Improving Insider Threat Training, Awareness, and Mitigation Programs at Nuclear Facilities

Shannon Abbott[1]

Abstract

In recent years, insider threat programs have become an important aspect of nuclear security, and nuclear security training courses. However, many nuclear security insider threat programs fail to address the insider threat attack and monitoring potential that exists on information technology (IT) systems. This failure is critical because of the importance of information technology and networks in today's world. IT systems offer an opportunity to perpetrate dangerous insider attacks, but they also present an opportunity to monitor for them and prevent them. This paper suggests a number of best practices for monitoring and preventing insider attacks on IT systems, and proposes the development of a new IT insider threat tabletop that can be used to help train nuclear security practitioners on how best to implement IT insider threat prevention best practices. The development of IT insider threat best practices and a practical tabletop exercise will allow nuclear security practitioners to improve nuclear security trainings as it integrates a critical part of insider threat prevention into the broader nuclear security system.

Introduction

In recent years, insider threat mitigation programs have become increasingly important at nuclear facilities and more broadly. The nuclear security community has been working to develop insider threat mitigation programs, though they very seldom focus on mitigating threats to information technology (IT) systems despite the realization that cyber security at nuclear facilities is becoming increasingly important in an ever-connected world. Much like insiders can have critical knowledge that allows them to physically impact nuclear facilities, they also have the ability to impact the information technology systems at a nuclear facility, which can have disastrous impacts on the plant itself. In fact, one Chatham House report on cyber security at civil nuclear facilities noted that, "Cyber security training at nuclear facilities is often insufficient. In particular, there is a lack of integrated cyber security drills between nuclear plant personnel and cyber security personnel."[2]

While the IT insider threat has been somewhat neglected at nuclear facilities, researchers in the information technology field have devoted nearly two decades to understanding how to mitigate and prevent insiders threat attacks from occurring. Specifically, the Computer Emergency Response Team (CERT) and the Software Engineering Institute (SEI) have published *The CERT Guide to Insider Threats* which offers a comprehensive explanation of three types of insider

---

[1] Shannon Abbott is a nuclear security intern at Sandia National Laboratories and a Master of International Affairs candidate at the Bush School of Government and Public Service at Texas A&M University. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

[2] Caroline Baylon, Roger Brunt, and David Livingstone, "Cyber Security at Civil Nuclear Facilities," September 2015, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf, ix.

attacks (theft, sabotage, and fraud), as well as mitigation strategies. CERT insider threat programs are both well-known and well respected. Nearly two decades of knowledge and lessons learned can be leveraged to improve insider threat mitigation training programs at nuclear facilities on the whole system level. Insider threat cannot be done effectively without addressing how humans interface with IT systems, IT systems interface with security systems, and so forth. This paper aims to improve insider threat training programs as a whole and will do so by accomplishing two tasks: first to understand insider threat mitigation best practices within the information technology field that can be applied to nuclear facilities; and second, to develop the framework for a tabletop exercise that can be utilized to help employees to understand how to build a robust insider threat mitigation program—including information technology.

Insider Threat Best Practices

The CERT Guide to Insider Threats lays out three types of insider threats that can occur at nuclear facilities.

IT Sabotage

The first, insider IT sabotage is defined as, "insider incidents in which the insider uses information technology (IT) to direct specific harm at an organization or individual."[3] Additionally, they note that most insiders who commit an IT sabotage act did so due to disgruntlement and unmet expectations. This could mean that the employee did not receive an expected raise, had trouble with their supervisor, was transferred to a new department, had their access to resources changed, or other such precursors. In most cases in the CERT database, it seems that the saboteurs were about the be terminated from their positions.[4] Many disgruntlement issues can be avoided by the implementation of strong Human Reliability Programs (HRP) that encourage reporting strange behavior of colleagues. Because this can be a sensitive issue organizations should also consider implementing whistle-blower protections to prevent retribution for those reporting issues.[5] However, there are specific measures that organizations can take to prevent sabotage of their IT systems. Five such measures include carefully managing access paths, prioritizing IT alerts, targeted monitoring, securing the logs, and ensuring a secure backup process.

Managing Access Paths

In most organizations, when employees begin work they are allowed access to the IT system so they can access email and carry out any work functions necessary. For most employees access may be fairly basic—however, others, such as system administrations or some operators many need additional access to more information systems. One way to mitigate the insider threat is to

[3] Dawn Cappelli, Andrew Moore, and Randall Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)* (Upper Saddle River, NJ: Addison-Wesley, 2012), 23.

[4] Cappelli, Moore, and Trzeciak, 24.

[5] Cappelli, Moore, and Trzeciak, 23-35.

ensure that employees have no more access than necessary.[6] For example, an administrative assistant does not need to access any information systems necessary for operating the facility. However, one important aspect of ensuring that employees have no more access than necessary means ensuring that system administrators need to closely monitor what access accounts are created and who has access to the system through them. For example, it is important to monitor when accounts are created or ensure that there is a current list of who has access to shared accounts. When an employee is terminated, it is important to cut off all access paths that they had so they cannot commit an insider attack after leaving the organization. Additionally, monitoring access paths can prevent insiders from perpetrating an insider attack while they are still employed at a facility by disallowing them access to more IT systems than they need for their current position. For example, if a systems administration were to move to a facility operator position he would not still need access to the systems administrator accounts as well as the facility operation network. Ensuring that employees have the proper amount of access and former employees do not have any is an important step to mitigating the insider threat.

Prioritizing IT Alerts

It is not necessary to monitor every change in an organization's network or source code—this could cause an overload of work for employees. However, in system critical code or networks, organizations should use a configuration-management system that can track changes and begin an authorization chain for changes to critical systems.[7] This is beneficial for two reasons—first because it forces organizations to prioritize their assets and understand what is mission-critical. Second, it makes it considerably more difficult for an insider to change an important system that will cause a disaster at the facility.

Targeted Monitoring

Organizations should implement a system that allows it to monitor the activities their employees are performing on IT systems. While it is not practical for organizations to monitor the activities of every employee, it is both important and reasonable to collect logs such as [THESE LOGS]. However, logging a variety of activities allows organizations to more closely monitor the activities of employees who are showing signs of distress at work.[8] If an employee has come to the attention of Human Resources, they can monitor that employee's activity to ensure that they are not perpetrating an insider attack. However, in order to successfully carry out targeted monitoring the organization should have clearly documented policies for why they are doing additional monitoring, when that monitoring should begin and end, and what they are monitoring. It should all be done in accordance within the laws of the country or state in which a facility is located.

Securing the Logs

[6] Cappelli, Moore, and Trzeciak, 50-52.

[7] Cappelli, Moore, and Trzeciak, 53-54.

[8] Cappelli, Moore, and Trzeciak, 55.

Some IT-savvy insiders will take steps to cover their steps by altering or deleting the log files that are supposed to be monitoring their activities[9]. In order to prevent this from occurring, organizations should be sure to secure their logs and implement continuous logging to a secure log server. This will ensure that an insider is not able to alter the logs that may be able to detect them before the attack cures or implicate them later.

Secure Backup Process

Finally, it is important for organizations to have a secure backup process so that if an insider attack does occur an organization is able to recover quickly. This is, perhaps, more difficult for nuclear facilities than traditional businesses when it comes to infrastructure, but it is still an important step for businesses to take to protect their systems. This can be done by ensuring that backups are stored both in physical form and digitally. The organization should implement controlled access to the facility where such backups are stored, as well as implementing controlled access to the physical media. Additionally, when changes are made to the backup system, organizations should always require that employees institute the two-person rule.[10]

Theft of Intellectual Property

Intellectual property (IP) is defined by CERT as, "intangible asset created and owned by an organization that are critical to achieving its mission."[11] With this definition in mind they define theft of intellectual property as, "an insider's use of IT to steal proprietary information from the organization. This category includes industrial espionage involving insiders."[12] Unlike private businesses, nuclear facilities do not rely entirely on their intellectual property in order to make a profit. However, if an insider was able to steal security schematics, blueprints of the plants, personally identifiable information (PII) belonging to employees or other sensitive information it could lead to disastrous consequences. The two most common ways that insiders exfiltrate information is over a network through email or file transfers, or by physically removing the data on laptops or other removable media. While some insiders did remove physical papers, the CERT database shows that only 6% removed physical paper copies of IP. The following sections will address how to best mitigate these types of removal.

Network Exfiltration

Network exfiltration is typically done over email or over virtual private networks (VPN). It is important to note that in cases of theft of intellectual property most insiders steal the data within thirty days of leaving the organization. This means it may be worth checking an employee's email and VPN access logs to examine their activity in the month before they left the organization. Additionally, many insiders in the CERT database used personal email at work to

[9] Cappelli, Moore, and Trzeciak, 56.

[10] Cappelli, Moore, and Trzeciak, 57.

[11] Cappelli, Moore, and Trzeciak, 61

[12] Cappelli, Moore, and Trzeciak, 61.

exfiltrate data. In order to prevent this type of insider threat organizations may consider banning the use of personal email accounts on a work network. Additionally, they should consider routinely inspecting log files for suspicious access, large file transfers, irregular emails, or unusual access hours. While these steps may not prevent evert case of network exfiltration, they take important steps to catching those who do.

Physical Exfiltration

Physical exfiltration usually happens on thumb drives and portable hard drives or laptops. Preventing physical exfiltration of data can mean barring the use of removable media, or limiting who can use different types of removable media. However, if no limits are placed on the use of removable media, organization can create log files for file transfers to removable media. This will allow organizations to monitor for suspicious use or suspiciously large downloads.

Insider Fraud

CERT defines insider fraud as, "an insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or the theft of information that leads to an identity crime (identity theft, credit card fraud). While all organization, including nuclear facilities, should be concerned with protecting PII of employees, preventing identity crimes from occurring are certainly not the most important task of nuclear facilities. However, while nuclear facilities may not be concerned with preventing the same type of insider attacks that private companies are, there are still important IT best practices that can be taken from insider fraud cases. These lessons include maintaining a sufficient separation of duties and practicing password security.

Separation of Duties

If possible, businesses should build business processes into online systems. For example, if a supervisor needs to approve an action it should be done online using that supervisor's account, not using paper forms.[13] This allows organizations to utilize their IT systems to promote greater security at their facilities and make it more difficult for insiders to skirt the approval process.

Password Security

When conducting training stress that employees should not share their passwords with anyone. It may be helpful to remind employees that if someone else uses their account to commit a crime it will be difficult to prove it was someone else.[14]

Insider Threat Exercise

For physical nuclear security systems, it has been useful to have tabletop exercises to help professionals gain an understanding of how to best physically secure a facility. Sandia National

[13] Cappelli, Moore, and Trzeciak, 125.

[14] Cappelli, Moore, and Trzeciak, 126.

Laboratories has developed a tabletop exercise to help visiting scholars and students think about who may access such areas. Developing a tabletop to help students think about how to determine access to information technology at nuclear facilities may be useful and help put frame the above insider threat mitigation best practices as useful policies for nuclear facilities. The following section of this paper will examine how to best think about the different levels of cyber access in a way that may ultimately be useful in developing a new cyber version of the insider threat mitigation tabletop that better integrates lessons on preventing insider attacks from the information technology research.

Physical security at nuclear facilities is often thought about in terms of access, authority, and knowledge. Developing a tabletop exercise for implementing IT-related best practices at nuclear facilities could be done in one of two ways. First, the tabletop could take different job families (administrative, operator, security, support, etc.) and ask participants to assign them access to a set of computing resources based on their business needs. Second, the tabletop could ask participants to look at case studies where IT controls have failed to prevent an insider attack and ask them to identify changes that may have prevented the insider attack in the first place. These two approaches are further detailed below.

Job Family Based Tabletop

A job family based tabletop would require a significant amount of thought about what the important job families are at nuclear facilities. A preliminary list includes:

- Administrative (Human resources, administrative assistants, etc.)
- Operations
- Security
- Support (IT staff, procurement, etc.
- Legal

These job categories begin with broad categories, but it may be beneficial to break these job families down into smaller groups. For example, within the IT staff it may be important to separate out the systems administrators from the technologists. This level of stratification could ultimately make the tabletop exercise far more complex than originally anticipated.

Additionally, a job family based tabletop would require additional thought about what type of computing resources should be available to be assigned to each type of job family. This may prove to be difficult to breakdown IT resources at a level that is both realistic and not overly simplified. However, if a job family based approach was implemented some possible categories may include:

- Personnel records
- Operation-critical IT resources
- IT log files

This is certainly not a comprehensive list, but it showcases the type of IT resources that could be included. If implemented, the job family based tabletop could include a table for participants to fill out and assign each job group IT access. Following each group's assignment, the group as a whole would be able to talk through the decision-making process.

Case Study Based Tabletop

A case study based tabletop would utilize examples of insider incidents and allow participants to read through the profile of the attack and make recommendations on what changes could have been implemented in order to avoid such an attack. The recommended measures can easily be broken down into measures to prevent access, authority, and knowledge, or left more general. The tabletop could utilize insider incidents already in the CERT database, could rely on write-up of incidents not included in the CERT database such as the Edward Snowden incident, could create its own untrue, but realistic incidents, or could utilize a combination of any of the above.

The case study tabletop provides an advantage because it would be much simpler to put together than the job family tabletop. It would require a bit of preparation in putting together the case studies for use, but it would not require as much thought about splitting up job families or resources as the job family based tabletop would. It is worth noting that the case study method may be more realistic than the job family approach and thus may present a better opportunity for participants to learn in a hands-on way that replicates the real world.

The case studies chosen can highlight both intentional and unintentional insider threats. One example of a short case study participants may be presented with is:

"A consultant in the commercial facilities industry downloaded the organization's proprietary software and, upon termination, tried to sell it to another organization for nearly $7M. She also used another organization's bank account to pay for a personal credit card bill, costing the second organization more than $425,000. It is believed that access to this account came from the consulting work from the first organization."[15]

Participants could examine this case study and determine that the when the consultant downloaded proprietary software it should have set off an alert that a large and important file was being removed from the network. They may also note that she should not have access to the second organization's bank roll unless she was working directly for them. These are just two example that come directly from the best practices listed above, and are not the extent of measures that could have been taken to prevent or detect this insider attack much sooner. Many other insider cases can provide examples and teach students about how to apply best practices to real events to prevent the insider attack.

Recommendations

Ultimately, the case study based tabletop would be the easiest to implement, and would likely be the most effective as it allows participants to examine real cases of the insider threat and work to prevent them. However, this tabletop and the best practices will be the most useful if included in a broader discussion of the insider threat and security and safety systems at nuclear facilities. The IT insider threat is just on portion of an important problem, and is totally integrated with nuclear security as a whole. In today's world, it is unlikely that an insider would be able to perpetrate an

[15] "Insider Threat Examples by Sector," SCADA Hacker, https://scadahacker.com/library/Documents/Insider_Threats/Insider%20Threat%20Examples%20by%20Sector.pdf.

attack without the use of some IT connected system that, if monitored ad utilized correctly, can help to detect the event before it occurs. However, it is also important to note that IT insider threats cannot be detected without the use of additional programs such as human reliability programs and behavioral monitoring programs. Ultimately, nuclear security relies on organizations and people who can integrate all of the programs mentioned above, as well as many others, in order to ensure the security of their facilities.

In order to make practical use of this information, presenters could take the identified best practices and include them in overall nuclear security training courses. Additionally, when fully developed, the could utilize and share the IT insider threat tabletop for their courses. A future topic of research would include determining how to utilize the IT insider threat tabletop in a broader insider threat exercise integrating it—even as an exercise—into the whole system. Additionally, it may be useful to develop a specific IT insider threat presentation or subset of a presentation that could be presented separately for interested parties. Utilizing this presentation and tabletop will also present lessons learned that can be utilized to improve both aspects in the future.

Conclusion

Developing a set IT insider threat best practices and correlating tabletop adds a new aspect to nuclear security trainings that does not currently exist. Adding this important aspect of nuclear security allows practitioners to strengthen nuclear security as a whole. In an increasingly interconnected world, it will only become easier for insiders to perpetrate an attack on critical infrastructure using IT systems. However, this interconnectedness also allows for additional opportunities to monitor and detect insider threats before they occur. While best practice and tabletop exercises are not a foolproof way to eliminate the insider threat, making practitioners aware of the threat that exist as well as ways to mitigate it is increasingly important.