SANS

Analyst Program

Whitepaper

Combating Insider Threats with People, Processes, and AI-Based Technology

Written by **Heather Mahalik**

July 2021

BlackBerry

Introduction

All organizations, big and small, face the risk of insider attacks. Those who assume "it won't happen to me" make a grave mistake. This paper walks you through attack definitions, risks, and the latest defenses to help increase your organization's resiliency to these types of devastating attacks.

Insider threats represent one of the more difficult threats to detect from both a human and technology perspective. Even worse, you might not detect them for an extended period of time, allowing attackers prolonged access to proprietary information that can affect your organization's financial viability for years to come.

As the first step in prevention, you need to understand the problem and severity of these types of attacks. What risks exist? Do *insider risks* differ from *insider threats*? Why do these definitions matter? Understanding the different threats helps you prepare better defenses.

We are human, and humans who are not educated about potential threats pose a great risk to all organizations.

A human-only security team cannot detect all threats. Even the best defenders need technology to assist in protecting their organizations. The right level of protection requires the implementation of advanced technology software that studies employee behavior by leveraging user and entity behavioral analytics. Despite their immense value, however, some user and event behavior analytics (UEBA) solutions can prove complicated to customize and scale, which may hinder an organization's capability to manage alerts and investigations. Adding to the challenge, organizations often have insufficient knowledge about their employees, their roles, and typical job duties, which in turn limits how well UEBA solutions can perform. As a result, organizations often find these products difficult to configure and hard to understand.

So, what does this all mean? It means that you need next-generation machine-learning-powered technology as an ally right alongside your human defenders. You want to empower security teams (rather than overwhelm them) with forward-leaning AI-based tools that stop chaos before it begins.

Key topics covered in this paper include:

- The definition of insider threats and how these attacks occur
- How insider risks differ from insider threats
- Challenges in combating these attacks
- The reality of these threats and why you need to take them seriously
- How to mount a defense against insider risks, even unintentional risks

Defining Insider Attacks

Your organization seems to employ the right people, and you take employee satisfaction seriously. The teams get along well, and it appears that everyone agrees with your mission. So, what makes people do the wrong thing? Why do some employees become a threat to your organization? Is it intentional? Is it accidental? Were they recruited? Most organizations, even those with the strongest defenses in place, find it extremely difficult, if not impossible, to fully map the mindset of disgruntled employees and recognize threats before they happen. Defenders and other employees untrained to look for abnormal behaviors may miss something. Stopping insider threats before they activate becomes exponentially more difficult, and so the risk remains.

Understanding insider threats and the difference between insider threats and insider risks will help when it comes to building a defense to protect your organization. According to the National Counterintelligence and Security Center (NCSC), "All organizations are vulnerable to insider threats from employees who may use their authorized access to facilities, personnel, or information to harm their organization, intentionally or unintentionally."[1] The NCSC also states, "The harm can range from negligence—such as failing to secure data or clicking on a spearphishing link—to malicious activities like sabotage, intellectual property theft, fraud, or workplace violence." Figure 1 depicts the difference between insider threats and insider risks.

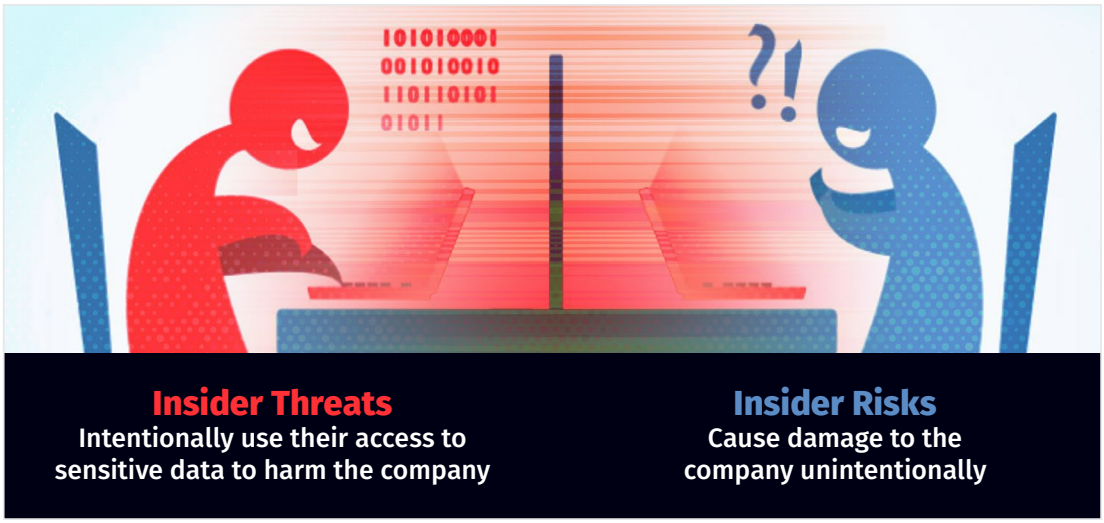

Figure 1. Difference Between Insider Threats and Insider Risks

Understand the differences between insider threats and insider risks. Discuss them with your employees.

[1] "NCSC Issues 'Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective'," The National Counterintelligence and Security Center, www.dni.gov/index.php/ncsc-newsroom/item/2197-insider-threat-mitigation-for-u-s-critical-infrastructure-entities-guidelines-from-an-intelligence-perspective

Insider Risks

Insider risks derive from users/employees who are often unaware and do not intend to cause harm to the organization. Insider risks arise from targeted attacks such as mass mailing, spearphishing, credential stealing, and more. Phishing is still an extremely popular entry point because it is inexpensive and effective. Objectives determine threat actor behavior, which typically remains similar from victim to victim. For example, the use of stolen credentials may enable the threat actor to propagate throughout the organization's network, access targeted resources, exfiltrate sensitive data, and deploy ransomware to complete the double extortion found in today's ransomware attacks. Insider risk is extremely common in incident response cases.[2] The threat is real, and the landscape for such is not diminishing.

Assume your employees will make a mistake. Create training that educates employees about safe links. What makes a link unsafe and, more importantly, how can the employee detect it? Implement the training and send periodic tests with phishing links to test whether anyone in your organization doesn't understand the risk. Make it easy for employees to report a phish. For instance, consider implementing a *Report a Phish* button in the corporate mail client. A breach can occur with a single click.

In addition to proper training, awareness, and drill, anti-spam and anti-phishing tools can serve as another line of defense. Such tools can detect the phishing attack before it hits the employee's inbox, protecting both your organization and the employee.

What do insider risks look like in reality? A simple scenario is as follows. Molly works closely with the CEO. She receives an urgent email that includes a link for her to click to approve a document sent from the CEO. The email looks like all other emails she receives on a daily basis. She clicks the link, but the attachment she expects to see does not appear. Nothing "happens" (or so Molly thinks). Several days or weeks later, the attack is discovered, and Molly didn't even know it happened. She had no ill will toward her company. She had often received messages from her CEO and just clicked a link as she always had in the past, thus allowing the attacker access to the system. Could this have been prevented? Is your organization ready to defend against these risks? What policies/procedures does your organization implement when something like this occurs? What would have happened had Molly reported the email to the security team?

[2] "The Five Most Dangerous New Attack Techniques and How to Counter Them," RSA Conference, www.rsaconference.com/library/video/the-five-most-dangerous-new-attack-techniques-and-how-to-counter-them, posted March 2019. This paper's author was among the presenters.

Insider Threats

Figure 2. Edward Snowden, Classic Insider Threat (Image source: theguardian.com)

Insider threats also pose a significant risk to a company and prove difficult to combat from both a technical and a user perspective. The term *insider threats* refers to acts perpetrated with malicious intent by employees with the goal of harming or sabotaging an organization. These employees are often disgruntled, want revenge, or are influenced by money or ego. According to Verizon's 2021 Data Breach Investigations Report, insider threats cause 28% of breaches, and financial gain motivates 76% of the insiders.[3] Edward Snowden (Figure 2) is a notorious example of an insider threat.

Train your employees and defenders to take notice of employees who experience behavior changes or exhibit behavior that seems incongruous with their job duties. Implement an AI tool that helps your defenders detect abnormalities. Those who spend extravagantly, are in the office at odd hours, are now distant or distracted but were happy before, all demonstrate potential indicators of behavior anomalies. A false alert to your defenders is better than a full breach of your data. Ensuring your security team follows up with all reports will keep your organization safe. This issue is discussed in the "Defensive Considerations" section of this paper.

Implement employee training to teach what to look for when it comes to insider threats. Explain the symptoms and common characteristics of a disgruntled employee. Access free online resources to help you create such training.

While insider threats are less common than insider risks, these attacks do happen, as incident response investigations and even major government breaches attest. Sometimes an organization may suspect that an insider represents a legitimate concern or threat and need help proving it. Other times, however, the organization recognizes the insider as the threat and investigates any incidents. Sadly, the latter is more common, and that means the breach has already occurred. When organizations detect insider threats, the punishment depends on the severity of the situation. Some employees are simply terminated, whereas others face prosecution.

Consider this example of an insider threat. Darryl works for a company that used to have 10 employees, is extremely close with the owner, and has access to everything in the company, including proprietary data. The company sells to a larger organization, and Darryl is unhappy that he didn't receive retention bonuses like his co-workers did. A competitor offers him money to provide access to files, accounts, and potentially his credentials. Darryl enters this slippery slope.

[3] "2021 Data Breach investigations Report," Verizon, www.verizon.com/business/resources/reports/dbir/

Challenges in Combating Insider Attacks

Why does combating these attacks prove so difficult for defenders? Protecting your assets and organization while not overburdening employees or otherwise hindering their work requires walking a fine line. Threat detection programs and applications may add overhead to users and thus impede their work performance. Most organizations struggle to find and retain good talent, and imposing burdensome procedures on that talent does not help keep them happy. Employees want efficiency and freedom, while organizations seek safety. Employees also expect some privacy. How do you find the happy medium?

Employees want efficiency and freedom, while organizations seek safety. Employees also expect some privacy. How do you find the happy medium?

To detect attacks before they happen, organizations need easy-to-use and easy-to-configure, optimized continuous authentication tools. Put in place in advance of an attack, such preventive measures would have helped in several cases that unfortunately became newsworthy. For example, the Coca-Cola and Eastman investigation showed that insider threats may span across many companies. If insider Dr. Xiaorong You had been detected, she would not have successfully shared proprietary information from both Coca-Cola and Eastman.[4] This is just one example; other companies such as Boeing[5] and Capital One[6] also fell victim to insiders who breached company trust.

TAKEAWAY

No organization is immune to this threat, so we must all remain proactive and vigilant.

Why Be Prepared for the Worst

Insider attacks can happen to any kind of business, nonprofit, or other organization. Because human behavior and loyalty can change quickly, no organization can consider itself entirely safe. Good defenses can help limit threats or even stop them before they actualize, but such defenses do not happen overnight. They require a great deal of thought and effort. What will keep your organization safe from a threat that could cripple your environment? Continuous monitoring is a common defense, but what else can help? Companies need a tool that provides a greater level of protection as it learns the behaviors of employees and alerts on any abnormality that could legitimately threaten the organization—something that learns on the personal level without being overbearing.

Planning your defenses will help stop threats before they happen.

Imagine knowing the typical behavior of everyone in your environment and then ascertaining whether someone other than the legitimate user is using a compromised credential. Certain AI-based tools do precisely that by learning the normal behaviors of your employees and their daily activity and then raising an alert flag when any abnormal activity occurs. Passive biometrics, such as typing and mouse usage

[4] "Coca-Cola Trade Secret Theft Underscores Importance of Insider Threat Early Detection," CSO, www.csoonline.com/article/3613953/coca-cola-trade-secret-theft-underscores-importance-of-insider-threat-early-detection.html

[5] "Mitigating the Insider Threat: Boeing's Successful Approach," Security Magazine, www.securitymagazine.com/articles/88654-mitigating-the-insider-threat-boeings-successful-approach

[6] "Capital One Breach Highlights Challenges of Insider Threats," Decipher, https://duo.com/decipher/capital-one-breach-highlights-challenges-of-insider-threats

patterns (speed, key transition, movements, and other sometimes subconscious behavior), make this response possible. These types of persona-learning tools can monitor normal user behavior and detect anything unusual for that person on that specific device. If a deviation from normal occurs, your AI tools can challenge the user for authentication or lock the account. Tools with such capabilities augment humans to make your company's level of protection that much stronger.

Human behavior varies significantly from user to user, and behavioral analytics can aid in anomalous detection. As previously stated, organizations want to avoid burdening the user while simultaneously providing the capability to obtain a digital fingerprint for specific users. This software sits invisibly on the endpoints and can also adjust the security policies and restrictions based on environmental risks such as location. Coffee shop access, for instance, often entails greater risk than access from home or corporate HQ, which means the software could automatically apply a more restrictive policy when the user is in the coffee shop vs. HQ.

Biometrics and authentication programs detect insider risks. Insider threats represent a more difficult problem. With insider threats, user behavior across the network, keyboard, and mouse will match, so we need specific models and rules that detect user behavior anomalies *across* peer groups. Organizations also need to look beyond biometrics to application and network access patterns for the user. For example, if a person in IT accesses and downloads sensitive Salesforce data, you want such behavior flagged as a risk. Other scenarios could include sending data outside of the company network, uploading to external sites, or accessing systems that are not usual based on the user's prior normal activity.

Because you want to detect insider threats and risks before they begin, you need to implement software that understands users and detects unexpected behavior. User behaviors are set, and any unusual behavior should trigger additional hurdles for the user to clear. For example, let's say a software solution fingerprints Alex's behavior. If Alex repeatedly tries to access a file she doesn't have access to or log in to a site that she hasn't accessed before, roadblocks pop up to confirm Alex's identity. A trust score determines the size of the roadblock. These roadblocks may include authentication prompts that force users to re-authenticate for access or locking the account to force users to call the help desk to verify their identity.

The security team should also maintain a watchlist of those who are leaving the company, being tracked for poor performance, or have been reported as a potential threat. The watchlist arms your defenders with a place to start keeping a close eye.

TAKEAWAY

User trust scores can be adjusted by organizations to take progressively stronger actions as users exceed score thresholds.

Defensive Considerations

A layered defense approach for technology may help in maintaining a smaller and more manageable footprint. The first step involves a basic block and tackle strategy, where the company defines boundaries and enforces them by blocking access (see Figure 3). This approach can entail such simple measures as limiting or blocking websites in the workplace, preventing personal email and social media downloads, and blocking file sharing. In addition, in sensitive areas this layer of defense may restrict removable media and personal device usage such as phones, cameras, and more.

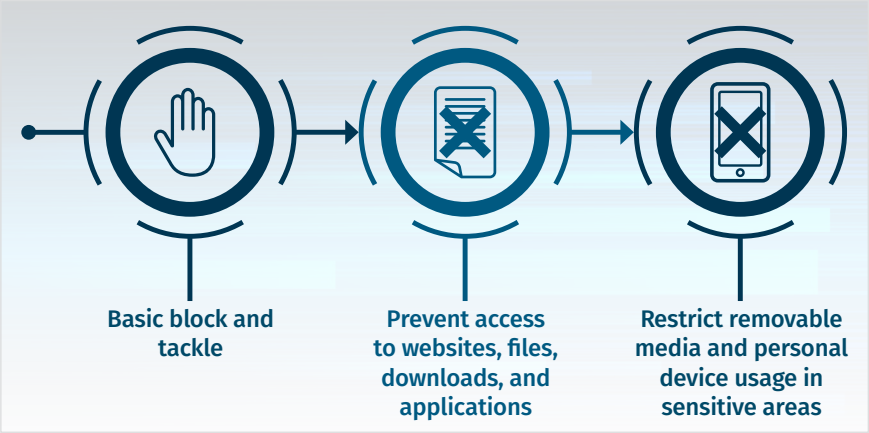

Figure 3. The Block and Tackle Approach

A second layer may involve more advanced technology. At this layer, you first want to create digital profiles or fingerprints for all users. This profile will track all user actions as defined by the organization (for example, key presses/logging, how users leverage their devices, and what users commonly access on systems). Organizations need advanced tools and software that work behind the scenes without burdening the user. You must respect and protect employee privacy while also trying to secure your organization. To maintain privacy and protect against threats, the software should use metadata as much as possible to identify users and encrypt and protect these profiles. As always, thoroughly test before implementation.

The third layer employs the right people as your defense: your security team. You must train your team to use the technology implemented in your organization and to look for anomalies. If you do not know normal, you will find it difficult to recognize abnormal. Your team needs proper education, training, and motivation. Figure 4 provides tips for a security team to remain diligent and successful against insider threats.

When employees leave the company, remove all their access from systems to which they previously had access. Remote access after an employee exits represents a huge (and common) risk. Provide access only where needed.

Figure 4. Defensive Tips for Security Teams

Consider employees an extension of your security team. When something seems "off," how do employees report it? You want this method in place and to take it seriously. Specify how employees should report security issues, and identify who manages these submissions. Define the required actions. Implement protections for employees who report an insider threat.

Implement a reporting policy that protects the employee coming forward with potential insider information. Always treat tips as a threat and investigate them.

Figure 5 summarizes the best security defenses that you can implement within your organization to protect against breaches. With all these layers, organizations must consider their security stack efficiencies to prevent bulky or resource-intensive programs or applications running on devices and machines that may impact employee daily functions.

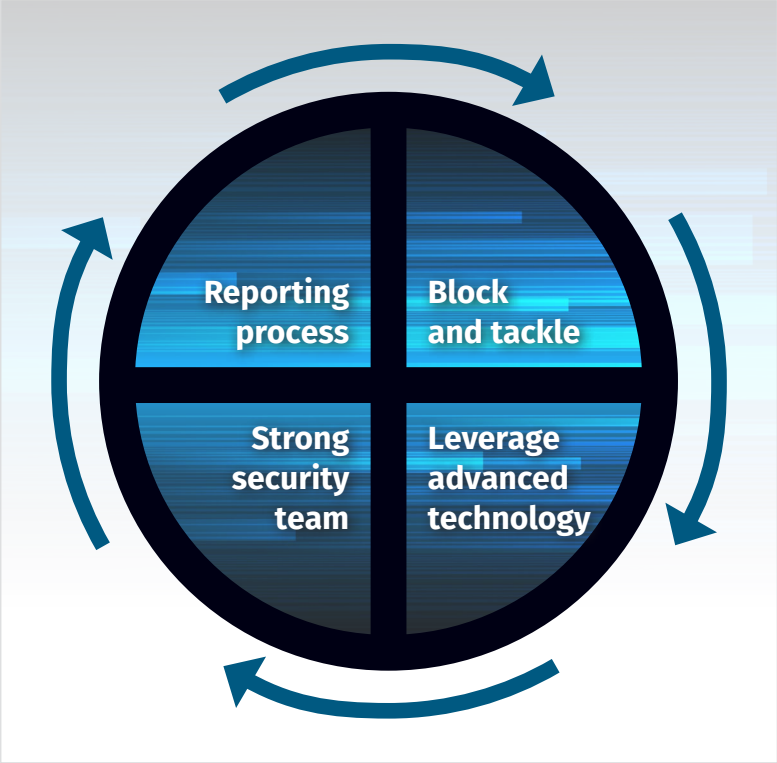

Figure 5. The Layer Defense Summary

A LESSON LEARNED

In 2018, Elon Musk and Tesla fell victim to an insider threat. An employee wanted revenge for not receiving a pay raise, so he sabotaged the company.[7] Good defense layers would have likely helped stop this insider who sabotaged Tesla's code.

Nevertheless, it appears that Tesla learned from the experience. In 2018, the company might not have had a strong reporting system, but by 2020 things seem to have changed. An employee reported and effectively stopped a potential ransomware attack against Tesla. Tesla must have implemented a solid security team who takes reports seriously and acts to protect their organization.[8]

TAKEAWAY

Organizations want solutions that are compact (not intrusive) and configurable to meet the needs of the company while maintaining employee privacy.

[7] "Insider Threat Becomes Reality for Elon Musk," CSO, www.csoonline.com/article/3284444/insider-threat-becomes-reality-for-elon-musk.html

[8] "A Tesla Employee Thwarted an Alleged Ransomware Plot," Wired, www.wired.com/story/tesla-ransomware-insider-hack-attempt

Conclusion

Machine learning and artificial intelligence are excellent defenses against insider threats and risks. Human involvement in the form of a security team should be augmented by AI-based tools that aim to halt threats before they cross the threshold of your organization. Software exists that can digitally fingerprint users using low-burden passive biometrics. You can leverage baseline analytics to detect abnormal behavior and deploy a security hurdle.

This paper examined the similarities and differences between insider threats and risks, provided examples of how attacks can happen to the largest and smallest of organizations, and discussed how to create a strong defense to protect your organization. Combating such problems remains an ongoing and formidable task for defenders. Commercial solutions can amplify the power behind prevention and detection. Understanding the problem, the threat, and implementing defense policies *before* something happens is key. Your goal is to know what normal looks like so that you can defend against abnormal.

Insider Attacks Prevention Checklist

1. Understand the attacks and educate your company. Insider threats and insider risks are two different attacks, yet both can cause major breaches in seconds.
   - ☐ Implement a plan to report insider threats and act on them. All tips should be taken seriously.
2. Form a first line of defense against insider threats/risks.
   - ☐ Hire the right defenders. Make sure they understand the risks, are trained properly, and are qualified for their position and responsibilities.
   - ☐ Implement AI-based technology to aid in first-line detection.
   - ☐ Implement biometrics and authentication programs that detect abnormalities and halt activity.
   - ☐ Train your defenders and any outsourced companies on the proper configurations and usage of your defense solutions.
3. Protect your organization when employees leave the company.
   - ☐ Immediately remove employee access upon departure or termination.
     - ☐ Workstations
     - ☐ Network access and shares (remember cloud storage)
     - ☐ Building access
   - ☐ Move old files to a new location if you must preserve them. Otherwise, wipe them from the workstation.
   - ☐ Ensure that workstations remain offline.

About the Author

Heather Mahalik is a SANS senior instructor and course lead for FOR585: Smartphone Forensic Analysis In-Depth. As the senior director of digital intelligence at Cellebrite, Heather focuses on forensic research and making the community smarter on all aspects of digital intelligence. Her background in digital forensics and e-discovery covers smartphone, mobile device, and Mac and Windows forensics, including acquisition, analysis, advanced exploitation, vulnerability discovery, malware analysis, application reverse-engineering, and manual decoding. Prior to joining Cellebrite, Heather focused on mobile device forensics in support of the U.S. federal government and served as a technical lead performing forensic examinations for high-profile cases. Heather maintains www.smarterforensics.com, where she blogs and shares presentations.

Sponsor

SANS would like to thank this paper's sponsor:

BlackBerry®