FORTINET

Recognizing the Many Faces of Insider Threats

Table of Contents

FORTINET

Executive Overview

Insider threats pose significant risks to businesses. Whether caused by carelessness or malicious intent, insider threats can be mitigated. To truly understand the risk of insider threats, one must first know the different forms that they can take. This eBook breaks them down into five personas: disgruntled employees, corporate spies, accidental exposures, outgoing employees, and fraudsters, each of which has unique motivations and behavior patterns.

In a recent survey, "employees" topped the list of actors that companies are most concerned about exposing their organization to risk—both knowingly and unknowingly.[1]

01 Introduction: Spotting an Inside Job

Rapid expansion of the network attack surface is impacting businesses of all sizes and industries. Almost 80% of organizations are introducing digitally fueled innovation faster than their ability to secure it against cyberattacks.[2] This creates many exposures, with insider threats posing significant risks to organizations, their data, and their brand reputations. A recent study reveals that 30% of all breaches are caused by malicious or negligent insiders.[3]

Damage from insider sources can be hard to detect because these threats encompass a wide range of behaviors and motives. It could be a disgruntled employee attempting to disrupt operations, a staff member looking to earn extra cash by selling customer data, or a well-intentioned co-worker who merely sidesteps a company policy to save time.

Organizations often underestimate the potential impact of insider threats. Following are five insider profiles that security leaders need to understand in order to identify the who and why behind common threat exposures within organizations.

The cost of malicious insider attacks has increased by 15% in the past year, equating to an average of US$1.6 million annually for an organization.[4]

02 Disgruntled Employee

As with any other relationship, the employee-employer dynamic changes over time. Small resentments and grievances can build up and turn into grudges against the company and/or leadership team. The internal reasons that an employee might use to justify doing harm to the organization may include:

- **Unkept promises.** Someone may have been told that there is room for advancement but gets upset when they do not receive a promotion they feel has been earned.
- **Undervalued.** Some employees may feel as though the organization is not challenging them and/or offering them compensation commensurate with their talents and abilities.
- **Unheeded advice.** If an employee repeatedly provides what they think is sage advice on pressing issues and the advice is never taken, then their opinion of the company or leadership may sour.

Human indicators—such as constant foul moods, incessant complaining, or veiled threats—can be precursors to a staff member taking "lone-wolf" action to harm the company from the inside. Threats posed may include transfer of proprietary information by email, cloud uploads, unauthorized remote desktop protocol (RDP) installations, or copying to physical media (e.g., USB thumb drive). Risk of sabotage that disrupts network or business operations by intentionally introducing malicious code is another potential attack vector.

A disgruntled employee may or may not be tech savvy, so the trail they leave after attempting to pilfer data may be well-hidden. Being able to detect this behavior before any significant damage can be done is paramount.

In a Deloitte study on cyber risk in the electric power industry, internal threats attributed to disgruntled employees are among the most common threats.[5]

03 Corporate Spying

Corporate espionage is always a possibility for any business with intellectual property. An employee who needs money for personal reasons (e.g., family illness, debts, addiction) can be vulnerable to solicitation for trade secrets or sensitive data from a competing entity. But corporate spies do not always have to be turned; they may also be planted in an organization early on by a competitor or a nation-state to await further instruction.

The clandestine nature of corporate espionage means it is usually difficult to detect from a human perspective. Depending on the industry, corporate spying can amount to policy violations, criminal misconduct, or even treason (as within a government organization or critical infrastructure such as energy). Exfiltration of sensitive or valuable files by physical or digital methods is the most common goal. Installing software for remote access or stealing user or device credentials are other potential objectives of corporate spies.[6]

The FBI's Counterintelligence Division reported a sharp spike in the number of espionage investigations last year, citing a 53% increase in caseloads as evidence.[7]

04 Goofs: Accidents, Ignorance, and Arrogance

Mistakes happen—and unintentional damage as a result of careless actions is exceptionally common today. Well-intentioned employees often commit errors out of basic ignorance, taking a hasty shortcut for the sake of productivity, laziness, or even out of arrogance—thinking that a particular company policy does not apply to them.

Writing passwords on sticky notes, allowing a stranger to "tailgate" through a physical access control after a badge swipe, or indiscriminate clicking on email or weblinks can lead to damage from malicious outsiders who are trolling for an unwitting pawn on the inside. Other examples of nonmalicious employee goofs include: decrypting a sensitive document and then putting it on a shared drive, saving sensitive files on a personal hard drive for fast and easy access, disabling endpoint security and control, and using personal email accounts for official communications.

Even with robust employee education that reinforces good cyber hygiene, it often just takes one slip-up to put the company at risk of data exfiltration or network tampering. There are unfortunately a limited number of technical controls to address this particular insider threat vector.

According to Ponemon Institute research, 64% of attacks resulted from employee or contractor negligence.[8]

05 Exit Strategy

There comes a time in almost everyone's career when they decide that a change is necessary—whether it is for new challenges or advancement in salary and title. While bringing experience and fresh ideas to a new company is part of the equation, taking customer data from a previous employer is not. When it comes to dealing with employee exits, companies should be mindful of those who have access to:

- **Customer data** such as contact information, budgets, or price lists
- **Intellectual property** such as code, schematics, and business processes
- **Technical data** such as configuration or vulnerability information

It can be very difficult for a company to predict when one of its best employees might leave the company. Once an employee tenders their resignation, though, it is time to act. Companies must have protection in place to detect if any sort of data theft is being perpetrated.

Boredom, malaise, and burnout all lead to employee turnover—and greater risk exposure. Virtually every organization faces threats as a result, with almost 40% of U.S. adult workers saying they are considering quitting their jobs due to burnout.[9]

06 Fraud

Like spying, employee fraud may be driven by malicious personal gain or desperate personal circumstances. If an opportunity exists and the reward outweighs the risk, a fraudster inside the organization may take advantage. Insider fraud can be very damaging to an organization. At the very least, stolen data (e.g., customer credit card numbers, financial information, electronic health records) is being sold on the black market. This impacts the company brand and consumer trust when breaches are discovered and made public. But organizations also face steep legal repercussions and increasingly harsh compliance penalties for mishandling the personally identifiable information (PII) of customers.

Fraud can be fairly easy to detect if normal behaviors are established. Databases and file transactions on employee systems and the network can be monitored. A database query that fetches many records, followed by the creation of a spreadsheet file can help pinpoint how and when data is being exfiltrated—and by whom.

The average cost of an insider security breach more than doubles if the type of incident involves an imposter or thief who steals credentials.[10]

07 What to Watch For

Threat management programs must include a robust understanding of each of the above insider profiles, their motivations, and the situations that give rise to them. Combining this understanding with the right tools (such as endpoint monitoring, user behavior analysis, as well as data loss prevention controls) can give businesses a far greater chance of mitigating threats and keeping critical resources safe. Further, combining accurate user behavioral data with artificial intelligence allows deep visibility and even more accurate user monitoring on an endpoint-by-endpoint basis.

In response to the aforementioned insider threats, some questions to help direct improvements to your organization's existing security posture might include:

- Are any users logging on at abnormal times?
- Are users attempting to access files that they are not supposed to?
- Are you noticing attempts to copy or move confidential material?
- Can you establish a baseline of activities performed by suspicious users on a regular basis?
- Can deviations from established normal user behaviors be flagged as alerts?
- Are database logs being sent to analytic tools?
- In the event data is being compromised, are any automated responses in place to revoke privileges and prevent data loss?
- Is an ongoing cyber-hygiene employee training program in place to reinforce proper care and procedure to help avoid unintentional user risks?

[1] "Mobile Security Index 2019," Verizon, March 2019.

[2] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture/Ponemon Institute, March 6, 2019.

[3] "2018 Breach Data Investigation Report," Verizon, April 10, 2018.

[4] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture/Ponemon Institute, March 6, 2019.

[5] Steve Livingston, et al., "Managing cyber risk in the electric power sector," Deloitte, January 31, 2019.

[6] Alastair Paterson, "Don't Fall Victim to IP Theft and Corporate Espionage," SecurityWeek, February 1, 2018.

[7] John Slattery, "Economic Espionage and the Growing Case for Corporate Counterintelligence," SecurityInfoWatch, June 15, 2018.

[8] "2018 Cost of Insider Threats: Global Organizations," Ponemon Institute, April 2018.

[9] "your best employees are leaving. but is it personal or practical?" Randstad, August 28, 2018.

[10] "2018 Cost of Insider Threats: Global Organizations," Ponemon Institute, April 2018.

www.fortinet.com

364132-0-0-EN

October 15, 2019 3:49 PM

eb-insider-threats