Secureworks®

WHITE PAPER

# What You Need to Know to Combat the Insider Threat

## It's common for organizations to focus a large portion of their security strategy around potential outside cyber-threats.

However, studies show that insider threats are on the rise and many times are more difficult to identify.[1] Learning and observing common insider behaviors and technical actions is one of your greatest stronghold against these insiders.

In this white paper you will learn the potential damage an insider threat can cause an organization, along with ways to identify them. In addition, you will discover that building an Insider Threat Interdisciplinary Working Group is critical for observing and documenting behaviors and actions so that appropriate measures can be taken to protect against the insider threat.

Espionage has been around as long as man has engaged in commerce and formed armies to protect communal economic and security interests. Examples of economic espionage abound, including a research chemist for a global pharmaceutical company who stole trade secrets for more than three years, offering them for sale through a company where she was a 50 percent partner. Another is a disgruntled former employee who entered into a consulting agreement with a rival company and gave them trade secrets he had stolen from his previous employer. In another event, an employee gave his employer's trade secrets to an investor he believed was willing to finance a business for him in India.

According to the FBI, theft of intellectual property is an increasing threat to U.S. organizations and can go unnoticed for months or even years. In addition, Veriato's 2018 Insider Threat Report states 53 percent confirm insider attacks against their organization in the previous 12 months (typically less than five attacks). 27 percent of organizations say insider attacks have become more frequent.

Understanding the types of insider threat events that can occur, the damage they can cause to an organization and the behaviors insider threats exhibit is the first step to awareness and protection. However, managing the risks of potential insider threats is not a job that one security manager can handle, but requires an interdisciplinary working group focused on open communication across functions.

In this briefing you will learn that the motives and indicators of insider threats vary greatly and why a structured Insider Threat Committee is required to protect your organization from these threats.

**23%**

***attacks were deliberately malicious, while 13% involved user credential theft.[2]***

**53%**

***confirm insider attacks against their organization in the previous 12 months (typically less than five attacks). 27% of organizations say insider attacks have become more frequent.[3]***




Secureworks

## A Deeper Look at the Insider Threat

An insider threat is the potential violation of system security policy by an authorized user.[4] Regular employees pose the biggest insider threat to organizations (56 percent). This is followed by privileged users, such as managers with access to sensitive information, (55 percent) and contractors/temporary workers (42 percent) according to 2018 research.[5]

Insider threat motives will vary, but many times will fall under the category of IP Theft, which is motivated by fraud or espionage.

- **IP Theft:** The use of insider access and knowledge to steal IP from an organization.
- **Fraud:** Unauthorized modification or theft of an organization's data or good for personal gain.
- **Espionage:** The use of insider access to obtain classified information for industrial or economic exploitation.

### The Impact of IP Theft

Every company's nightmare is to have its intellectual property stolen. Trade secrets, product plans and customer lists are three common assets targeted by insider threats. With this stolen information these insiders can start competitive businesses, sell the IP for financial gain, or leverage it for sabotage or personal advancement. These insiders are sheep in wolves clothing, so it is important to understand where they target most frequently, how to detect them, and your potential financial impact to understand and mitigate your risk.

***While the true cost of a major security incident is 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.[6]***

The importance of observing and reporting suspicious behaviors as an early detection measure are critical. However, 15 percent of organizations do not have appropriate controls to detect and prevent an insider attack, while another 12 percent are not sure.[7]

Educating organizations on the reality of insider threats, how to be watchful for specific behaviors and enforcing a zero tolerance approach are the first steps to securing your operations.

## Monitoring Behaviors

Insider threats modus operandi (MO) is having a low profile; it's easy for insiders to blend into the rest of the organization without raising red flags in the midst of day-to-day fires and standard business operations. However, many times they leave clues; altering their actions and behaviors slightly, providing a glimpse into a much larger and destructive operation that is underway. Keeping your eyes and ears open at all times to unusual or inconsistent behaviors is the most effective way to detect who within your organization is a potential insider threat. Below is a list of common behaviors that may indicate an insider threat.

It is important to keep in mind that these behaviors can be reactions to traumatic events that have occurred in an employee's personal life and further examination should be handled with care. For example, it wouldn't be uncommon for someone who lost a loved

one to display sudden signs of depression. Engaging in an appropriate investigation is the key to determine if any threat truly exists. Remember that behaviors associated with IP Theft are representative of patterns, not one isolated instance of a behavior.

| Behaviors Associated with Theft of IP | | |
|---|---|---|
| Threats | Bizarre behavior | Unreasonable |
| Substance abuse | Paranoid | Desperation |
| Outside suspicious associations | Depression | Sudden unexplained affluence |
| Overwhelmed | Angry, argumentative & confrontational | Leverages resources for side business |

## Monitoring Technical Actions

In addition to suspicious behaviors, many times technical actions can be a tip off that an employee may be an insider threat. An insider will frequently attempt to gain access or privileges to systems, information, or physical locations that are not needed for their assigned duties. If these accesses are not granted, they may try and take matters into their own hands by attempting to gain access through other means. Social engineering co-workers to gain access to a physical location, documents, or network access through their employer's systems are a few tactics they may try.

In some cases, they will go as far as using hacking tools through a network connection. These tools can be used both on the internal network and from a network not belonging to the company. Once the insider has access to the targeted data they will need to remove the data from the company's location to exploit its value. Use of cell phone cameras, mobile media, printing, emailing, FTP, and "backdoors" are a few of the common channels used to successfully acquire the data. Below is a list of technical actions that can be a sign of an Insider Threat.

| Technical Actions and Behaviors | | |
|---|---|---|
| Violates "need-to-know" | Unauthorized use of mobile media/cloud services | Downloads or installs malicious code or tools |
| Former employee accessing network resources | Attempts to obtain unauthorized access | Relabeling disks |
| Unauthorized encryption | Modification of ISP's service logs | Unauthorized information transfer |
| Theft of hardware, software, and documents | Violation of acceptable use policy | Violation of physical security policies/procedures |
| Disabling of anti-virus and other security features | Refusal to return laptop upon termination | Network probing |
| Use of backdoor accounts | Excessive printing | |

## Implementing an Insider Threat Interdisciplinary Working Group

Educating cross functional groups to identify insider threat behaviors and technical actions is a portion of the puzzle, however it won't guarantee an armor of protection. If groups are in silos with no formal communication plan in place, you are at risk that concerning behavior or technical observations will be overlooked and never reported, resulting in a greater likelihood that an insider threat will achieve his or her objective.

Building a team across the organization along with a communications framework is vital for open dialogue and the greater likelihood that concerning indicators will get reported and investigated in a timely and proper way.

The list below represents the Insider Threat Interdisciplinary Working Group along with the roles and areas of responsibility each functioning group should be reporting to the group at large.

- **Executive Chair** – The Interdisciplinary group starts with the executive sponsor. This role drives the vision, goals, and objectives of the Interdisciplinary group by coordinating the various member groups to ensure unity of effort. The executive chair sets the strategy, meeting requirements and tasks necessary to enforce cooperation.
- **Ethics** – This is a team that sets the acceptable behavioral boundaries within an organization most often expressed in personnel and company polices and communicated through training. Policies may set behavioral boundaries for various actions such as gift acceptance and giving, intra-office relationships, use of company resources for personal use, and other behavioral expectations. Often suspected violations are referred to appropriate personnel for investigation.
- **Investigations** – This team is responsible for performing formal investigations. They gather physical and electronic evidence, conduct interviews, and perform other investigative actions related to security incidents and suspected violations of company policy. Other authorized investigative activities may be conducted by HR or IT Security as skill sets or the functional responsibilities dictate. Investigative results may be used to establish a pattern of behaviors consistent with insider threats. Intent is sometimes the most difficult element to establish and may be contrary to employees stated reasons for committing certain acts. Skilled investigators rely upon identifying actions, which logically infer intent rather than relying solely upon a person's statements.
- **Physical Security** – This team is responsible for tracking when and where employees badge in and out for access, manage additional requests for increased access, and identify security violations and attempted violations. Many times an Insider Threat will change their working hours in order to work without supervision or attempt to gain access to records or physical spaces.

- **IT Security** – This team is typically imbedded into the IT department or is assigned to the Chief Information Security Officer. The IT Security team is responsible for monitoring IT alerts and network security violations. Every organization has different guidelines, but a few examples of incidents may include: emailing sensitive information to an external email address, uploading proprietary data to a 3rd party website, loading unauthorized software to corporate computers, copying information to mobile media (thumb drives/CDs), and claiming the loss of laptop. All of these actions and other suspicious network activities should result in an investigation.
- **Audit** – This is a team dedicated to ensure compliance with company standards and procedures, while managing external regulatory oversight. By the nature of their duties, they conduct many interviews, reviews of records, and are often aware of strained relationships with individuals disgruntled in work and personal matters. They potentially have valuable insights that are not formally documented in Audit Reports. However, their insights could be crucial when viewed through the lens of an insider threat perspective.
- **Human Resources** – This team has volumes of information that could be indicative of insider threats, yet many times are not involved in investigations of Insider Threats. HR has many great tools that can help paint a more complete picture drawn from knowledge of performance evaluations, harassment claims, and disruptive and/or disgruntled employees.
- **Legal** – This team is mandatory for the success of the Insider Threat Interdisciplinary program. There are many sensitive and confidential restrictions on the use of information maintained by the various members of the Inter- disciplinary Working Group. Legal will help in navigating the competing laws, regulations and policies, while allowing the business to protect itself against criminal acts an insider may inflict upon the company and its employees.

While it's important to keep responsibilities separate across the teams to avoid bias and conflict of interest, depending on your corporate structure, the hierarchy of teams may be structured for the best opportunity for collaboration. For example, Ethics and Audit may be housed within Human Resources while Investigations, Physical Security and IT security may be subsets of your security operations group.

To facilitate collaboration among the teams of the Insider Threat Interdisciplinary Working Group, it is suggested that a group email or confidential blog be created to enable the posting of suspicious incidents and for the coordination of activities in response. With this visibility into the activities of every team, all others will understand how best to support the effort to thwart insider threats in a unified way.

## Overcoming Organizational Weaknesses

Corporate standards, policies, and organizational preparation play a critical role in the efforts to resist insider threats. Starting with the hiring process, this is a key time to identify potential behavior problems prior to providing access to work spaces, networks, employee and client personal information. It is critical that a thorough background check

is provided that includes at a minimum: identity verification, financial and drug screening, criminal history checks, and education, employment, and certification verifications. If you are hiring someone who would need higher levels of access to network capabilities or critical IP a more detailed investigation should be conducted.

Once an employee has been vetted and is onboarded, it is critical that onboarding security awareness training occurs that covers acceptable data use policies, security responsibilities, ethical standards, and what, when, and how to report concerns both officially and anonymously. Most importantly you should cover what not to do. Security awareness training should be mandatory and offered annually to all employees to ensure everyone is up to date with all security guidelines and updates.

If an employee has not followed your security guidelines, or is displaying concerning behavior, the sooner a formal documented investigation is started the sooner you will be able to address any potential risks. It is critical that a proper investigation is conducted prior to taking any actions toward a suspicious employee. If premature disciplinary actions occur, including dismissal or prosecution, without an investigation and action plan to prevent potential violence, you may put your entire organization— including employees—at risk.

Organizations must take the approach that no single employee is irreplaceable. By segregating duties, you will minimize the potential damage that any one employee can cause. Insiders come in at all levels, from janitorial employees to top executives and 3rd party vendors so it is important to have your guard up regardless of a person's position.

## Conclusion

When looking at the spectrum of insider threat activities there is no single profile to identify a malicious insider. Age, gender, positions in a company, and technical competency all vary greatly from incident to incident and are unreliable as predictors of malicious activities. What is commonly observed in all insider cases are the changes in behavior. Observing any negative changes in productivity, interaction between supervisors and co-workers, and tardiness are just a few actions that should be noted and reported. However, this cannot be achieved alone. Implementing an Insider Threat Interdisciplinary Working team is a proactive measure that can help provide a bird's-eye view of your organization. Enabling this broader team to keep their eyes and ears open for technical and behavioral clues is your best defense against the insider threat.

Sources:

[1-2] Ponemon Institute, 2018 Cost of Insider Threats

[3, 5-7] Veriato 2018 Insider Threat Report

[4] DHS Science and Technology Directorate, Cyber Security Division – Insider Threat

Secureworks®

## Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™


### Corporate Headquarters

**United States**
1 Concourse Pkwy NE #500 Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

### Europe & Middle East

**France**
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

**Germany**
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

**United Kingdom**
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

**United Arab Emirates**
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

### Asia Pacific

**Australia**
Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

**Japan**
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp