CYBERSECURITY CRITICAL POSITIONS
Best Practices Guide for Insider Threat Mitigation: Nuclear Facilities

ADVANCING INFCIRC/908 INTERNATIONAL WORKING GROUP:
Cybersecurity Focus Group

In 2019, the inaugural INFCIRC/908 international symposium was held in Brussels, Belgium, co-hosted by Belgium's Federal Agency for Nuclear Control and the US Department of Energy's National Nuclear Security Administration. One key outcome of the symposium was the establishment of the Advancing INFCIRC/908 International Working Group and its five Focus Groups: National Policy and Regulatory Frameworks, Trustworthiness & Reliability, Security Culture, Physical Protection & Technical Measures, and Cybersecurity. Composed of INFCIRC/908 subscriber state international subject matter experts in their respective areas, each Focus Group was tasked with providing the INFCIRC/908 community of practice with practical products for insider threat mitigation.

The Cybersecurity Focus Group is co-led by Chile and the U.S. with additional support from Germany and Switzerland. The present guide under consideration, Cybersecurity Critical Positions Best Practices Guide for Insider Threat Mitigation, is one of the Cybersecurity Focus Group's practical products and has been split into two parts to cover nuclear facilities and radiological facilities with their own respective, though conceptually similar, recommendations under a graded approach to cybersecurity.

INSIDER THREAT MITIGATION

Introduction

As the nuclear industry becomes increasingly computer-based, the importance of effective cybersecurity at nuclear facilities has grown ever more essential to safe and secure operations. While cyber outsider adversaries remain a key concern of nuclear facilities worldwide, the cyber insider adversary poses a unique challenge to operational and security teams at specific nuclear facilities. However, given critical cybersecurity roles and responsibilities common to most, if not all, nuclear facilities, it is possible to provide practical guidance for insider threat mitigation associated with those roles to prevent and protect against the emergence of a cyber insider threat.

Purpose

The purpose of this document is to provide practitioners an overview of common cybersecurity roles and responsibilities at nuclear facilities that pose unique insider threat mitigation challenges, complete with associated risks and mitigation recommendations. It is entirely possible that some roles identified in this guide go by different titles from one nuclear facility to the next, however practitioners should be able to read this guide and identify similar common roles unique to their facility context.

BACKGROUND:

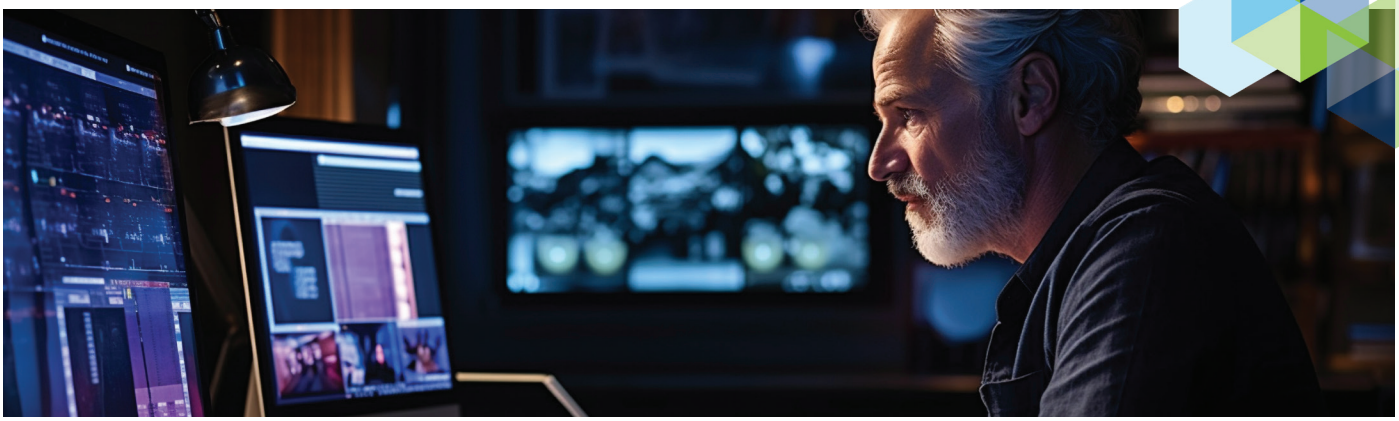
The Cybersecurity Zero Trust Model for Insider Threat Mitigation

The general approach based on a zero-trust model assumes all individuals with granted access to networks or other information technology are not just insiders, but would-be insider threats. Accordingly, technical, physical, and administrative controls are implemented based on general best practices to mitigate assumed insider threats.

To establish an effective insider threat mitigation program, organizations need to consider the following aspects:

1. Policies and procedures governing insiders
2. Understanding personnel roles and responsibilities
3. Establishing training programs based on personnel roles and responsibilities
4. Encouraging a culture of reporting irregularities, including insider behavioral red flags
5. Conducing exercises to assess system effectiveness based on current risk environment and identify areas for improvement
6. Periodically evaluating security controls based on changes in threat environment

CYBERSECURITY CRITICAL POSITIONS AND RESPONSIBILITIES
for Insider Threat Mitigation at Nuclear Facilities



Personnel
Non-Management
(regardless of role or responsibilities)

Facility personnel have basic responsibilities associated with understanding the rules and guidance associated with cybersecurity. This includes how to identify reportable items associated with an insider threat and, if there is a question, who they should report it to. These items should be part of the organization's general approach to insider threat mitigation and include both preventive and protective measures.

RISK:

Facility personnel represent the nearest access point to networks and information technology and can turnover into an insider threat or become an unwitting insider when exploited by an adversary.

MITIGATION:

Basic level training for facility personnel which should include non-management personnel roles and responsibilities, prohibited items (USB drives, mobile devices) awareness, unwitting insider awareness, and how to report a security event to management. In the absence of specific regulatory requirements, non-management personnel should be subject to periodic trustworthiness and reliability determinations and fitness for duty determinations that incorporate drug and alcohol testing, background checks, and other indicators of suspicious behavior under a graded approach.

Personnel
Management/Leadership

Organizational leaders need to understand business risks associated with insider threats. This includes what information is sensitive, what risks are assumed, and what preventive and protective measures programs are in place (detection, delay, response, emergency plans) addressing both witting insider threats and unwitting insiders.

RISK:

In addition to understanding the difference between a witting insider threat or unwitting insider, management represents a higher value target based on their access to, authority over, and knowledge of what operational, organizational, and personnel information is important and/or valuable.

MITIGATION:

Leadership positions require periodic trustworthiness and reliability reviews through drug and alcohol testing, background checks, performance evaluation and other attributes of program implementation. Under a graded approach, requiring management and leadership to participate in continuous behavioral observation programs may be warranted.

Personnel
With Administrative Rights and Other Cyber Enabled Positions

Any position or role across the organization with access to information technology or networks can potentially affect the confidentiality, integrity, or availability of information. In most cases the information of concern will exist in digital form. Sometimes that information is available in hardcopy or printed form but can still be a potential target for deletion, restricting access, unauthorized access, and manipulation.

RISK:

Personnel with administrative rights and other cyber enabled positions have computer-based functions and access to physical protections systems (i.e., badging and access control), operational environments (i.e., industrial control systems/operational technology), logging of actions and process deliverables (i.e., engineering workstations, historians, human machine interfaces), and information systems (i.e., password management, user accounts). Cybersecurity critical positions are those with administrative rights, which, if exploited, could potentially create opportunities for unrestricted access to sensitive facility processes and data.

Access and the ability to manipulate information could directly lead to theft or unauthorized use of nuclear material; and/or the indirect sabotage of critical operational, safety, and security equipment resulting in unacceptable radiological consequences. Additionally, the manipulation of information could lead to a disruption in operations or create a situation where theft and unauthorized use of nuclear material would be more successful.

MITIGATION:

Depending on the specific personnel role being addressed, various mitigation measures exist to reduce the risk or impact of compromised personnel. Mitigation measures such as separation of duties or procedural checks and balances, as well as the more traditional network-based mitigations (such as two-factor authentication) can help reduce risk associated with specific personnel roles. Additionally, frequent review of access and actions logs should be completed, and administrative controls should be implemented that limit the use of accounts with elevated administrative privileges only when needed. Finally, in the absence of specific regulatory requirements, personnel in this category should be subject to periodic trustworthiness and reliability determinations and fitness for duty determinations that incorporate drug and alcohol testing, background checks, and other indicators of suspicious behavior under a graded approach.

Operators

Controlling and maintaining equipment (pumps, fans, compressors, condensers, feedwater heaters, filters, and chlorinators) that supply water, fuel, lubricants, air, or power to plant facilities, turbines, generators, and boilers requires operators be allowed access to all plant areas. Due to this level of access, the organizations become comfortable with seeing these individuals in various locations within the facility which increases the insider threat potential of these individuals.

RISK:

Although assigned roles and responsibilities typically require elevated access at a facility or site, operators tend to be at a lower pay grade, providing an adversary with opportunities to compromise them if finance-related problems arise in their personal life. In cases where an operator is working to gain a better position within the organization, they may become disgruntled if they are overlooked for potential advancement or perceive that their professional opportunity is reduced.

MITIGATION:

Operators should be included in a Fitness-for-Duty-Program (FFD) which would provide oversight, supervisory observation, routine drug and alcohol testing, background checking, and other attributes of an effective cybersecurity observation program, this program provides a cyber-focused opportunity to identify and mitigate risks before they are exploited by the adversary.

Engineers

Professional engineers contribute significantly to ensuring the effectiveness of cybersecurity measures within nuclear facilities. Their roles, including design engineers, operational engineers, and system engineers, encompass a range of responsibilities aimed at safeguarding critical infrastructure and mitigating cyber insider threats, among other things. While engineers play crucial roles in maintaining the cybersecurity of nuclear facilities, it is essential to recognize that these roles carry high levels of insider risk due to their knowledge of, access to, and authority within networks and other computer-based systems.

Design engineers

Design engineers should prioritize the responsibility of considering and incorporating cybersecurity and insider threat mitigation concerns in the initial design and construction of nuclear facilities. Working alongside cybersecurity professionals, they integrate advanced security features into the physical design. This includes implementing access control measures, intrusion detection systems, and secure communication channels. By adhering to cybersecurity and insider threat mitigation best practices during the design phase, design engineers contribute to long-term facility security and resilience.

RISK:

Design engineers, are involved in the initial design and construction phases, as well as ongoing upgrades to the facilities infrastructure and systems, and have access to critical information and possess technical expertise that can be misused or exploited. With their knowledge and privileged access, design engineers could intentionally design systems with hidden vulnerabilities, allowing unauthorized access to or compromise of the overall security of the nuclear facility, or even introduce networked or computer-based system vulnerabilities, such as intentional backdoors to the system. When looking at upgrades at nuclear facilities, one way that a design engineer could pose as a threat is by unauthorized design modifications during the update, resulting in vulnerabilities, compromise to facility security, and other unforeseen risks. Overall, their understanding of the plant's infrastructure, coupled with their privileged access rights, results in increased insider risk.

MITIGATION:

To prevent unauthorized design modifications during updates, nuclear facilities should enforce an in-depth change management process. This process should involve multiple levels of approval and verification for design changes, ensuring only a team of authorized personnel can make modifications. It is also advisable to implement regular audits and reviews of design updated to detect any unauthorized alterations. Design engineers should be regularly trained and educated on the importance of adhering to security protocols and the potential consequences of unauthorized modifications.

Operational engineers

Operational engineers oversee the day-to-day operations of nuclear facilities, adhering to basic cybersecurity protocols. Ideally, they remain vigilant in monitoring and controlling plant systems, and work closely with dedicated cybersecurity professionals to promptly detect and mitigate any cyber insider threats. Preferably, with ongoing training, operational engineers are equipped to identify irregularities or suspicious activities within control systems, and other operational systems, ensuring the overall security and resilience of facility operations.

RISK:

Operational engineers, responsible for day-to-day operations, possess extensive knowledge about facility systems, controls, and protocols. It is important to keep in mind that, due to their privileged access and authority over critical systems, operational engineers can pose a bigger threat as an insider due to their extensive knowledge, access, and authority, in comparison to other types of engineers within nuclear facilities. Their understanding of operational procedures, alongside their privileged access, can allow them to bypass security measures, or exploit or introduce new system vulnerabilities.

MITIGATION:

To prevent insider threats from operational engineers at a nuclear facility, strict access controls should be implemented, granting employees access only to the information necessary for their job roles and responsibilities. Another important mitigation aspect should be the implementation of separation of duties, which ensures that no single operational engineer has unrestricted access and control over critical processes. As always, it is important to implement regular security training and awareness to educate operational engineers on the importance of security protocols and the consequences of insider threats.

System engineers

System engineers specialize in the design and integration of various systems within nuclear facilities. Collaborating closely with operational and design engineers, as well as cybersecurity professionals, they develop comprehensive and secure architectures. Conducting risk assessments, system engineers identify vulnerabilities and implement security controls. Their efforts extend to safeguarding critical systems, such as control systems and communication networks, against cyber insider threats throughout the lifecycle of the facility.

RISK:

System engineers, specializing in system design and integration, hold valuable insights into the architecture and vulnerabilities of nuclear facilities. With their high level of knowledge and privileged access, a system engineer could manipulate the system configurations or compromise security controls. Due to the deep understanding of the system's intricacies, control systems, protocols, and operational procedures combined with their access and authority, a system engineer carries elevated insider risk of wittingly or unwittingly creating opportunities for system compromise or exploitation at a nuclear facility.

MITIGATION:

To prevent insider threats from system engineers at nuclear facilities, it is important to implement the concept of least privilege. This ensures that system engineers only have access to the specific resources required for their designated tasks. Continuous monitoring of their activities, along with behavioral analysis, can help identify suspicious behavior or potential red flags in real-time, enabling timely intervention and response to mitigate insider threats effectively. As always, it is important to implement regular security training and awareness to educate system engineers about the importance of adhering to security protocols and the consequences of insider threats.

In summary, the collective expertise of facility engineers, encompassing operational engineers, system engineers, and design engineers, is indispensable in protecting against cyber insider threats within nuclear facilities. Collaborating with cybersecurity specialists, these

professionals are instrumental in safeguarding critical infrastructure and proactively addressing cyber insider threats. However, the nature of engineering roles creates heightened insider risk from both general security and cybersecurity-specific perspectives. Implementing robust security measures, including access controls, monitoring systems, regular risk assessments, can mitigate associated insider risks. Additionally, creating a culture of cybersecurity through continuous training and awareness programs promotes responsible behavior among engineers, ultimately decreasing the risk of an occurrence of a cyber insider threat.

Reactor Operators and Senior Reactor Operators

Nuclear power reactor operators control nuclear reactors by adjusting and controlling reactor operations, which affect operations efficiency and the power generation capability for Nuclear Power Plants. Reactor operators monitor reactors, turbines, generators, and cooling systems, adjusting controls, as necessary. Reactor operators start and stop equipment, and record the data produced. Overall involvement in the plant, activities, implementation of procedures, and total plant control goes through operators.

RISK:

Although extensive resources are utilized to monitor reactor operators, the U.S. nuclear industry has had examples of criminal activity and other serious protocol breaches within a nuclear power plant. These nuclear security events have been due to greed, outside circumstances disgruntling employees, and sometimes just a human situation that impacted the ability of an employee to maintain a trustworthy approach.

MITIGATION:

Reactor operators should be enrolled in the site's FFD program. They should be closely monitored by management; based on observation of skill, training, and the application of the FFD at the site. Although monitored, disgruntled and unhappy employees still exist, and insider risk remains.

Radiation Protection Technicians

Radiation protection technicians, also known as health physics technicians and nuclear technicians, monitor radiation levels, protect workers, and decontaminate radioactive areas. They work under the supervision of nuclear scientists, engineers, or power plant managers and are trained in the applications of nuclear and radiation physics to detect, measure, and identify different forms of radiation. They possess knowledge of federal regulations and permissible levels of radiation. As an insider, a radiation protection technician would know what could affect operations or cause radioactive releases within the plant.

RISK:

Radiation Protection Technicians are deployed within a nuclear facility to monitor radiation protection, but like any staff inside the site, they could become an insider threat due to family life stresses, possible financial issues, conflicts with management or colleagues, or psychological or behavioral issues.

MITIGATION:

As an insider with access to vital areas, the usual FFD process should be applied to every radiation protection technician. However, during certain times of facility operation, such as an outage, an excessive number of staff are on site and observation capabilities by management could become limited. Random FFD testing should be maintained, but changes in behavior are difficult to recognize even through direct observation. To establish defense in depth, direct observation should be complemented by administrative, technical, and physical protection controls.

SECURITY OFFICERS:

Nuclear security officers are on an active, rotational schedule and their duties include analyzing and defending the reactor's vital areas and components and identifying and neutralizing threats with the help of assigned weapons, actions, and tactics. They must ensure that training and tactical drills follow competent authority requirements based on the organization's protection strategy.

RISK:

Security officer positions may be either under the direct employment of the site organization or contracted to an off-site organization to save costs. Many are younger individuals who are starting in the industry and may have a police or military background. The possibility of approach by outside entities looking to create collusion capabilities within the facility are possible. Acquiring insider access through a security officer provides a higher potential for success based on the security officer's high level of physical access. Contract disputes, scheduling disagreements, multiple consecutive shifts, and rotating schedules could affect an individual and lead to their disgruntlement and emergence as an insider threat.

MITIGATION:

If the security officer is an employee with unescorted access to vital areas at all times during duty hours, or under some or all operating conditions, they should be enrolled in the FFD program for random testing, observation, and daily monitoring. An increased risk of collusion exists during an outage situation or multiple shift changes this would be an indicator requiring an active observation program by management and peers.