# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Key Survey Findings</td>
<td>4</td>
</tr>
<tr>
<td>Insider Threat Detection</td>
<td>5</td>
</tr>
<tr>
<td>Insider Threat Program</td>
<td>16</td>
</tr>
<tr>
<td>Sponsor Overview</td>
<td>24</td>
</tr>
<tr>
<td>Methodology &amp; Demographics</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>37</td>
</tr>
</tbody>
</table>
INTRODUCTION

Today’s most damaging security threats are not originating from malicious outsiders or malware but from trusted insiders - both malicious insiders and negligent insiders. This survey is designed to uncover the latest trends and challenges regarding insider threats as well as solutions to prevent or mitigate insider attacks.

Our 400,000 member online community, Cybersecurity Insiders, in partnership with the Information Security Community on LinkedIn, asked Crowd Research Partners to conduct an in-depth study of cybersecurity professionals to gather fresh insights, reveal the latest trends, and provide actionable guidance on addressing insider threats.

The resulting Insider Threat Report is the most comprehensive research on the topic to date, revealing how IT and security professionals are dealing with risky insiders and how organizations are preparing to better protect their critical data and IT infrastructure.

We would like to thank Interset for supporting this research.

In addition, we want to thank all survey participants who provided their time and input in support of this study.

We hope you will enjoy reading this report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Holger.Schulze@Cybersecurity-Insiders.com
KEY SURVEY FINDINGS

1. Ninety percent of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).

2. A 53% majority have confirmed insider attacks against their organization in the previous 12 months (typically less than five attacks). Twenty-seven percent of organizations say insider attacks have become more frequent.

3. Organizations are shifting their focus on detection of insider threats (64%), followed by deterrence methods (58%), and analysis and post breach forensics (49%). The use of user behavior monitoring is accelerating; 94% of organizations deploy some method of monitoring users and 93% monitor access to sensitive data.

4. The most popular technologies to deter insider threats are Data Loss Prevention (DLP), encryption, and identity and access management solutions. To better detect active insider threats, companies deploy Intrusion Detection Prevention Solutions (IDPS), log management and SIEM platforms.

5. The vast majority (86%) of organizations already have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.
INSIDER THREAT
Too often, people associate the term “Insider Threats” in cybersecurity with malicious employees intending to directly harm the company through theft or sabotage. In truth, negligent employees or contractors unintentionally cause an equally high number of security breaches and leaks by accident.

In this year’s survey, companies are equally worried about accidental/unintentional data breaches (51%) through user carelessness, negligence or compromised credentials as they are from deliberate malicious insiders (47%).

What type of insider threats are you most concerned about?

- Malicious/deliberate insider (e.g. willfully causing harm) - 47%
- Accidental/unintentional insider (e.g. carelessness, negligence or compromised credentials) - 51%
- Not sure - 2%
Security professionals have a unique responsibility to detect and respond to cyber attacks. This job becomes increasingly more challenging when threats come from within the organization from trusted and authorized users. It is often difficult to determine when users are simply doing their job function or actually doing something illegal or unethical.

The survey indicated both regular employees (56%) and privileged IT users (55%) pose the biggest insider security risk to organizations, followed by contractors (42%).

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

- Regular employees: 56%
- Privileged IT users/admins: 55%
- Contractors/service providers/temporary workers: 42%
- Customers/clients: 22%
- None: 2%
- Not sure/other: 6%

*Multi-response questions do not add up to 100%
Data is no longer just an IT asset; it’s a core strategic asset and some types of data are more valuable than others. Confidential business information, which encompasses company financials along with customer and employee data, is a highly strategic asset and equally a high-value target. Again this year, confidential business information (57%) takes the top spot as most vulnerable to insider attacks, followed by privileged account information (52%), and sensitive personal information (49%).

What type(s) of data are most vulnerable to insider attacks?

- **57%** Confidential business information
  - (Financials, customer data, employee data)
- **52%** Privileged account information
  - (Credentials, passwords, etc.)
- **49%** Sensitive personal information
  - (PII/PHI)
- **32%** Intellectual property
  - (Trade secrets, research product designs)
- **31%** Employee data
  - (HR)
- **27%** Operational/infrastructure data
  - (Network, infrastructure controls)
- Not sure/other 1%
Cybercriminals see a greater opportunity in targeting where corporate data is located in volume. Databases (50%) and corporate file servers (46%) pose the highest risk. In this year’s survey, mobile devices are perceived as a lesser target and least vulnerable (25%).

What IT assets are most vulnerable to insider attacks?

- **Databases** 50%
- **File servers** 46%
- **Cloud applications** 39%
- **Cloud infrastructure** 36%
- **Endpoints** 33%
- **Network** 32%
- **Active directory** 30%
- **Business applications** 29%
- **Mobile devices** 25%
ACCIDENTAL INSIDERS

The most common culprit of insider threat is accidental exposure by employees. Cybersecurity experts view phishing attempts (67%) as the biggest vulnerability for accidental insider threats. Phishing attacks trick employees into sharing sensitive company information by posing as a legitimate business or trusted contact and they often contain malware attachments or hyperlinks to compromised websites.

What do you see as the biggest enabler of accidental insider threats?

- Phishing attempts: 67%
- Weak/reused passwords: 56%
- Unsecured WiFi networks: 32%
- Unlocked devices: 44%
- Bad password sharing practice: 44%
The survey reveals cybersecurity professionals perceive the following three responses as the top enablers for insider attacks: too many users with excessive access privileges (37%), increasing number of devices with access to sensitive data (36%), and technology becoming more complex (35%).
We asked cybersecurity professionals to assess their organization’s vulnerability to insider threats. Ninety percent of organizations feel vulnerable. Only six percent say they are not at all vulnerable to an insider attack.

How vulnerable is your organization to insider threats?

90% feel vulnerable to insider threats

Extremely vulnerable: 28%
Very vulnerable: 13%
Moderately vulnerable: 43%
Slightly vulnerable: 6%
Not at all vulnerable: 4%
Cannot disclose/not sure: 6%
Looking back, 33% of organizations experienced five or less insider attacks in the last 12 months, while 20% experienced six or more attacks.

Twenty-seven percent say their organizations have experienced more frequent insider threats in the last 12 months. Nearly half of the security professionals (46%) polled believe the frequency of insider attacks has remained at the same levels while 21% say the frequency has decreased.

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

- 33%: 1-5
- 8%: 6-10
- 8%: 11-20
- 4%: More than 20
- None/not sure 47%

**Have insider attacks against your organization become more or less frequent over the last 12 months?**

- More frequent 27%
- Same 46%
- Less frequent 21%
- Not sure 6%
Two-thirds of organizations (66%) consider malicious insider attacks or accidental breaches more likely than external attacks.

Forty-four percent of organizations perceive all (malicious, external and accidental) attacks as equally damaging, while 31% believe malicious/deliberate insider attacks are more damaging than external attacks (14%). The low weight placed on accidental insider breaches (11%) seems too low, perhaps underestimating the potential damages.
While true cost of a major security incident are not easy to determine, the most common estimate is a range of $100,000 to $500,000 per successful insider attack (27%). Twenty-four percent expect damages to exceed $500,000.

What would you estimate is the potential cost/loss of an insider attack in US Dollars?

- 16% < $100K
- 12% $100K to $500K
- 9% $500K to $1M
- 3% $1M to $2M
- 10% > $2M
- 23% No value of loss
- 27% Not sure
DETECTION
Insider data 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. Fifteen percent of organizations said they do not have adequate controls in place.

The good news is security practitioners realize that advanced detection and prevention are key; the majority of respondents (73%) have implemented security controls and policies to deal with impeding threats.

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

- **YES** 73%
- **NO** 15%
- Not sure 12%
An organization’s control framework is the set of safeguards, separation of duties and recommended actions for IT professionals to use to minimize security risks and exposure. We asked security practitioners what security controls they use to deal with inevitable insider threats.

Data Loss Prevention (DLP) (60%) and encryption of data (at rest, in motion, in use) (60%) were both tied for the top spot. Respondents said Identity and Access Management (IAM) (56%), and endpoint and mobile security (50%) were also deployed to avert insider attacks.

What controls do you have in place to deter insider threats?

- **60%**
  - Data Loss Prevention (DLP)

- **60%**
  - Encryption of data (at rest, in motion, in use)

- **56%**
  - Identity and Access Management (IAM)

- **50%**
  - Endpoint and mobile security

- **29%**
  - Cloud Access Security Broker (CASB)

Enterprise Digital Rights Management Solutions (E-DRM) 29% | Privileged account vault 27% | Other 1%
There are numerous methods and security tools available to help cybersecurity professionals detect and analyze insider attacks. A vast majority of the respondents identified the use of more than one security tool in their organization. By merging and analyzing these disparate sources, organizations are better able to deal with security breaches.

The survey concluded that most insider exploits are detected through Intrusion Detection and Prevention System (IDS/IPS) (63%), Log Management (62%), and Security Information and Event Management (SIEM) (51%) tools.

What controls do you have in place to detect and analyze insider attacks?

- Intrusion Detection and Prevention System (IDS/IPS) 63%
- Log management 62%
- Security Information and Event Management (SIEM) 51%
- Predictive analytics 40%
- User and Entity Behavioral Analytics (UEBA) 39%
- Other 2%
Identification, tracking and monitoring of key assets and system resources can help avert or limit an organization’s exposure to insider attacks. When security professionals manage and monitor their key assets, they are able to react faster and with more precision to mitigate incidents. More than three-fourths (78%) of respondents inventory and monitor all or the majority of their key assets.

An overwhelming majority (93%) of organizations monitor access to sensitive data. The level of monitoring varies; 47% continuously monitor data access and movement to proactively identify threats. Remarkably, five percent do not monitor data access and movement at all.

**Do you monitor key assets and system resources?**

- Yes, all key assets are inventoried and monitored: 42%
- Yes, a majority of key assets are inventoried and monitored: 36%
- Yes, but less than 50% of key assets are inventoried and monitored: 10%
- No, we have not completed the inventory of key assets: 5%
- Key asset management is not part of our security posture: 7%
- Not sure/other: 7%

**Do you monitor access to sensitive data?**

- Yes, we continuously monitor data access and movement and proactively identify threats: 47%
- Yes, but access logging only: 24%
- Yes, but only under specific circumstances (e.g., shadowing specific databases or files): 14%
- Yes, but only after an incident (e.g., forensic analysis): 8%
- No, we don't monitor data access and movement at all: 5%
- Not sure: 2%
INSIDER MONITORING

The increasing volume of insider threats have caused cybersecurity professionals to take more action and deploy User Behavior Analytics (UBA) tools and solutions to help detect, classify and alert anomalous behavior. The number of organizations monitoring their user behavior has increased significantly compared to last year (94% this year compared to 42% last year). The number of organizations that don’t monitor their users dropped from 21% last year to only six percent this year.

In this year’s survey, respondents said that they leverage User Activity Monitoring (UAM) (44%) as their top solution to manage user behavior within core applications, followed closely by the use of server logs (42%). Eight percent of respondents have no visibility at all, a decrease from last year of five points, which signals that organizations are investing in tools and resources to have better visibility into user activity.

Do you monitor user behavior?

- Yes, but access logging only: 44%
- Yes, we use automated tools to monitor user behavior 24x7: 29%
- Yes, but only under specific circumstances (e.g., shadowing specific users): 15%
- Yes, but only after an incident (e.g., forensic analysis): 6%
- No, we don’t monitor user behavior at all: 5%
- Not sure/other: 1%

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

- Have deployed user activity monitoring: 44%
- Rely on server logs: 42%
- In-app audit system/feature: 32%
- Have deployed keylogging and/or session recording: 26%
- No visibility at all: 8%
- Not sure/other: 3%
Every organization must be vigilant when it comes to data protection. Not all insider threats are malicious; some are the result of an honest mistake or careless employee behavior. Monitoring allows cybersecurity professionals to decrease their risk exposure by quickly detecting unusual employee system activity. Ninety percent of the respondents believe that it is necessary to monitor access to the organization’s sensitive data.

Identification of high-risk insiders is a key part of a threat prevention strategy. One way to identify these individuals is to profile their behavior and work patterns. Hostility toward other employees, late or excessive missing work, undue work outside normal work hours, and declining performance are just some of the indicators. Organizations surveyed strongly believe it is necessary to identify high-risk insiders based on their behaviors (88%).

Do you think it’s necessary to monitor and profile how insiders are accessing your sensitive data?

- Yes 90%
- No 3%
- Not sure 7%

Do you think it’s necessary to identify high-risk insiders based on their behaviors?

- Yes 88%
- No 6%
- Not sure 6%
The number of organizations that do not leverage threat analytics continues to decline year after year. This year, only 14% of respondents said they do not use analytics, compared to 30% last year.

Does your organization leverage analytics to determine insider threats?

- Yes – security analytics: 55%
- Yes – data access and movement analytics: 46%
- Yes – user behavior analytics: 38%
- Yes – activity management and summary reports: 33%
- Yes – predictive analytics: 32%
- No: 14%
- Not sure: 7%
Organizations are shifting their focus on detection of internal threats. In this year’s survey, detection (64%) surpassed deterrence methods (58%) to take the top spot, followed by analysis and post breach forensics (49%).

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

- Detection (e.g., user monitoring, IDS, etc.) 64%
- Deterrence (e.g., access controls, encryption, policies, etc.) 58%
- Analysis and post breach forensics (e.g., SIEM, log analysis, etc.) 49%
- Post breach remediation (e.g., back-up/disaster recovery, etc.) 41%
- Deception (e.g., honeypots, etc.) 28%
The survey reveals that organizations have recognized the growing significance of insider threats and are investing resources to develop comprehensive incident response plans. A vast majority (86%) of organizations have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.

How would you rate the maturity of your insider threat program?

- **36%** Mature
  (We have a formal threat detection, auditing and incident response program for insiders)

- **50%** Maturing
  (We are developing a formal program for insider threats)

- **10%** Immature
  (We have no formal program)

- **4%** Not sure
A majority of respondents surveyed (81%) say their organizations are moderately to very effective when it comes to addressing insider threat prevention and detection. Thirteen percent expressed that their organization’s insider threat programs are ineffective, while six percent do not have a program in place.

How effective do you consider your insider threat prevention and detection methods?

- 81% think their organizations are moderately to very effective addressing insider threat prevention and detection
- 48% are somewhat effective
- 10% are somewhat ineffective
- 3% are very ineffective
- 6% do not have an insider threat program
- 33% are very effective
For the third year in a row, lack of training and expertise (52%) remain the biggest barriers to better insider threat management. Other barriers include the lack of suitable technology (43%), while tied for third place in this year’s survey are both lack of collaboration among departments (34%) and lack of budget (34%). Notably, lack of budget fell from second place last year to third this year.

What are the biggest barriers to better insider threat management?

#1
52%
Lack of training and expertise
8% p.p. from last year

#2
43%
Lack of suitable technology
15% p.p. from last year

#3
34%
Lack of collaboration among separate departments
14% p.p. from last year

#4
34%
Lack of budget
16% p.p. from last year

Lack of staff 22% | Not a priority 10% | Not sure/other 5%
Detecting and preventing insider attacks are much more challenging than external breaches, as they are users with legitimate access that unwittingly create vulnerabilities or intend to maliciously exploit an organization’s cyber assets. Slightly more than one-fifth of respondents claim detection of insider threats is within minutes (22%), while 28% say within hours.

In this year’s survey, organizations are even more confident in their ability to quickly recover from insider attacks. Most organizations feel they could recover from an attack within a week (89%) up 18% from the previous year. Only two percent of companies believed they would never fully recover.

50% organizations detect an insider attack within hours
Not sure 8%

49% organizations mitigate and stop an insider attack within hours
Not sure 10%
Looking ahead, close to half of the surveyed organizations (49%) expect budget increases. Forty-three percent expect their IT budgets to remain flat, while only one percent foresee their security funding shrinking. This is a marked improvement in budget outlook compared to last year’s survey.

Defending against security attacks is an ongoing challenge; cybersecurity professionals are equally concerned about the rise in the volume and frequency of both external and insider attacks. Forty-three percent of organizations allocate over eight percent of their IT security budget to preventing, detecting, and mitigating insider threats.
Having a well understood information security policy and documented procedures help protect organizations and reduce risk from both internal and external cyber threats. The primary policy-based insider threat management methods that organizations have in place are the use of company policies and training (68%), internal audits (63%), and background checks (56%).

Organizations realize that prevention and awareness are key cornerstones in the defense against insider security breaches; an overwhelming majority (82%) have implemented insider security programs.

- **What administrative policies and procedures do you have in place for insider threat management?**
  - Internal audits: 63%
  - Background checks: 56%
  - Data classification: 50%
  - Information security governance program: 43%
  - Whistleblower program: 27%

- **Do you offer training to your employees and staff on how to minimize insider security risks?**
  - **YES**: 82%
  - **NO**: 13%
  - Not sure: 5%
Creating an integrated view of data across an enterprise enables a more holistic risk profile than that supplied by individual systems. As more data becomes available, contextual data between different data sources can be analyzed to uncover more threats than previously possible. For example, data from business systems provide context into security systems and operational systems to determine if a user’s actions are normal for the current state of company growth, or if they are indications of a compromised account.

The survey found that 75% of survey respondents currently incorporate IT infrastructure data, such as network and printer logs, into insider-threat detection programs. Beyond this, 34% of survey respondents have security data lakes that can be leveraged to uncover advanced threats, which typically escape detection unless more integrated data and security analytics are available. With 25% of insider threat programs incorporating a commercial data lake, it’s clear that security across an enterprise is becoming a cross-functional endeavour.

Does your Insider Threat Detection program leverage information from across the organization?

- **75%**
  - IT infrastructure systems
  - (network, printers, etc)

- **56%**
  - Security systems

- **47%**
  - Operations systems

- **43%**
  - Financial systems

- **37%**
  - Business systems

HR systems % | Security datalake 34% | Commercial datalake 25% | Other 4%
Security is clearly becoming more of an integral part of doing business, as opposed to an add-on to running a business. The interconnectedness of the digital age creates greater attack surfaces, especially from within the enterprise (or from illicit connections which masquerade as being from within the enterprise).

There is a greater need for insider threat programs to detect deliberate and unintended security compromises than ever. Where 54% of insider threat programs are being driven by a proactive IT team initiative, 39% are driven by a proactive security team initiative. Governance, compliance, and directives from an executive management team also drive more than a third of insider threat programs. One fifth of insider threat programs are driven by confirmed or suspected incidents, with 18% being a directive from the board of directors.

What is the primary driver of your insider threat program?

- Directive from the executive management team 32%
- Previously confirmed incident 22%
- Suspected incident 21%
- Directive from the board of directors 18%
- We do not have an Insider Threat program 5%
Inside Threat or Insider Threat? What difference does one letter make? The two are not the same, yet they are similar enough that 80% of insider threat programs encompass inside threats.

An insider threat refers to an internal employee who accesses data in non-compliant ways (for example, Edward Snowden). An inside threat includes APT (Advanced Persistent Threats), malware, ransomware, or phishing attacks that originate from outside the enterprise then internally accesses or distributes data in non-compliant ways. Ultimately both can cause the same outcome in terms of compromised security posture and data loss. The majority of insider threat programs encompass the detection and investigation of inside threats.

Does an Insider Threat program also encompass detection and investigation of Inside Threats?

- 80% YES
- 20% NO
Interset is a security analytics pioneer. An In-Q-Tel company, Interset expands risk visibility and optimizes strained security resources by distilling billions of events into a handful of prioritized threat leads. Built upon a highly scalable big data architecture with unsupervised machine learning, Interset transforms security operations efficiency and focuses resources only on the risks that matter.
This research is based on the results of a comprehensive online survey of 472 cybersecurity professionals to gain deep insight into the insider threat faced by organizations and the solutions to detect, remediate, and prevent it. The respondents range from technical executives to managers and IT security practitioners, representing organizations of varying sizes across all industries.

**JOB TITLE**

- Director: 34%
- Manager/supervisor: 25%
- CTO, CIO, CISCO, CMO, CFO, COO: 19%
- Vice president: 9%
- Specialist: 9%
- Other: 4%

**DEPARTMENT**

- IT Operations: 59%
- IT Security: 30%
- Other: 11%

**COMPANY SIZE**

- Fewer than 100: 5%
- 100-999: 37%
- 1,000-4,999: 27%
- 5,000-10,000: 17%
- Over 10,000: 14%