ISACA

A Holistic Approach to Mitigating Harm from Insider Threats

Security

CONTENTS

4 **Introduction**

4 **What Is an Insider Threat?**

4 / What Is a Security Program?

5 / What Is an Insider Threat?

6 **Who Are the Insiders?**

6 / Malicious vs. Malignant Insider Threats

7 / Outsiders Become Insiders

7 / MICE—What Turns a Good Insider Bad

8 / Insiders to Worry About

8 / Well-Meaning Employees

9 / Malicious Employees

9 / Contractors

9 / Vendors

10 / Support Contractors

10 / Customers

10 **Tesla—An Iconic Example**

11 **A New Approach**

11 / User-Initiated Loss

12 **Human Security Engineering**

12 / Removing the Insider From the Process

12 / Creating a User Environment That Mitigates Opportunities

13 / Anticipating and Mitigating User-Initiated Loss

13 **Conclusion**

14 **Acknowledgments**

ABSTRACT

All enterprises face potential losses due to insider threats, whether the threat actors are malicious or otherwise. This white paper delves into where insider threats come from, how to anticipate them and the psychology behind them. In this ISACA white paper, learn about new insights that your enterprise can use to anticipate and assess insider threats and mitigation tactics to reduce the associated risk.

Introduction

The term insider threat may bring to mind the image of a bitter disgruntled employee who wants to exact revenge on the enterprise. A classic example of an insider threat is the character Dennis Nedry[1] in the movie *Jurassic Park*, a system administrator who sabotages systems so that he can steal information and sell it to a competitor. Fans of Harry Potter films might consider the Voldemort supporters who infiltrated the Ministry of Magic[2] as insider threats.

Movies also often depict whistleblowers to be a form of insider threat—heroes overcoming evil corporate practices and divulging information that saves the world from a variety of evils. The whistleblowers figure out a way to subvert the best protections and tightest security to free information for the greater good. The images are always dramatic.

The fortunate or unfortunate reality, depending on perspective, is that insider threats are rarely as interesting as the characters in books or movies. They are much more mundane and typically are not part of a high stakes cat-and-mouse game. This is a gift and a curse. Insider threats are not as sophisticated as often portrayed, but they can harm their targets through simple and common actions that are difficult to detect and mitigate.

This white paper provides an overview of insider threats and suggests a new paradigm for viewing and mitigating insider threats and related harmful user actions.

What Is an Insider Threat?

The implication of insider threats is that it is difficult to stop insiders who are truly clever and motivated; however, the reality is very different. Based on a wide variety of insider threat investigations, most revealed insiders who were apathetic or otherwise well meaning.

The implication of insider threats is that it is difficult to stop insiders who are truly clever and motivated; however, the reality is very different.

Although insiders may have worked at enterprises considered sophisticated, the tactics that they used were typically mundane and basic and did not rise to the level of genius. Indeed, some investigated insider threats involved Chinese intelligence agencies that recruited insiders[3, 4] or trusted employees who were sociopaths who offered their services to Cuban and Russian intelligence agencies in exchange for money.

To understand the insider threat, it is necessary to take a step back and consider what is a threat in general and evaluate how threats impact a security program.

What Is a Security Program?

By definition, security is being free from risk—but it is impossible to be free from risk. Even though a security professional's job is securing IT assets, it involves balancing potential loss with the requirement to provide access, with limited resources and policy and procedural constraints.

1 Fandom, "Dennis Nedry," Jurassic Wiki, https://jurassicpark.fandom.com/wiki/Dennis_Nedry
2 Fandom, "Fall of the Ministry of Magic," Harry Potter Wiki, https://harrypotter.fandom.com/wiki/Fall_of_the_Ministry_of_Magic
3 US Department of Justice, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technology Data for Years," 30 October 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal
4 Ratman, G.; "Report: Underground hackers and spies helped China steal jet secrets," *Roll Call*, 15 October 2019, https://www.rollcall.com/2019/10/15/report-underground-hackers-and-spies-helped-china-steal-jet-secrets/

Fundamentally, maximum risk exposure equates to the value of the enterprise. To a small extent, exposure incidents have harmed personal reputations of the people involved in exposed enterprises. The risk to the enterprise value is determined by vulnerabilities and threats. Vulnerabilities are the weaknesses that can be exploited. Threats are the entities that exploit vulnerabilities in a manner that can result in harm.

Fundamentally, maximum risk exposure equates to the value of the enterprise.

Without a vulnerability, a threat cannot put enterprise value at risk. Without a threat, a vulnerability cannot be exploited to create a loss. Threat and vulnerability are necessary to have risk.

Vulnerabilities can be technical, operational, physical or personnel-related in nature. Threat actors can exploit the vulnerabilities that best suit their needs and capabilities. For example, a group of cybercriminals based in Europe do not ordinarily exploit physical vulnerabilities in a South American enterprise.

Threats can be anything (e.g., object, substance or human) that is a potential cause of an unwanted incident. Regarding types of threats, natural disasters cause more harm than malicious individuals, short of launching weapons of mass destruction. Hurricanes and typhoons can devastate areas and seriously hamper computer operations. When a random power outage hits a particular location, enterprises can stop functioning. For example, in 2003, a tree fell and knocked out a power line, causing a chain reaction that resulted in a massive power outage in the northeastern United States. Fifty-million people and all the businesses in the region lost electricity.[5,6]

The human type of threat can be insiders or outsiders. They can be nation states or petty criminals. They can be well-meaning people or malicious actors. If they are ever in a position to initiate a loss, they are a threat.

To stop losses, it is necessary to implement countermeasures. Countermeasures are processes that directly reduce vulnerabilities or threats. At its most basic, the implementation of countermeasures constitutes a security program.

What Is an Insider Threat?

The reason for discussing risk management and security programs before delving into the insider threat is that it is important to strategically grasp why the insider threat is a unique concern.

Threats exploit vulnerabilities that match the access and capabilities of the threat. Unlike outsiders, insider threats have ready access to physical, technical, operational and personnel vulnerabilities. These threats also have permissions and assumed access that outsiders do not. Even in zero trust environments, enterprises provide insiders with some level of trusted access. Zero trust is limited to a technical environment—it does not address physical, operational or personnel vulnerabilities.

Unlike outsiders, insider threats have ready access to physical, technical, operational and personnel vulnerabilities.

Insiders have inherent knowledge about where enterprise value lies. If they want to cause harm, steal information, etc., they have an advantage in knowing exactly how to do it and an easier time executing their actions. More concerning is that even well-meaning insiders can unintentionally cause significant harm due to their access.

Insiders present a special risk to an enterprise and, therefore, require special effort to mitigate potential attacks.

[5] Minkel, J.; "The 2003 Northeast Blackout—Five Years Later," *Scientific American*, 13 August 2008, www.scientificamerican.com/article/2003-blackout-five-years-later/

[6] Electric Choice, "9 of the Worst Power Outages in United States History," www.electricchoice.com/blog/worst-power-outages-in-united-states-history/

Who Are the Insiders?

Although the concept of an insider might seem straightforward, its various motivations and the levels of damage that can be incurred make it a more complicated concept.

Malicious vs. Malignant Insider Threats

Many insider threats are not malicious. Any entity with the potential to cause harm, for any reason, is a threat. Well-intentioned people cause harm on a daily basis. Accidents happen.

For example, Reality Winner, a defense contractor with access to US National Security Agency (NSA) information, passed intelligence about Russian election interference to reporters at The Intercept. Her intent allegedly was not to commit espionage to benefit a hostile government, but rather to provide The Intercept with proof that the actions of the NSA were reasonable. Whatever the motive, intelligence was leaked to outsiders.[7]

Inefficient business practices/operations can cause a great amount of loss, and, regardless whether they involve people, need to be accounted for in risk management plans. It is necessary to consider all types of losses, regardless of the intent of the source of the loss.

An insider threat program needs to consider all sources of insider threat. Malignant threats are those threats that are unintentional. There is no motive, good or bad, for causing the losses associated with malignant threats.

Malignant threats are those threats that are unintentional. There is no motive, good or bad, for causing the losses associated with malignant threats.

Malignant threats are those threats that are endemic to enterprise operations. They are constant and likely greater in aggregate than the loss from a malicious insider that everyone fears. Hurricanes are not malicious, but they can cause more damage than terrorist attacks.

In enterprises, the accidental loss of a USB drive or laptop can be as harmful as the theft of a device. According to the "Verizon Data Breach Investigations Report", accidents—such as entering the wrong email address—are a major source of data breaches.[8]

Malicious insider threats are clear in their intent. They want to cause harm or potentially just gain benefits without regard to the impact on an enterprise. For example, an individual who wants to steal data for profit causes harm to an enterprise and its clients, but that is just an outcome of achieving the person's intent.

Malicious insider threats are clear in their intent. They want to cause harm or potentially just gain benefits without regard to the impact on an enterprise.

In one insider case, six competitors were bidding on a large assessment contract. The sales representative from one of the competitors accidentally clicked on "Reply all" in the email response to the solicitation and sent the firm's proposal, with pricing and strategy, to all bidders. This not only gave the other competitors an advantage in seeking the current contract, but also gave them a long-term advantage over the exposed bidder, in that they all could guess its pricing strategies, discounts, perceived competitive advantages, etc., on future competitive proposals.[9]

Although this case is an example of a malignant insider threat, it is worth considering whether it would matter if it were due to a malicious insider. Arguably, this malignant scenario is worse, because a malicious party likely would have shared the information with one competitor, not all of them. What is more important is that the incident likely

[7] Andone, D.; S. Sendik; "NSA leaker Reality Winner sentenced to more than 5 years in prison," CNN Politics, 23 August 2018, https://edition.cnn.com/2018/08/23/politics/reality-winner-nsa-leaker-sentenced/index.html
[8] Verizon, "2021 Data Breach Investigations Report," https://www.verizon.com/business/resources/reports/dbir/
[9] The author was a recipient of the email in this case.

resulted in the bidder's exclusion from the work, because the client saw that it was unable to adequately secure its own intellectual property.

Frequently, people discount the likelihood of insider threats because they do not believe that they will encounter an evildoer, and they rarely do. However, considering that malignant insider threats are common and frequent, it is wise to encourage action to address this type of threat. On a positive note, the countermeasures that stop malignant insider threats will generally stop malicious insider threats.

Outsiders Become Insiders

One critical aspect to consider is that outsiders generally become insiders. For example, phishing is a popular strategy for attackers because it allows an outsider to obtain insider credentials or exploit an insider's access. It is possible for a malicious outsider to compromise the credentials of the most loyal employee in an enterprise and take action using the employee's account.

The infamous Sony hacks in 2014[10] compromised administrator accounts. That situation is not unique—any legitimate account can present a malicious threat.

MICE—What Turns a Good Insider Bad

In general, malicious insiders do not usually start out with the intent to be malicious. The Computer Emergency Response Team at the Software Engineering Institute at Carnegie Mellon University, which performed extensive studies on insider threats, found that there was usually a significant emotional event (SEE)[11] that caused the insider to take malicious actions.

A SEE is some type of emotional trigger that prompts the insider to want to cause harm. Examples include traumas, such as a financial setback, being reprimanded at work, not getting a promotion and going through a divorce. The event triggers an action that the person may have been contemplating but would otherwise not have taken.

A SEE is some type of emotional trigger that prompts the insider to want to cause harm. Examples include traumas, such as a financial setback, being reprimanded at work, not getting a promotion and going through a divorce.

For example, Kevin Mallory, a former respected CIA operative[12] was more than $230,000 in debt and behind on his mortgage. When Chinese intelligence operatives approached him via LinkedIn, he agreed to provide them with top-secret intelligence, including the names of agency operatives, in exchange for money. His motive was to save his house and try to get out of debt, but he rationalized his behavior and convince himself that he was helping the United States by gathering information on Chinese intelligence methods.

Mallory is a stereotypic example of someone who did something that would have been unthinkable to him under other circumstances, but who somehow found a way to justify his actions to himself. In this case, he was not acting out of anger toward the United States and a desire for revenge, so he found another way to justify his behavior.

Rationalization is a critical issue for many malicious insiders. They will find some way to convince themselves that their actions are justified.

Frequently, the rationalization is evident in their language patterns. Common excuses that spies and criminals have offered during interviews[13] include the following:

- Insisted they did not steal information; they made a copy of it.
- Described felonies as a teenage hobby.
- Claimed if the information was as valuable as the enterprise claimed, the enterprise should have protected it better.

[10] VanDerWerff, E.; T. Lee; "The 2014 Sony hacks, explained," Vox, 3 June 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea
[11] Collins, M.; M. Theis; R. Trzeciak; J. Strozer; J. Clark; D. Costa; T. Cassidy; M. Albrethsen; A. Moore; "Common Sense Guide to Mitigating Insider Threats," 5th Edition, Carnegie Mellon University Software Engineering Institute, December 2016, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484738
[12] Dilanian, K.; "How a $230,000 debt and a LinkedIn message led an ex-CIA officer to spy for China," NBC News, 4 April 2019, www.nbcnews.com/politics/national-security/how-230-000-debt-linkedin-message-led-ex-cia-officer-n990691
[13] The author of this paper conducted this research as background for Winkler, I.; *Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day,* Wiley, USA, 2005.

- Argued that if the enterprise had paid them better, they would not have needed to supplement their income.
- Claimed that because they created the information, they really did not steal it.

For many, there is always a justifiable reason for the crime.

Human intelligence operatives, aka spies, use the acronym MICE (money, ideology, coercion and ego) to identify the people they recruit to spy against their own countries. This term applies to people who are susceptible to manipulation. Generally, people unilaterally choose to harm their enterprise and become a malicious insider for the same following reasons.

- **Money** is the need or desire for financial gain. Employees might have a critical need for money or perhaps a strong desire for more money than they are making. They may rationalize that an enterprise is not paying them enough.
- **Ideology** refers to a political or ethical reason for employees betraying their enterprise. Some people become disillusioned. Some become whistleblowers when they find corrupt practices. In some cases, people involved with foreign intelligence operations may realize that their efforts are not actually supporting their country but are furthering the goals of predatory individuals running the operation. Their disillusionment may turn into a willingness to support another country.
- **Coercion** is essentially blackmail. A person may be compromised because of a situation that may cause embarrassment or other harm. For example, when someone gives a spy compromising information, the spy can then use that information as a threat, by saying, "Unless you continue to give me information, I will disclose that you gave me information in the past." For a target who wants to escape exposure, this is a point of no return.
- **Ego** refers to a person becoming a malicious insider due to perceived unfair treatment. The individual may be upset over not getting a promotion or not getting sufficient respect. The person may feel held back from advancement. Any potential slight can be justification to harm the enterprise.

Although these are distinct categories, motivations are usually more complicated. Any person who commits some form of unethical act will likely claim an ideological reason. The claim of a moral reason often carries over to whistleblowers.

A whistleblower is "one who reveals something covert or who informs against another."[14] Although whistleblowers may be afforded legal protections from retaliation, such as employment termination, research indicates that, in some cases, established processes were not followed—which, in turn, calls into question the real motivation for raising the alleged employer wrongdoing.

Insiders to Worry About

There are reasons to worry about all insiders, but listing them by type is helpful to understand which people represent a significant threat and determine where to focus prevention and mitigation efforts.

Well-Meaning Employees

Well-meaning employees are trusted insiders. They never intentionally harm the enterprise. However, they are a malignant threat who inadvertently may cause harm in the course of normal business operations. Accidents happen. Sometimes, employees are just one part of an inefficient process.

Well-meaning employees are trusted insiders. They never intentionally harm the enterprise. However, they are a malignant threat who inadvertently may cause harm in the course of normal business operations.

This category is not specific to particular employees. It includes all well-meaning people with insider access. While it is true that nonemployees, such as contractors and volunteers, may have less loyalty to an enterprise, they are typically as reliable and trustworthy as employees. Whatever their status, well-meaning individuals who have the necessary access present the greatest source of losses that an enterprise typically experiences.

[14] Merriam-Webster, "whistleblower," www.merriam-webster.com/dictionary/whistleblower

Malicious Employees

Although well-meaning employees might be the source of the greatest losses of an enterprise, that is only because they occupy a significantly greater proportion of the general population. Only one-to-four percent of people have antisocial personality disorder, according to estimates, and might be considered sociopaths or psychopaths.[15] These are people who might intentionally cause harm if given the opportunity. They do not think like most people. They are often very intelligent, and they generally lack empathy.[16] If they come across an opportunity to benefit, whether it is at the expense of an enterprise or not, and if they calculate that they may get away with it, they may cause harm.

Unfortunately, there are also the otherwise ethical people who experience a SEE and intend to make amends later. They may take money for medical care or another critical need. It is for this reason that the US intelligence community, for example, tracks the financial status of people with clearances.

Contractors

Contractors often have access to enterprise data—in many cases, the same access as employees. Contractors are frequently trusted with critical access like employees. In many cases, contractors may have more access than employees. For example, many enterprises use contractors to support their IT infrastructure. A system administrator has access to all the information inside an enterprise, and, if the administrator role is performed by an outside contractor, that contractor has critical access.

Although a contractor may be more trustworthy than many employees, there may be competing concerns and loyalties. For example, budget information can indicate whether an enterprise is willing and able to raise the rates it pays to contractors. If an enterprise wants to replace a contractor, the enterprise might entail more risk than when replacing a regular employee, because the enterprise typically has less control over the systems and data in the contractor's possession. Minimally, a contractor likely does not have the same loyalty to an enterprise as a regular employee, given the lack of benefits.

If an enterprise wants to replace a contractor, the enterprise might entail more risk than when replacing a regular employee, because the enterprise typically has less control over the systems and data in the contractor's possession.

Vendors

Vendors are suppliers that can provide products or services to an enterprise. The risk they present depends on the purpose they serve and the access provided to them. Vendors can have partial or complete access to various parts of an enterprise infrastructure. Although some vendors may intentionally target an enterprise, the concern typically focuses on the possibility that a vendor may employ a rogue individual who has access to enterprise information or other resources.

Although it is not impossible for a vendor to leverage its access to an enterprise to compromise the enterprise, the more critical concern is that a malicious outsider will view the vendors of an enterprise like an extension of its operations. The vendors can unintentionally provide a back door into an enterprise. For example, the 2013 Target hack began when an intruder sent a phishing message to a vendor and then used stolen credentials to access a vendor network, which was a conduit to the Target business network.[17]

Although it is not impossible for a vendor to leverage its access to an enterprise to compromise the enterprise, the more critical concern is that a malicious outsider will view the vendors of an enterprise like an extension of its operations.

[15] Holland, K.; reviewed by T. Legg; "What Is a High-Functioning Sociopath?," Healthline, 28 May 2019, www.healthline.com/health/mental-health/high-functioning-sociopath
[16] *Ibid.*
[17] Krebs, B.; "Target Hackers Broke in Via HVAC Company," KrebsonSecurity, 5 February 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Support Contractors

Support contractors occupy a unique category. They are people who provide a service that the enterprise does not consider a core competency. For example, most enterprises outsource their cleaning services, IT support and automobile fleet maintenance. These workers frequently go unnoticed.

It is not impossible for criminals to intentionally get jobs inside an enterprise that they are targeting. In *2600: The Hackers Quarterly*, a hacker wrote about penetrating a targeted enterprise by obtaining a job at the cleaning service that it used. The cleaning service was always in need of employees and carried out no background checks. After inside the enterprise, the hacker obtained computer access and stole information.[18]

Customers

While vendors and contractors often are critical to enterprise functions, customers are even more critical. Depending on the industry, customers may have access to business functions, and their behavior may result in losses. To a certain extent, enterprise customers can influence the way it conducts business. Consider the following incident:

An oil enterprise employee reported a coworker for unusual activity. Telephone records revealed that the coworker was calling a known intelligence operative at a foreign consulate on a regular basis. The security team found that the enterprise was negotiating drilling rights with that country, and, during the negotiations, its representative told enterprise officials that it would be a sign of good faith if the enterprise hired 30 recent college graduates. The enterprise negotiators readily agreed. The employee in question was one of the 30 hires. The enterprise wanted to determine how to identify potential concerns with the other 29 employees.

It appeared that the foreign country was trying to determine the enterprise's estimate of the size of its oil reserves. The country also wanted to obtain any technologies that it could provide to enterprises within the country. Although this is an extreme case of a customer spying on an enterprise, situations like this can occur at a variety of levels in customer and vendor relationships. Adversarial dynamics are common in business relationships.[19]

Tesla—An Iconic Example

There are countless cases of insiders gone rogue. Martin Tripp, a disgruntled Tesla employee, is a prime example. Tripp worked at the Tesla Nevada Gigafactory, which manufactured batteries. He was hired as a process technician and was apparently upset at being reassigned to another position, according to allegations made by Tesla CEO Elon Musk and in legal filings.

Tripp apparently started a fairly complex scheme to exact his revenge. He began to modify the Tesla computing environment to periodically extract gigabytes of valuable Tesla information. The exfiltrated information included Tesla financials, details for the process of manufacturing the batteries for the Tesla Model 3, and details about the raw materials involved in the manufacturing process. Tripp also took photographs and videos of the factory that indicated that Tesla was wasting a great deal of material.

In court filings, Tripp indicated that he worked with a short seller of stocks, and that the leak of the information that he stole was expected to drive down Tesla stock prices. To settle the case, Tripp paid Tesla $400,000.[20]

[18] Referenced material as originally published is no longer available online (see https://store.2600.com/collections/back-issues). Subject matter is also referenced in *Corporate Espionage* (Prima, 1997) and *Spies Among Us* (Wiley, 2005).
[19] The author was hired by the impacted enterprise to assist in the investigation and mitigation efforts.
[20] Hawkins, A.; "Tesla whistleblower Martin Tripp ordered to pay $400,000 to settle hacking case," The Verge, 1 December 2020, www.theverge.com/2020/12/1/21755428/tesla-martin-tripp-settlement-whistleblower-hacing-amount

Perhaps one of Tripp's most nefarious actions was placing the malicious software that he wrote onto coworkers' computers. That action suggested that Tripp was attempting to frame his former coworkers for his actions.

This case is an example of typical insider threat psychology at work. Tripp became upset at being reassigned from a job he apparently liked. He then became determined to exact revenge, because of the perceived insult to him. It appears that Tripp then devised a plan to make money by collaborating with someone who would benefit from a downturn in Tesla stock prices. Tripp then worked to disclose an inefficient business practice. Instead of acknowledging that he wanted revenge (for an attack on his ego) and wanted to profit from it in the process (money), he claimed he was a whistleblower attempting to disclose information Tesla had been hiding from the public. He offered no justification for attempting to frame his coworkers.

A New Approach

When enterprises consider losses from insider threats, the motivation for the action is irrelevant. Stopping malicious insiders is not enough. Well-meaning insiders can be even more harmful than malicious insiders. Further, well-meaning insiders can have their credentials compromised by outsiders.

To mitigate the insider threat, it is necessary to discount motivation. It is important to consider whether actions themselves are potentially harmful rather than to focus on the individuals carrying out the actions.

To mitigate the insider threat, it is necessary to discount motivation. It is important to consider whether actions themselves are potentially harmful rather than to focus on the individuals carrying out the actions.

User-Initiated Loss

Perhaps the biggest consideration when addressing insider threat is how to understand a user's part in an incident. Strategically, it is helpful to think of the user's action as user-initiated loss (UIL). There are several reasons for making the distinction between user and action.

The word user is self-explanatory. The user is pivotal in the insider threat. The word initiated is used very intentionally. Specifically, a user does not directly cause a loss. The user initiates the action that results in the loss. Just because a user takes an action, it does not mean that loss should inevitably result. For example, just because a user clicks on ransomware in a phishing message, that does not mean ransomware should load onto the user's system. Other safeguards should be in place. The user should not have permission to install software. The system should have effective antimalware. The user does not personally encrypt each bit of a hard drive; the operating system does that.

Many people who focus on security awareness imply that a potentially harmful user action is due to error or lack of awareness. Whether there is lack of awareness or error does not matter. Harm is harm, and the same actions that result from malice may also result from error. Therefore, when countering the insider threat, it is important to take away implications of motivation and to phrase the problem in a manner that acknowledges ways to mitigate losses before they are realized.

To mitigate the insider threat, it is important to remove preconceived notions about intent or possible damage. It is more effective to focus on mitigating UIL and to emphasize that the loss can be stopped before it is realized.

Human Security Engineering

Considering the insider threat from a systems perspective involves focusing on the proximity of the error. When there is a software bug, a good software engineer does not focus solely on the error in the line of code but considers how the line of code came to be, and how the software programming process could have been improved to proactively remove the error. The engineer considers how software testing could have been improved to find the bug before it made it into production, and how the entire system might be made more resilient to proactively account for a software bug.

When examining the relationship between a human action and potential harm, it is necessary to consider why the harm was allowed to come into being:

- Why was the system designed to facilitate the harm?
- What processes could have mitigated the harm?
- Why did the system fail to stop the inevitable initiation of that harm?

The process of writing better software systems is intrinsic to the software engineering discipline. The process of proactively accounting for the insider threat is human security engineering. Human security engineering is a process that proactively accounts for and mitigates UIL.[21]

Removing the Insider From the Process

Perhaps one of the most effective methods to mitigate UIL and the insider threat as a whole is to remove the user from the process. Insiders cannot create damage, malicious or malignant, if they are not in a position to do so. Reengineering a process to remove the insider can mitigate loss.

Removing the user can be accomplished through a variety of means. One approach is to automate a process. For example, many applications replace cashiers and salesclerks, removing the possibility of accidental errors or theft in processing financial transactions. The use of mapping apps to provide directions not only greatly reduces the likelihood of misrouting rides, but also removes the possibility of taxi drivers intentionally taking longer routes to run up fares.

Machine learning and artificial intelligence allow automation of a variety of functions to remove opportunities for errors and allow more accuracy. For example, in cybersecurity automation, machine learning provides a more accurate and reliable method for identifying potential security incidents buried in gigabytes of log data.

Creating a User Environment That Mitigates Opportunities

It is impossible to mitigate insider threats out of all functions. Therefore, it is necessary to find other ways to reduce the risk that an insider may pose. One method is to reduce data access by limiting individual permissions to sensitive data. When access is limited, the compromise of data becomes less likely simply because fewer people are in a position to compromise that data.

Likewise, consider the damage that phishing and ransomware cause. Email filters prevent phishing messages from getting to an insider. An insider who does not receive a phishing message cannot launch ransomware or otherwise fall for its pretext.

The tighter the controls around the insider, the less opportunity there is for the insider to create loss of any type. The controls can be technical, operational or physical. An insider does not have to have unlimited access. To the extent possible, everyone should have least privilege.

[21] See also Winkler, I.; T. Brown; *You Can Stop Stupid*, Wiley, USA, 2021.

Anticipating and Mitigating User-Initiated Loss

Despite the best efforts of an enterprise, an insider will initiate some sort of loss. Users make errors. Users may be malicious. Accidents happen. There likely will be a lack of awareness in some respects. These circumstances are expected and should be planned for.

Cybersecurity is not unique in having to meet the insider threat challenge. Accounting has long learned to deal with the insider threat, proactively and reactively. Safety professionals know to deal with user errors and the expectation of injuries. This is not to say that these and other disciplines completely eliminated losses, but many have learned to build in protocols to mitigate UIL proactively and reactively.

It is necessary to proactively consider, from a cybersecurity perspective, what loss a user (or another insider) can initiate. What are the actions an insider can take, and what chain of events might a user initialize? For example, if a user clicks on a phishing message, the phishing message might cause ransomware to execute. However, that ransomware can execute only if a user has permission to install software. Antimalware can be installed proactively to prevent ransomware from loading.

Technology is critical to prevent, detect and respond to insider threats. Data leak prevention software stops the loss of data regardless of user intent. Behavioral analytics can be valuable in detecting misuse and abuse of accounts or systems due to any motivation. All technical countermeasures have potential usefulness in mitigating the insider threat.

Although these observations may seem simplistic, they offer a starting place for understanding how to view the actions that insiders initiate and how to begin implementing the countermeasures that naturally present themselves. It should never be a surprise when insiders take actions that can start a chain of events that may result in harm.

Conclusion

The insider threat is inevitable. It is impossible to stop malicious entities from existing. Even if it were possible, it would solve just a small part of the problem, because malignant insider threats are the greatest source of loss. Despite the massive potential of the losses, whether arising from malicious motivation, they can largely be anticipated.

Through anticipation of user-initiated losses, they can be proactively mitigated. The application of human security engineering principles reduces the likelihood of users being in a position to initiate a loss. Proactively anticipating the inevitability that other countermeasures will fail makes it possible to mitigate insider threats in whatever form they take.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Ira Winkler
CISSP
President, Secure Mentem, USA

Expert Reviewers

Vilius Benetis
NRD Cyber Security, Lithuania

Donald Carpenter
CISM, Security +, ITIL
USA

Michael Gioia
CISM, CDPSE, CISSP, PCIP, GSLC
Bentley University, USA

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP (Cyber)
BRM Advisory, Australia

Board of Directors

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, USA

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

John De Santis
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE
Chief Information Security Officer, UNOPS, Denmark

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC
Chief Executive Officer, introSight Ltd., Israel

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

DISCLAIMER

ISACA has designed and created *A Holistic Approach to Mitigating Harm From Insider Threats* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/insider-threats

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/