January 16, 2023

Insider Threats

What is an insider threat?

An insider threat is the result of potential and motivation for an insider to use their access or knowledge of an organization to cause harm to that organization (CISA). An insider threat can be a consequence of a disgruntled employee, a stressful work environment, or negligence by the organization (SEI Insider Threat Report, 2008).

Why are insider threats a risk?

Insider threats are among the most challenging attacks to detect and prevent. According to researchers, a quarter of all cyberattacks are committed by insiders and nearly a third of these attacks cause more severe damage than attacks committed by outsiders (Homoliak, Cornell U.). Identifying insider threats is challenging because of the human factor involved; humans are unpredictable, and although there are indicators of an insider likely to exploit their organization, these indicators are not present in every case.

Managing insider threats

Insider threats can be difficult to mitigate; it requires finding a balance of trust involved that can make or break the security infrastructure of an organization. Since the dawn of the internet and the need for digital security, organizations have implemented a “castle-and-moat” approach to cybersecurity, which consists of securing their networks from outside threats, like a moat, at the cost of leaving the door open for threats from inside their networks (Parde, MIT). According to CrowdStrike and IBM – two of the world's leaders in information security – a better, more comprehensive approach to mitigating threats from inside and outside a network is a “zero-trust” model. A zero-trust model consists of treating insiders and outsiders as one in the same; this means that an employee does not have access to the entire network simply because they are an employee and that everyone, including employees, is authenticated any time they access the network (Raina, CrowdStrike). In short, employees are only granted access to the parts of the network that are essential to their work and are treated as outsiders with few-to-no exceptions. There is rarely a “one size fits all” solution to any aspect of information security, but with respect to mitigating insider threats, implementing a zero-trust model is crucial.

Components of a zero-trust architecture

There are certain things that need to be considered when implementing a zero-trust security architecture regardless of the organization. According to the CISA, these considerations include:

1. The person of concern
2. The victim/target
3. The environment
4. The pre-involvement of law enforcement

Preventing and responding to insider threats based on a zero-trust architecture

The Person of Concern

Identifying an insider with the motivation and knowledge to carry out an attack is often the most difficult aspect of mitigating insider threats. There are three major situations that lead to the majority of insider threats: a disgruntled employee, a stressful work environment, or negligence by the organization (SEI).

An employee can become malicious towards his/her organization for a variety of different reasons ranging from personal situations, such as a divorce or financial troubles, to a direct conflict within the organization, such as a denied raise or promotion (SEI). Identifying employees with these motivations is difficult alone, but this becomes even more difficult in organizations with large amounts of employees. When feasible, every individual, especially those with access to sensitive data or networks, should be closely monitored in the work environment and outside of the office. According to the CISA, this monitoring should be looking for these key indicators:

- *Personal indicators*: "a combination of predisposition attributes and personal stressors currently impacting the insider." Personal indicators would appear primarily outside of the workplace, but some aspects could carry over to the office.
- *Background Indicators*: "events that happen before an individual is hired by an organization or before an individual obtains network organizational access." A comprehensive background check, interviews with former employers, friends and family members, would be the ideal way to identify background indicators.
- *Behavioral Indicators*: "actions directly observable by peers, HR personnel, supervisors, and technology." Close supervision is critical to identify behavioral indicators. Humans are unpredictable, but we tend to establish baselines for our behavior in which people deviate from when conducting an attack.
- *Technical Indicators*: "network and host activity." Technical indicators would include accessing remote servers for seemingly no reason, visiting sites known to harbor criminal activity, accessing files and documents without permission, or downloading files and documents without permission that include sensitive information and are not crucial to the employee's work. Identifying technical indicators of an insider threat requires the direct implementation of security software and hardware on an employee's workstation and the network at large.
- *Organizational/Environmental Indicators*: organizational policies and factors that "can escalate or mitigate behavioral changes in an individual's progression from trusted to insider threat." In most cases, organizational/environmental indicators can be identified

through disobedience or "bending the rules" to download files/documents or access sensitive information.
- *Violence Indicators*: "specific behaviors or collections of behaviors that can instill fear or generate a concern that a person might act." Violence indicators are often obvious and relate to a superiority complex or urge for increased control; these include harassment, intimidation, and bullying.

These indicators are not the only indicators of potential insider threats. Ultimately, the indicators will likely be unique to the situation, insider, or organization in question. As such, the best mitigation strategy for preventing insider threats is to listen to your intuition. A person or team's "gut feeling" can be a powerful tool. It is always best to air on the side of caution – if something "feels off," seems suspicious, or is out of the ordinary, it is always worth checking out.

The Victim/Target

An organization's risk management strategy should ultimately reflect the sensitivity of the information it holds or service it provides. Former cybercriminal and ex-U.S. most wanted criminal Brett Johnson has provided his expertise in the way that cyberattacks are motivated by three key factors: financial gain, hacktivism, or pride. Based on Johnson's expertise, it becomes clear that organizations with large amounts of money, provide controversial services, or are internationally well-known and trusted, are the most likely to be targeted by cybercriminals. Organizations that fall into this category include financial institutions (banks, credit bureaus, etc.), non-profits tied up in politics, critical infrastructure, or nation state affiliated agencies/organizations. There are alarming, but important, statistics that have been gathered regarding these issues:

- In 2021, financial industry organizations reported 703 cyberattack attempts per week (Fairchok).
- As of 2016, there were 80 different hacktivism groups active around the world (Fowler).
- Governments are the most targeted sector since 2020 (Konkel).

Organizations that fall into these criteria should place an extreme emphasis on securing their systems from insider threats. Any organization that processes credit cards, personal identifiable information (PII), or similar data should have a strong emphasis on digital security as well, as these institutions can fall under multiple criteria.

The Environment

A hostile work environment facilitates more issues in that environment. This principle also applies to cybercrime; an employee that does not respect or is angry with his or her superiors is more likely to commit a crime intended to harm that organization. To address this reality, organizations should:

- Promote a healthy working environment. This includes reasonable pay, honest consideration for promotions, addressing employee concerns, and general respect in the workplace.
- Promote a work-life balance. Work-life balance is often overlooked in organizations, which leads to employees feeling unheard, disrespected, and not valued. Offering a reasonable number of sick days, vacation days, and being reasonably flexible with requests for these arrangements is key to maintaining a healthy work-life balance among employees.

Maintaining a healthy work environment is crucial to keeping employees on good terms with the organization, but it is also important to consider pre-disposed motivations for insider threats and to implement proper security practices to manage these vulnerabilities. These security practices should ensure a secure environment for sensitive information and systems while balancing the needs of the organization against the sensitivity of that information. Additionally, especially for large organizations, the security practices for one department or group of people does not necessarily need to be the same among all. This practice requires reasonable access control by the organization's information security teams and should *at a minimum* include:

- Multi-factor authentication: MFA, when implemented correctly, can easily balance the needs of employees while maintaining a good security posture with respect to outside sources in addition to restricting the ability for an insider to gain unauthorized access to an area or system with sensitive information.
- Physical security: employees, obviously, need access to the building where they work – but this does not mean they need access to all areas of that building. Using biometric scanners, RFID/NFA cards, or keycode access points, an organization can section off areas of the office and allow access only to those who require it. This mitigates the risk of, for example, a disgruntled employee sneaking into the datacenter to steal credentials of other employees.
- Network security: in the same concept of physical security, organizations should implement a zero-trust policy (see previous section). Organizations can additionally utilize network monitoring tools and services to surveil the movements of employees across the network(s).

It is important, however, that these security measures be implemented at a level of risk that suits the organization. Employees become frustrated when there is "too much" security, or if it is "annoying" to perform MFA in places where it is not necessary, and such annoyance could lead to an insider threat by upsetting an employee and promoting a bad relationship among him/her and his/her superiors.

Pre-Involvement of Law Enforcement

Establishing and maintaining a positive relationship with local and federal law enforcement in the area is important to ensure the proper steps can be taken if there is a threat to the

organization. Law enforcement agencies can also provide tips and services to help organizations boost their security posture.

It is important to establish a relationship with law enforcement *before* an incident occurs. This ensures that the law enforcement agency/agencies can respond effectively to the department or person needed and that a connection has already been established with this person. It is equally important that these connections be made prior to an incident to make sure the proper channels and procedures are established, and proper protocols are in place to respond effectively. This is especially important for instances of insider attacks – these attacks are often extremely time sensitive – insiders can use their advanced knowledge of the organization to move more quickly and efficiently in their malicious actions.

Bibliography

"Defining Insider Threats." Cybersecurity and Infrastructure Security Agency CISA. Accessed January 16, 2023. https://www.cisa.gov/defining-insider-threats.

Fairchok, Sherry. "Spike in Destructive Attacks, Ransomware Boosts Banks' Cybersecurity Spending in 2022." Insider Intelligence. Insider Intelligence, May 3, 2022. https://www.insiderintelligence.com/content/spike-destructive-attacks-ransomware-boosts-banks-cybersecurity-spending-2022.

Fowler, Kevvie, Curtis Rose, and Matthew Limbert. *Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not*. Cambridge, MA: Syngress, 2016.

Homoliak, Ivan, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martin Ochoa. "Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures." arXiv.com. Cornell University, September 2017. https://arxiv.org/pdf/1805.01612.pdf.

Konkel, Frank. "Microsoft: Government Most Targeted Sector by Hackers in Past Year." Nextgov.com. Nextgov, October 8, 2021. https://www.nextgov.com/cybersecurity/2021/10/microsoft-government-most-targeted-sector-hackers-past-year/185968/.

Moore, Andrew P, Dawn M Cappelli, and Randall F Trzeciak. Tech. SEI Insider Threat Report: *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*. Software Engineering Institute. Pittsburgh, PA: Carnegie Mellon University, 2008.

Parde, Nathan. "Zero-Trust Architecture May Hold the Answer to Cybersecurity Insider Threats." MIT News. Massachusetts Institute of Technology, May 17, 2022. https://news.mit.edu/2022/zero-trust-architecture-may-hold-answer-cybersecurity-insider-threats-0517.

Raina, Kapil. "What Is Zero Trust Security? Principles of the Zero Trust Model." CrowdStrike, October 17, 2022. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/.