CYBERSECURITY CRITICAL POSITIONS
Best Practices Guide for Insider Threat Mitigation: Radiological 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

Users of radioactive sources, regardless of the size of their organization such as research institutes, universities, medical facilities, or commercial companies, need to consider the potential cybersecurity risks associated with their operations. The nature of this work presents unique vulnerabilities that can be exploited by cyber insiders - trusted individuals within the organization with access to sensitive information. Depending on the size and resources of the organization, cybersecurity responsibilities might be assigned to dedicated IT staff (e.g., IT operator, IT administrator, system engineer, system owner), contractors, or sometimes managed by the users themselves. However, no matter the structure, there are two key roles crucial for a successful cybersecurity program targeting potential cyber insider threats.

Purpose

The purpose of this document is to provide practitioners an overview of common cybersecurity roles and responsibilities at radiological 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 radiological 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

Chief Information Security Officer

The first role is the Cybersecurity Executive, often referred to as the Chief Information Security Officer (CISO). The CISO is charged with setting the cybersecurity strategy for the facility. Their responsibilities include analyzing the facility's cybersecurity risk, particularly from potential cyber insiders, managing the facility's information security operations, providing and keeping up to date analysis of internal cybersecurity threats, and setting cybersecurity initiatives and budgeting. It is also essential for them to supervise and manage all cyber-related activities, projects, and programs to ensure they are adequately funded, staffed, and prepared to address the dynamic landscape of cybersecurity threats, with a special focus on those arising from within the organization. The overall focus of the CISO is to achieve implementation of robust security policies and an acceptable use policy to ensure employees' actions align with cybersecurity best practices for insider threat mitigation and beyond.

System Administrator

The second crucial role in countering cyber insider threats is the Systems Administrator. This person is responsible for maintaining the technical health and security of computer-based systems. Depending on the organization's size, this role might be managed by a team or a single individual. The tasks of a Systems Administrator that are particularly important for mitigating cyber insider risks include:

- Setting up, maintaining, and closing user accounts, carefully managing access control
- Password and identity management to prevent unauthorized access
- Reviewing log files of operating systems and applications for any abnormal activities
- Creating a backup and recovery policy to protect against internal sabotage
- Periodic monitoring of network connections for any signs of intrusions or unauthorized data transfers
- Updating systems with new versions and patches to fix vulnerabilities that could be exploited
- Documenting network configuration, software versions, etc., to aid in investigation and recovery efforts

By carefully considering these roles and implementing their functions effectively, organizations can strengthen their defense against potential cyber insider threats.

The Cyber Insider Risk

The best practices in this document are focused on securing physical protection systems that protect high-activity radioactive sources, but they could also apply to a site's IT systems or control systems for the radioactive source devices. These measures are tailored to implement cybersecurity controls that mitigate insider threats, to include a cyber insider.

Insiders pose unique risk to radiological facilities due to their authorized access to sensitive areas and knowledge of a facility's security and emergency response plans. This access and knowledge can provide an insider adversary with opportunities to disrupt or sabotage information and computing systems. Cyberattacks can compromise the confidentiality, integrity, and availability of security systems and operational technologies that protect radioactive material, jeopardizing human, and environmental health. A cyberattack on a facility conducted or facilitated by an insider adversary or unwitting insider must be considered in the facility's security planning. The cyber insider risk is two-pronged: first, cyber can be considered as an auxiliary attack vector in a blended attack; or second, a means for committing the main objective of a malicious act (e.g., theft of radioactive material or sabotage).

Blended attacks (i.e., a cyber and physical attack conducted simultaneously) are attractive because they take advantage of the privileged position of the insider adversary. This attack may include an active insider adversary, a passive insider adversary, or even a combination of both. By using an insider adversary, outsider adversaries can eliminate or minimize their need to be onsite. The insider adversary can perform cyber or physical actions that degrade the ability of physical protection systems to detect and respond to unauthorized access to radioactive material by either the insider adversary or the outsider adversaries. Unwitting insiders are also concerning as they may unknowingly support malicious acts by providing information or computer/network access (e.g., clicking on a malicious link or inserting a compromised thumb drive into a networked computer). As an additional concern, a social engineering attack to co-opt an unwitting insider is often easier, cheaper, and more likely to be successful than a purely technical attack.

The threat of attack from an insider adversary intending to cause harm, or an unwitting insider causing harm without malicious intent, is well documented. Historically, organizations have focused on mitigating these threats using external-facing cybersecurity controls such as firewalls, intrusion detection systems, and electronic access control tools (e.g., two-factor authentication). Today, organizations must broaden their security planning to include consideration for insider adversaries who can take advantage of critical processes, weak points, or the ability to conduct a cyberattack from within the network through the leveraging of authorized access. Realizing that, because of an insider adversary's assumed access level, none of the tools previously mentioned will detect anything abnormal as all operations will be initiated internally and appear as normal system functions. Unfortunately, cybersecurity measures and controls cannot eliminate all insider related risks (i.e., unauthorized data access, privilege escalation, or operational intrusion) to a facility's network and establishing an integrated, graded approach to mitigating cyber-based insider threats is challenging, especially for small radiological facilities with potentially limited resources both in staff and funding.

Starting a Cybersecurity Insider Threat Mitigation Program

A cybersecurity program is a necessity to ensure vulnerabilities are not introduced into a physical security program protecting radioactive sources. The integration of IP-based security system components will continue to increase making cybersecurity even more essential. Facility IT staff can help with the basics of a cybersecurity program, but professional cybersecurity support may be needed for the more technical tasks in developing a comprehensive program. Some of the cybersecurity controls recommended below are not solely focused on the insider threat; however, a comprehensive cybersecurity program should be developed to reduce or eliminate the opportunities for an insider to exploit weaknesses in the facility's cybersecurity program. The following are recommended tasks to establish a facility's cybersecurity program:

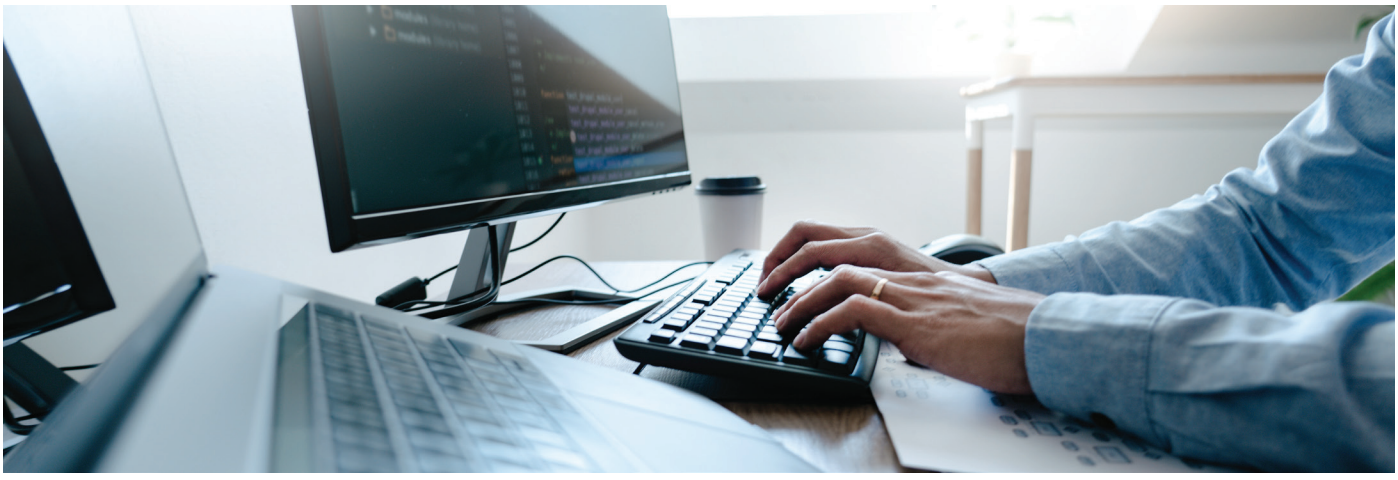
Developing a Cybersecurity Insider Threat Mitigation Program Starting Point

- Designate a staff member responsible for cybersecurity with sufficient education, training, and authority to implement the site cybersecurity program.
- Evaluate overall cybersecurity hygiene, posture, culture, and awareness level.
- Map out all connections and dependencies to other systems.
- Determine if physical protection system components are configured into logical security zones with minimum required traffic flows between zones.
- Determine if network-level access controls are implemented on the internal network infrastructure that interconnects physical protection system components.
- Use a system discovery tool to conduct an inventory of what devices are connected to the protection system and determine if only those authorized devices consistent with the security plan are connected. Vendors may have recommendations for the appropriate tool.
- Review all firewall security policies and device configurations to determine if security zones are defined, minimum traffic flows are enforced, attack detection is enabled, logging on permitted and denied traffic flows are enabled, and administrative access capabilities are restricted to the minimum necessary.
- Conduct a best practices evaluation for secure router and switch configuration, management, and operation.
- Identify potential attack vectors that can lead to potential compromise of the physical protection system, especially from connections permitted through the perimeter or from permitted remote access and management connections.
- Review overall attack surface, attack vectors, and firewall rules.
- When performing the review keep in mind such items as:
    - Network terminals vs. workstations.
    - Restricted connectivity using distributed firewall security zones vs. unrestricted internal network connectivity.
    - Hardened centralized server configuration vs. distributed server and software implementation.
- Use a vulnerability assessment tool to determine if servers contain potential vulnerabilities and require patching or other security measures to mitigate potential risk. This may require the assistance of cybersecurity experts as these tools have the potential to negatively impact systems.
- Conduct penetration testing to validate perimeter security design and implementation. The use of cybersecurity experts is recommended for this activity.

Implementing Cybersecurity Insider Threat Mitigation Controls

The following are cybersecurity controls consisting of technical, physical, and administrative measures that can be applied to current security systems either immediately or in the near-term, and in a quick and inexpensive manner. Some of these activities may require support from IT departments, cybersecurity staff, or a contracted service provider to implement because they are beyond the skill set expected of a layperson. These activities are included because they are recommended components of a comprehensive cybersecurity program.

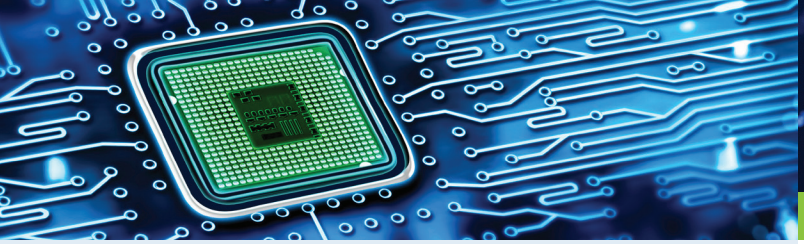
- Enforce strict user accounts with limited role-based permissions. Use the "least privilege" model for access to systems.
- Use strong, complex password management or use a passphrase. Passphrases are becoming the recommended control instead of passwords. If a password is used, a minimum of 12 characters is recommended.
- Remove unnecessary accounts, software, and processes.
- Install Anti-Malware Software and ensure it is kept current.
- Do not use software that is beyond end-of-life (for instance, Windows XP and Windows 7). New vulnerabilities are often found in this software, but the manufacturer is no longer providing patches.
- Ensure cybersecurity is included in the Site Security Plan with ongoing reviews and is updated following upgrades.
- Ensure cybersecurity events and predefined response actions are included in a Contingency Plan.
- Ensure the facility has an acceptable use policy for employees using company IT resources.
- Establish a baseline to identify all equipment, cabling, and circuits and update documentation to match the physical implementation of the system and implement a configuration management process for reviewing, approving, and documenting equipment and software changes, patches, etc.
- Ensure patches and firmware are derived from authorized vendors.
- Keep network switches, alarm panels, access control devices, computer BIOS, digital cameras, and other components patched to the current firmware version provided by the vendor.
- Restrict software and firmware upgrades to authorized system administrators/managers.
- Configure web browsers and dedicated e-mail accounts required by alarm management software to limit access to non-system related sites.
- Implement physical hardening of host computer locations, workstations, wiring closets, and on-site central monitoring stations to prevent a physical attack on the equipment or the introduction of malware via USB ports, etc.



- Perform port scanning of all physical protection system (PPS) components that connect to the network and communication infrastructure to ensure only authorized ports are open.
- Disable all unnecessary ports and associated services through hardware and software hardening.
- Use Mobile Device Management (MDM) for the administration of mobile devices accessing company networks.
- Ensure the site has a strategy for the development and implementation of plans, processes, and procedures for timely recovery and full restoration of any capabilities or services that are impaired due to a cyber event.
- Ensure the facility has an active employee security awareness program to potentially include phishing campaigns.
- Enable built-in firewall attack detection, logging, and alerting features that should already exist in most modern firewalls. Alerts should go to a Security Operations Center, SYSLOG server, a Security Event and Information Manager (SEIM), or at least provide assured means to get the alert to the responsible staff immediately.
- Enforce network traffic flows in existing firewalls.
- Utilize existing firewall DMZ as applicable (e.g., drop boxes, DNS, Web server).
- Enable port security on network switches, disable unused interface ports, and restrict administrative access.
- Create ACLs (access control lists) and restrict administrative access.
- Air gap the system if possible or at least minimize the number of perimeter interconnections to provide network isolation where feasible. Air gapped systems are not invulnerable to cyberattacks as systems should still be updated via USB drives, etc. Another option would be to implement a real time monitoring capability or a data diode.
- Configure a multi-zone network security architecture to isolate security protection components into logical layers and zones as appropriate.
- Utilize thin-client network terminals instead of Windows workstations where possible to reduce the attack surface, patching requirements, and total cost of ownership.
- Incorporate traffic encryption for communication over any external networks or telecommunications circuits.
- Add an intrusion detection system to analyze network traffic. This analysis will identify and alert personnel for attempted cyberattacks via suspicious packets and payloads.
- Use multifactor authentication:
    - Something a user possesses such as a badge or RSA token;
    - Something a user knows such as a PIN, password, or passphrase;
    - Biological characteristics of a user such as their fingerprint or iris pattern.
- Recommend that prior to deployment any new equipment and components be thoroughly evaluated for cyber vulnerabilities
- Evaluate, as practicable, supply chain risk for current and all potential future equipment and components.
- Validation of the software bill of materials (SBOM) by the end user against the certified SBOM of the vendor.
- Ensure excess computers and media are properly sanitized when disposed.

Sustainability

The following are best practices recommendations to sustain cybersecurity protection over the long term. An effective cybersecurity program requires constant attention to counter ever evolving cyber threat.



Sustaining a Cybersecurity Insider Threat Mitigation Program

- Implement a configuration management plan and update it regularly.
- Revisit program requirements and update policies and procedures for protection system configuration, change control, testing, personnel roles, and documentation at least annually; continually evaluate and address gaps.
- Update security plans periodically and after significant changes in your systems or networks.
- Maintain approved equipment lists including hardware, operating systems, application software, firmware, etc., and associated revision levels.
- Update mapping of interdependencies (hardware, software, hosts, and subsystems).
- Conduct end-to-end testing prior to incorporating new code or technologies.
- Implement comprehensive procedures and checklists for software and firmware upgrades.
- Manage and maintain software licenses.
- Regularly update software and ensure that it continues to be supported by the software vendor. This will minimize software cyber vulnerabilities.
- Run malware scans and update virus definitions on a frequent basis. Automated scans and updates may be used but be aware they may impact system performance. Where absolutely necessary from a functional standpoint, rare exceptions can be made and compensatory measures implemented to achieve a similar level of protection via alternative means.
- Perform penetration testing to ensure the effectiveness of hardening and architecture measures. Tests can be tailored to the specific Physical Protection System (PPS) requirements. Qualified cybersecurity experts should perform these tests.
- Conduct system monitoring of traffic over the network infrastructure and its attached components to detect cyber intrusion attempts; log system activity and report cyber alarm conditions.
- Periodically evaluate the recovery plan, which should include both contingency planning and backups.

23-50401