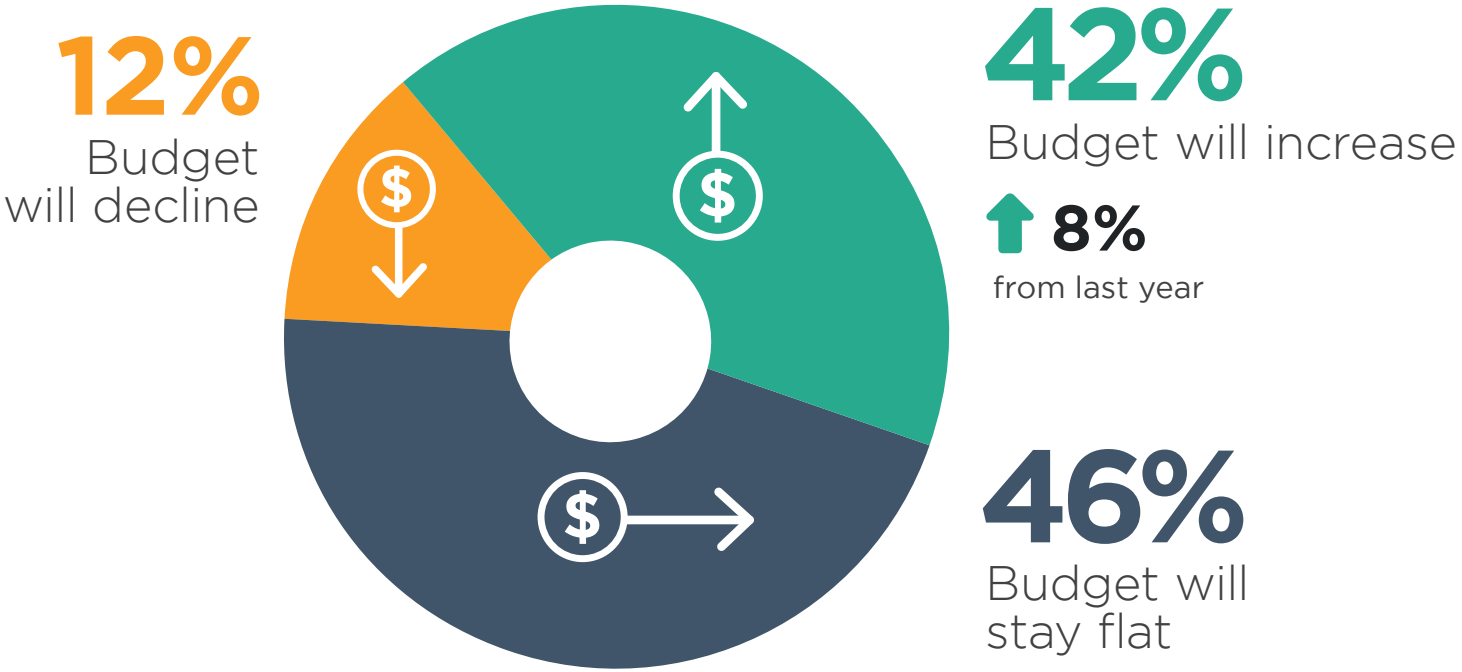
Analysis & Forensics
(e.g., SIEM, etc.)

Deception (e.g., honeypots, etc) 9% | None 7% | Not sure / Other 3%

BUDGET TRENDS

With insider attacks on the rise, 42 percent of organizations expect a security budget increase over the next 12 months. This represents a strong gain of eight percentage points from the previous year.

Q: How is your security budget changing over the next 12 months?



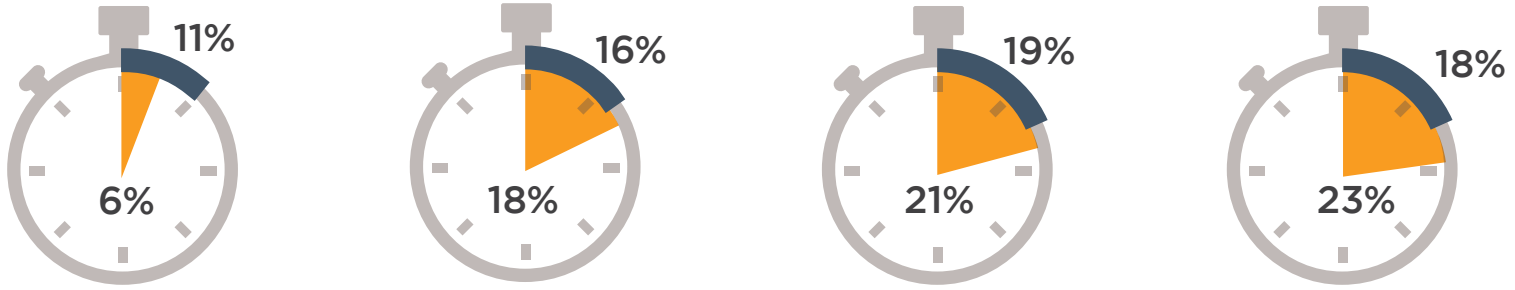
RECOVERY AND REMEDIATION

SPEED OF DETECTION & RECOVERY

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

Year over year companies are getting better at both detecting and recovering from insider attacks. This year most IT professionals feel their organization could detect an insider attack within one day, up six percent year over year.

Within one month 9% | Within three months 7% | Longer than three months 7% | No ability to detect 13%



Only **18%** within hours.

68% organizations recover from an insider attack within a week or less

Detection time Recovery time

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

Organizations are getting more confident of their ability to recover from an attack. Sixty-eight percent of organizations feel they could recover from an attack within a week - up over 20 percent from last year's survey.

Within one month 15% | Within three months 5% | Longer than three months 9% | No ability to recover 3%

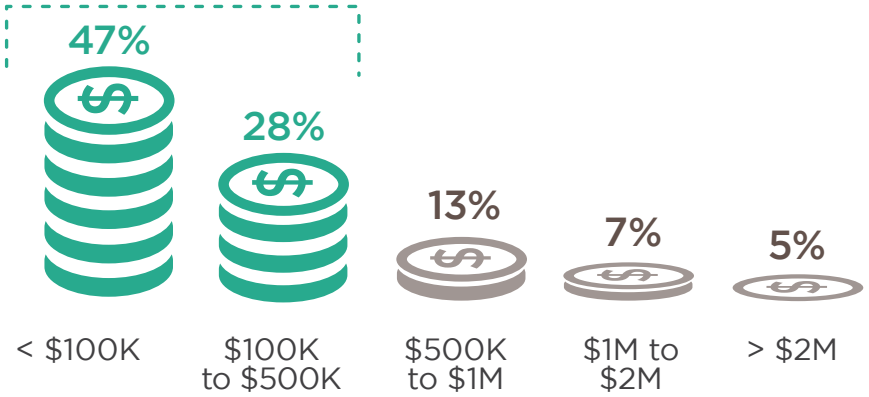
COST OF REMEDIATION

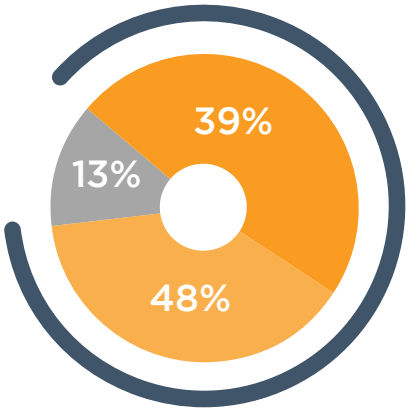
Q: What is the estimated, average cost of remediation after an insider attack?

Insider attacks can be costly to organizations, from immediate economic impact to long term damages in reputation and trust. This year, successful attacks are costing organizations even more money and the damage is getting more difficult to detect.

Over 75 percent of organizations estimate costs could reach a half a million dollars. Of those that are able to estimate the average cost of remediation, 25 percent believe the cost exceeds $500,000 and can reach in the millions.

75%
estimates cleanup costs up to $500K





87%
Difficult to estimate damages

- Very difficult
- Moderately difficult
- Not at all difficult

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

Eighty seven percent of organizations find it difficult to determine the actual damage of an insider threat. This is 20 percent more than last year.

DEMOGRAPHICS

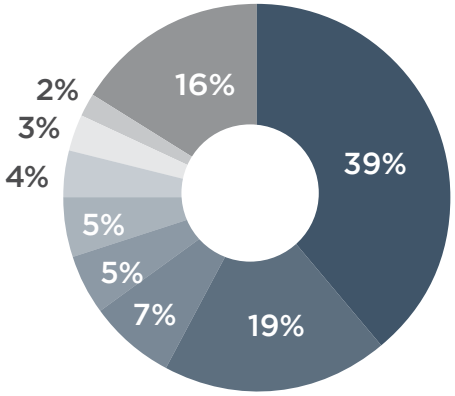
DEMOGRAPHICS

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

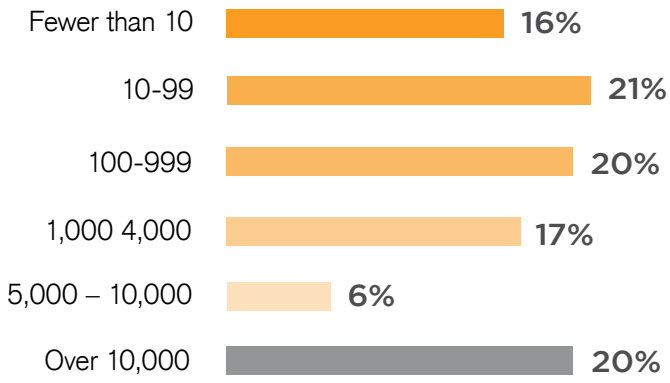
Specialist | Manager / Supervisor | Consultant | Owner / CEO / President | Director | CTO, CIO, CISCO, CMO, CFO, COO | Vice President | Other

DEPARTMENT



IT Security | IT Operations | Operations | Sales | Engineering | Compliance | Product Management | Marketing | Other

COMPANY SIZE



INDUSTRY

Technology, Software & Internet | Information Security | Financial Services | Government | Professional Services | Computers & Electronics | Manufacturing | Telecommunications | Healthcare, Pharmaceuticals, & Biotech | Education & Research | Energy & Utilities | Manufacturing | Transportation & Logistics | Other

SECURITY ANALYTICS FOR INSIDER THREAT — REDEFINED

BARRIERS TO IMPROVING INSIDER THREAT

Problem

- Lack of collaboration among departments is cited by almost half of survey respondents as the biggest barrier to success in mitigating insider threats — a 10-percent jump from last year. Another obstacle is lack of internal threat expertise.
- An equally noteworthy finding is how little organizations know about the extent of their own insider threats, despite a steady drumbeat of news about such incidents. And a surprising 43 percent still say that insider threats are “not a priority.”

Solution

- At the core of every effective insider threat program is a set of clearly defined management controls and workforce policies. But technology also plays a critical role in overcoming many barriers to program success.
- Haystax Technology’s Constellation for Insider Threat solution zeroes in on the highest-priority risks by:
  - ✔ Providing a single-screen information-sharing environment that is customizable and allows authorized users in all departments — not just the network security team — to see and act on the emerging threats that matter.
  - ✔ Running real-time behavioral, activity and event data against a fully developed risk model with over 700 key indicators to evaluate trustworthiness, overcoming any lack of internal expertise on insider threats.
  - ✔ Displaying aggregated risk results on a secure dashboard that highlights patterns and negative trends across the organization as well as a graph of all individuals in the organization, ranked from highest- to lowest-risk.

Haystax TECHNOLOGY
Security Analytics Redefined

FINANCIAL CONSEQUENCES OF INSIDER ATTACKS

Problem

- A trusted insider can inflict not just reputational or physical damage, but financial harm as well. Over 75 percent of survey respondents believe that the costs of remediating an insider attack could reach $500,000, with the other 25 percent anticipating costs in excess of $500,000 and possibly in the millions of dollars.

- Prevention can be costly, too. Analysts are already overwhelmed by the volume and velocity of threat data, and by the number of personnel who need to be monitored. Many companies hire more analysts or double-down on data-driven solutions that only result in a vicious cycle of more alerts — and then more analysts. And 50 percent of respondents say they lack the budgets to tackle even current insider threats.

Solution

- Constellation for Insider Threat prioritizes all types of adverse insider behavior early — helping avert major financial impacts. Using a 'whole-person' model, it can pinpoint malicious, negligent and inadvertent behaviors. Potential threat actors detectable by the system include:
  - The money-driven senior manager who steals sensitive documents and proprietary data weeks before leaving for a competitor.
  - The disgruntled employee who reveals an intense dislike of management on a public forum, as a precursor to more malicious activity that can damage revenue sources and profitability, or even physical assets and personnel.
  - The careless contractor who clicks unwittingly on a phishing email exposing the organization to data or monetary theft by outsiders.

- By codifying diverse expertise into the model, Constellation operates like a team of insider threat experts — but at a scale, velocity and volume that no human analyst could long endure. The system frees analysts to identify their highest priority threats while filtering out distracting false positives and useless anomaly alerts. It saves costs by specifying exactly the types of data needed for the threat model while ignoring data that is not useful, and also by identifying surrogate data that may be relatively cheaper to obtain.

Haystax TECHNOLOGY
Security Analytics Redefined

THE PREDICTIVE POWER OF PRIORITIZATION

Problem

- Three-quarters of organizations surveyed feel vulnerable to threats from within, a sizable increase from last year. While 20 percent more of them are leveraging analytics than last year (with over half now deploying some kind of technology solution), only eight percent deploy any kind of predictive analytics technology. Most of the threat detection, therefore, is forensic in nature rather than anticipatory.

- Network monitoring tools are very popular, but they merely send out a blizzard of alerts on anomalous activities without any context.

Solution

- What is needed is a comprehensive 'whole-person' view of behavior that accounts for major life events — along with related indicators such as poor performance reviews or financial difficulties — to indicate the presence of a potential threat. This more holistic approach to analytics can highlight negative-trending behaviors many months in advance of an adverse event.

- By using Constellation, organizations move to a more dynamic and predictive risk posture, making quicker decisions and speeding remediation for more effective protection of their critical systems, data, facilities and people. We start with a model of the insider problem, built with inputs from a diverse array of domain experts specializing in personnel issues, network security, financial fraud, IP theft and other areas. Data is then applied to the model and processed using other AI techniques to form a baseline view of each individual that can be continuously updated as new data comes in.

- By adopting this focus on the whole person with related activity in context, Constellation drastically reduces false positives and pinpoints the highest-risk individuals for analysts to investigate. And it does so much sooner than most conventional data analytics solutions.

Haystax TECHNOLOGY
Security Analytics Redefined

We've hit upon a novel approach to tackle the insider threat problem, redefining security analytics. Instead of starting with a massive pool of technical indicators and then mining this data for usable threat intelligence, we've encoded insider threat subject matter expertise into a model that applies multiple artificial intelligence techniques to identify relevant data and evaluate human behaviors. **Our advanced analytics score the highest-priority threat signals based on an organization's unique issues of concern, and in turn deliver dependable trustworthiness scores.** Our model-first approach to security analytics has been proven in operational settings to drastically reduce false positives, and identified as "pioneering technology" by respected industry analysts.

Learn more at: **www.haystax.com**

Haystax
TECHNOLOGY
Security Analytics **Redefined**