Best Practice Guide

Cybersecurity Best Practices for Gamma Irradiation Facilities

September 2026

iia

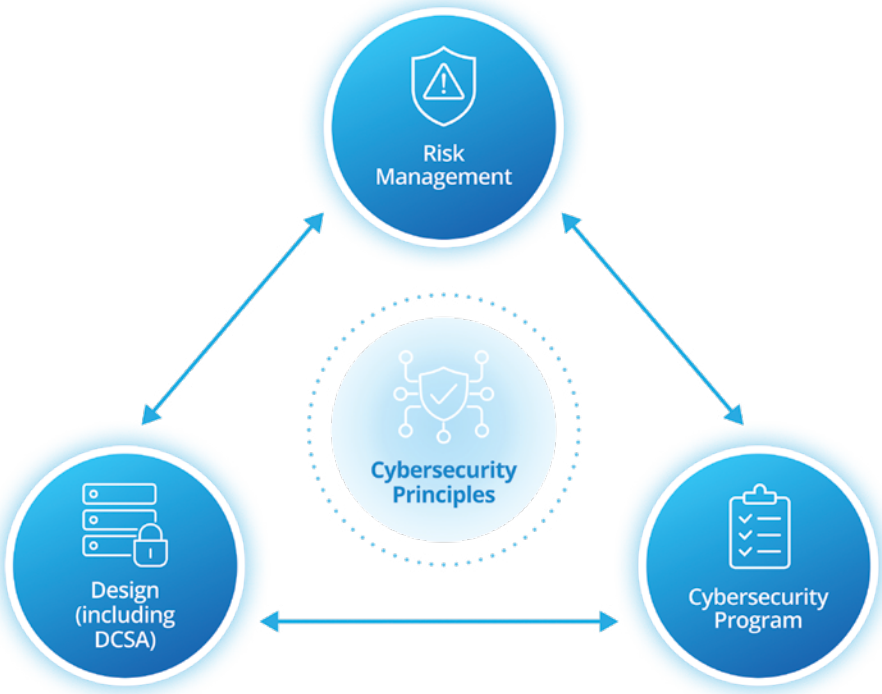
About this guide

Cybersecurity has become an ever pressing and important priority for organizations of all sizes around the world. Many reports have noted an increase in cyberattacks and exploited vulnerabilities across many different targets, one report went so far as to say, "2024 was the year of the enterprising adversary" [1]. Between November 2023 and October 2024, the Verizon DBIR team noted that of 22,052 incidents, 12,195 had confirmed data breaches, this is the highest number of breaches analyzed for a single report [2]. The impact of a cyberattack can result in financial loss, the inability to operate or provide a service, or the loss of assets such as data and facilities. Operators of gamma irradiation facilities additionally need to prevent cyber vulnerabilities from being introduced into a physical protection system that protects their high-activity cobalt-60 sources.

Operators of gamma irradiation facilities should therefore implement and manage cyber and computer security programs to protect their radioactive sources. At the time of publication, there is a lack of international and national standards on cybersecurity programs specific for users of radioactive sources. This document uses the Office of Radiological Security (ORS) *Cybersecurity Best Practices for Radioactive Sources* [3] as a starting point, and has been customized for the unique environment and challenges of gamma irradiation facilities.

This guide provides information on understanding the threat actors faced by gamma irradiation facilities and industry best practices to defend against cyberattacks targeting the computers within these facilities as well as those targeting physical protection systems. This guide covers fundamental cybersecurity principles and how they support risk management, designing, and implementing an effective cybersecurity program. This information is depicted in the figure below and is discussed at length in subsequent sections.

Figure 1: Cybersecurity Principles



Ultimately, these cybersecurity principles are intended to be holistic and should be part of a facility's overall risk management process. Without including cyber risks and cybersecurity in a risk management profile, gamma irradiators leave themselves completely vulnerable.

Further reading and other guidance, including that on the implementation of a cybersecurity program, is available and this is highlighted in this guide and a full list can be found in the attached Appendix.

This publication is the result of a collaboration with the US Department of Energy National Nuclear Security Administration's Office of Radiological Security and Sandia National Laboratories with the support of the International Irradiation Association (iia). The iia thanks and acknowledges the significant work undertaken by the experts of Sandia National Laboratories that has enabled and resulted in the publication of this document.

Particular thanks go to Jenna deCastro and Michael T. Rowland of Sandia National Laboratories, the lead authors of this publication.

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-NA0003525. SAND2024-14374O.

About the International Irradiation Association (iia)

The iia is a non-governmental organization (NGO) that represents the interests of the global irradiation industry and scientific community. A core aim of the iia is to promote the safe and beneficial use of gamma, electron-beam, and X-ray technologies. The irradiation community includes operators of gamma irradiation facilities that process products and material for many beneficial applications. Gamma irradiation facilities are industrial scale irradiation or radiation processing facilities that utilize cobalt-60 sealed sources. Membership of iia is diverse and includes corporations, research institutes, universities, and governmental bodies around the world.

To learn more about the iia, please visit https://iiaglobal.com/

Table of Contents

List of Figures

List of Tables

Acronyms and Definitions

Abbreviation	Definition
ACS	Access Control System
ALARA	As low as reasonably achievable
APT	Advanced Persistent Threat
CIA	Confidentiality, Integrity, Availability
DBIR	Data Breach Investigations Report
DCSA	Defensive Cybersecurity Architecture
DiD	Defense in Depth
DMZ	Demilitarized Zone
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
IaaS	Infrastructure as a Service
IAEA	International Atomic Energy Agency
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MFA	Multifactor Authentication
NCSC	National Cyber Security Centre
NRC	Nuclear Regulatory Commission
ORS	Office of Radiological Security
OT	Operational Technology
PaaS	Platform as a Service
PII	Personally Identifiable Information
PoE	Power over Ethernet
PPS	Physical Protection System
RF	Radio Frequency
SaaS	Software as a Service
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point

1. Overview

Radioactive sources are crucial for various commercial, medical, and research uses. It is essential to balance the advantages of the use of these sources with appropriate safety and security measures. The Office of Radiological Security (ORS) works in collaboration with a diverse array of partners, including government regulatory bodies, emergency responders, industry stakeholders, and international organizations to improve the security of high-risk radioactive sources. This initiative serves as a primary defense against unauthorized access to materials that could potentially be utilized in a radiological dispersal device, commonly known as a "dirty bomb." ORS prioritizes its efforts on securing high-activity sources, such as cobalt-60, utilized in gamma irradiation facilities [3].

ORS security recommendations are the result of many years of experience implementing security for more than 900 buildings in the U.S. and over 1,200 facilities in more than 80 countries worldwide. The cybersecurity best practices presented in this guide are consistent with U.S. government and industry recommendations such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Atomic Energy Agency (IAEA), and Nuclear Regulatory Commission (NRC) guidelines. However, this guide is not meant to provide specific guidance on implementing IAEA, NRC, or other guidelines or regulations.[1]

Large, multinational organizations with high-activity radioactive sources may already have an existing organization-wide cybersecurity program. However, smaller organizations may rely on IT staff, part-time contractors, or perhaps may have other staff such as a radiation safety officer, or operations manager perform key cybersecurity roles. This guide aims to provide all gamma irradiation facilities with approaches and strategies to counter cyber threats to radioactive sources and operational IT systems.

The overall objective of an effective cybersecurity program is to provide sufficient protection to the gamma source against theft or sabotage. However, the physical protection of the source may also be affected by an adversary that initiates a cyberattack that disrupts operations and/or security processes at the site. This attack would need to first gain initial access and persistence on a network and perform reconnaissance, then exploit systems to degrade or bypass security measures. These activities could also provide the adversary with greater capabilities that could facilitate a physical intrusion aimed at stealing or sabotaging the source. These consequences may be associated with cybersecurity risks which need to be effectively managed.

Example cyberattack scenarios include:

1. Cyberattack designed to degrade physical protection equipment. An adversary exploiting vulnerabilities in physical protection equipment to fail cameras and/or turn off intrusion detection and alarms in support of a physical intrusion. This scenario is directly associated with the unauthorized removal of radioactive material. Addressing risks associated with this scenario are prioritized by DOE/NNSA ORS.

2. Cyberattack resulting in the sabotage of control equipment. An adversary may cause the irradiator (source) control system to malfunction, fail, or cause damage to product/equipment to distract personnel in a manner that could decrease situational awareness.

3. Exfiltration of sensitive information. Social engineering could be used to exploit unwitting, benign insiders to gain access to physical protection systems, networks, and related subsystems without the need to hack or conduct a cyberattack using cyber tools. The adversary would gain access to sensitive information regarding personnel who have access to key locations of the gamma irradiator, possibly to target and extort these personnel to provide the adversary with physical access or valid credentials. For more details on insider threats, see Section 2.2.1.

1 Some international standards that can be reviewed are:
- ISO/IEC 27000 Series of Standards – Information Security Management [31]
- IAEA NSS 17-T [27], NSS 33-T [28], and NSS 42-G [29]
- ISA/IEC 62443 Series of Standards [30]

2. Cybersecurity Risk

Risk is the effect of uncertainty on an organization's objectives [4]. Risk is generally described in terms of likelihood multiplied by consequences. Likelihood of a successful cyberattack considers the threat (or adversary) and the vulnerability, or susceptibility, of the organization and its digital technologies to cyberattacks associated with the threat.

2.1 The Threat

Recent terrorist attacks in the United States, Europe, and Africa, and arrests of individuals plotting to commit acts of terrorism, demonstrate the continued and evolving threat to national security. Cyberattacks are an emerging threat vector for radiological security as intrusion alarms, video, and access control systems are rapidly migrating to use networks for their communications. A cyberattack alone cannot result in the theft or sabotage of a radioactive source but could make a physical attack on the facility easier by delaying detection and response. This is called a blended cyber/physical attack.

In recent years, cybersecurity has increasingly become a critical focus. Reports indicate that from 2021 to 2022, the exploitation of vulnerabilities surged by 55%, with 147,342 attempts documented in 2021 and 228,345 in 2022 [5]. The 2023 M-Trends report by Mandiant highlighted that "attackers are not giving up… we're seeing attackers cause bigger impacts with less skills. They're also more brazen and willing to get much more aggressive and personal to achieve their goals. They will bully and threaten and ignore the traditional rules of engagement" [6]. Furthermore, Verizon's 2023 Data Breach Investigations Report (DBIR) Report revealed that out of 3,966 incidents of system intrusion, 1,944 led to confirmed data breaches [7]. The consequences of a cyberattack can include financial losses, operational disruptions, or the loss of critical assets such as data and facilities. Additionally, operators of gamma irradiation facilities must ensure that cyber vulnerabilities do not compromise the physical protection systems safeguarding their radioactive sources.

In November 2024, the National Cyber Security Centre (NCSC) in the United Kingdom found that the number of significant cyberattacks was three times higher than in 2023. Of the 430 cyberattacks the NCSC provided support for, 89 were deemed "nationally significant," and China, Russia, Iran, and North Korea were identified as "real and enduring threats" [8].

Recent examples of different cyberattacks include:

1. Compromise of Telecommunications Systems: may prevent alarms from gamma irradiators to local law enforcement.

    a. In November 2024, an extremely aggressive, Chinese-based advanced persistent threat (APT) [9, 10], conducted successful cyberattacks against many U.S. telecommunications providers in addition to telecom providers in over twenty other countries. This attack was part of an extensive surveillance and intelligence collection campaign. Researchers believe the attack began in 2022 and, even more than two years later, still infects telecom networks. This APT successfully stole more than just phone call meta data, including source and destination phone numbers, time of day, and call length. They also acquired law enforcement surveillance request data in addition to compromising private communications of individuals involved in government or political activity [8, 10].

2. Ransomware Attacks: may affect operations, financial, and security systems thereby indirectly or directly impacting the ability to provide appropriate security to the sources.

a. Virtual Private Networks (VPNs) are essential for remote access, monitoring, and to enable work-from-home capabilities for key personnel. However, vulnerable VPNs, if compromised, can provide complete access to a network. In the case of the 2021 Colonial Pipeline attack, adversaries successfully "exploited a legacy VPN that shouldn't have been in use" [11] using leaked credentials to conduct a successful ransomware attack that cost the Colonial Pipeline Company an estimated 4.4 million USD in a ransomware payment and a five-day shutdown, which caused a surge in panic-buying of gasoline as Colonial Pipeline is responsible for almost half of the gasoline, jet fuel, and diesel piped throughout the East Coast [12].

b. In February 2024, Change Healthcare was the victim of one of the most significant ransomware attacks that resulted in a massive data breach, lengthy disruptions, and considerable recovery costs. The CEO of Change Healthcare testified the company issued a 22 million USD ransom payment and that the data breach impacted roughly one hundred million individuals [13], including threatening their access to medical care [14]. The CEO also testified the attack was a result of failing to use multifactor authentication (MFA) despite it being an industry standard best practice [14].

c. From December 20, 2019 to January 5, 2020, a ransomware attack on eHealth, a Saskatchewan business, resulted in over thirty patients receiving delayed cancer related treatments [15].

3. Supply Chain Vulnerabilities and Disruptions: may allow for adversaries to get initial access to internal networks. Initial access and persistence on internal computer networks could allow an adversary to plan a success with a higher likelihood of success.

   a. Although not an attack, the CrowdStrike software update failure remains a significant cyber incident that caused a global Information Technology (IT) outage that impacted numerous industries. According to reports, the failure cost Fortune 500 companies roughly $5.4 billion in losses and impacted an estimated 8.5 million machines. This incident exemplifies the impact of vulnerabilities introduced by the supply chain [8].

   b. In early March 2021, it was revealed that an attacker, Tillie Kottman [16], compromised Verkada's live camera feeds and personal information, including but not limited to customer names, email addresses, physical addresses, usernames and password hashes, and the geolocation data for security cameras. Some of the 150,000 compromised feeds included cameras that were in extremely sensitive areas like health clinics, schools, prison cells, and psychiatric hospitals [17].

The above examples highlight the increasing prevalence of cyber threats that pose significant risks to gamma irradiation facilities, particularly in the context of their reliance on telecommunications for security and emergency response. As highlighted by recent incidents, the notion of "when, not if" regarding cyberattacks should be a prevailing mindset among security professionals. This shift underscores the urgent need for gamma irradiation facilities to enhance their cybersecurity measures to protect against potential breaches that could compromise their operations, along with the safety and security of the radioactive materials they handle [2-4].

Telecommunications systems are essential for alerting law enforcement and emergency responders in the event of a security breach or potential attack. Any disruption or compromise of these systems could delay critical responses, increasing the risk of unauthorized access to high-activity radioactive sources. The recent example of significant cyberattacks, which have seen a marked increase in both frequency and sophistication, illustrates the vulnerability of irradiators to external threats. This situation necessitates a proactive approach to cybersecurity, ensuring that communication channels always remain secure and operational [8].

Moreover, the diffusion of state capabilities into the private sector and organized crime further complicates the security landscape for gamma irradiators [18]. As criminal organizations increasingly leverage advanced technologies and tactics, the potential for coordinated attacks on critical infrastructure, including gamma irradiation facilities, rises. This convergence of threats not only endangers the facilities themselves but also poses broader implications for public safety and national security [19].

Gamma irradiation facilities need the integration of robust cybersecurity measures and resilient telecommunications pathways to safeguard against evolving threats. One key best practice to ensure resilience is to utilize redundant and independent communication channels. An example of this is to use both wired communications and cellular networks to communicate alarms to local law enforcement. In doing so, facilities can enhance their operational performance by maintaining system availability to protect radioactive sources and contribute to the overall safety and security of the organization and community. Failure to address these vulnerabilities could have dire consequences, underscoring the imperative for continuous vigilance and adaptation in the face of an ever-changing threat landscape.

2.2 Who is the Threat?

Figure 2: Threat Types

The figure above depicts the various adversaries that pose serious threats to gamma irradiation facilities and highlights the motivations for each threat type. Each threat actor can, and often does, use the same tactics, techniques, and procedures as another. Alternatively, one threat actor can hire the services of another. For example, a Nation State may employ the services of a hacking group to attack another nation's critical infrastructure. While the initial adversary may appear to be different, the motivation remains the same. Of these threat types, ORS is most concerned with insider threats regardless of whether they are witting or unwitting insiders.

2.2.1 Insider Threat

Insiders pose a serious potential threat to gamma irradiator facilities due to their authorized access to sensitive areas and knowledge of a facility's security and emergency response plans. This information can provide an insider adversary with opportunities not otherwise available to external adversaries. A cyberattack conducted or facilitated by an insider blurs the conventional distinction between internal and external threats to a facility and must be considered in security plans.

Insider cyberattacks are attractive as they take advantage of the knowledge, access, and authority of the insider. By using an insider, external malicious actors can minimize their need to be on site to conduct the attack, however they may still need to be on-site to steal the source. The insider can perform cyber or physical actions that degrade the ability of physical protection systems to detect and respond to unauthorized access to radioactive material.

Insiders can be passive or active. An active insider can be non-violent or violent. An active, non-violent insider uses stealth or deceit to facilitate or conduct an attack [20]. An active, violent insider also uses stealth or deceit but is also willing to use physical force against facility personnel.

A passive insider may assist an adversary by providing information, such as access codes, disabling alarms, or blueprints, that can be used in performing an attack [20]. Performing these actions either willingly or unknowingly still pose serious threats to the overall security of a gamma irradiator. Unwitting insiders are concerning as they may unknowingly support malicious acts by providing information or network access, either by clicking on a malicious link or inserting a compromised thumb drive into a networked computer, to name a few examples.

Social engineering is a type of attack that provides the adversary with the ability to gain privileges and access to computer systems and networks of an unwitting insider. Social engineering is often easier, cheaper, and more likely to succeed than attacks aimed at exploiting an organization's internet facing devices (e.g., Firewall). The different types of social engineering attacks, and their success rates, are detailed in the table below.

Table 2.1: Common Types of Social Engineering

Phishing	Spearphishing	Pretexting	Baiting[2]	Smishing
Emails sent to many users with a malware-infected document or a link to a web page that elicits sensitive information (username/ password or personal information).	A customized phishing email that targets a single individual, based on their personal information, area of expertise, or appears to come from someone they know.	Attacker crafts a story that misleads the victim to provide sensitive information, username/password, or money.	Leaving a lure (e.g., a malware-infested USB drive) outside a facility, hoping an employee will plug it into their computer.	Attackers send malicious links to victims in text messages that are crafted to lead victims to open the link and inadvertently download malware, reveal sensitive information, or send money to cybercriminals [21].
Success Rate[3] 0.15%	Success Rate 35%	Success Rate 30%	Success Rate 45%	Success Rate 9% - 14%

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 such as multifactor authentication [22]. 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.

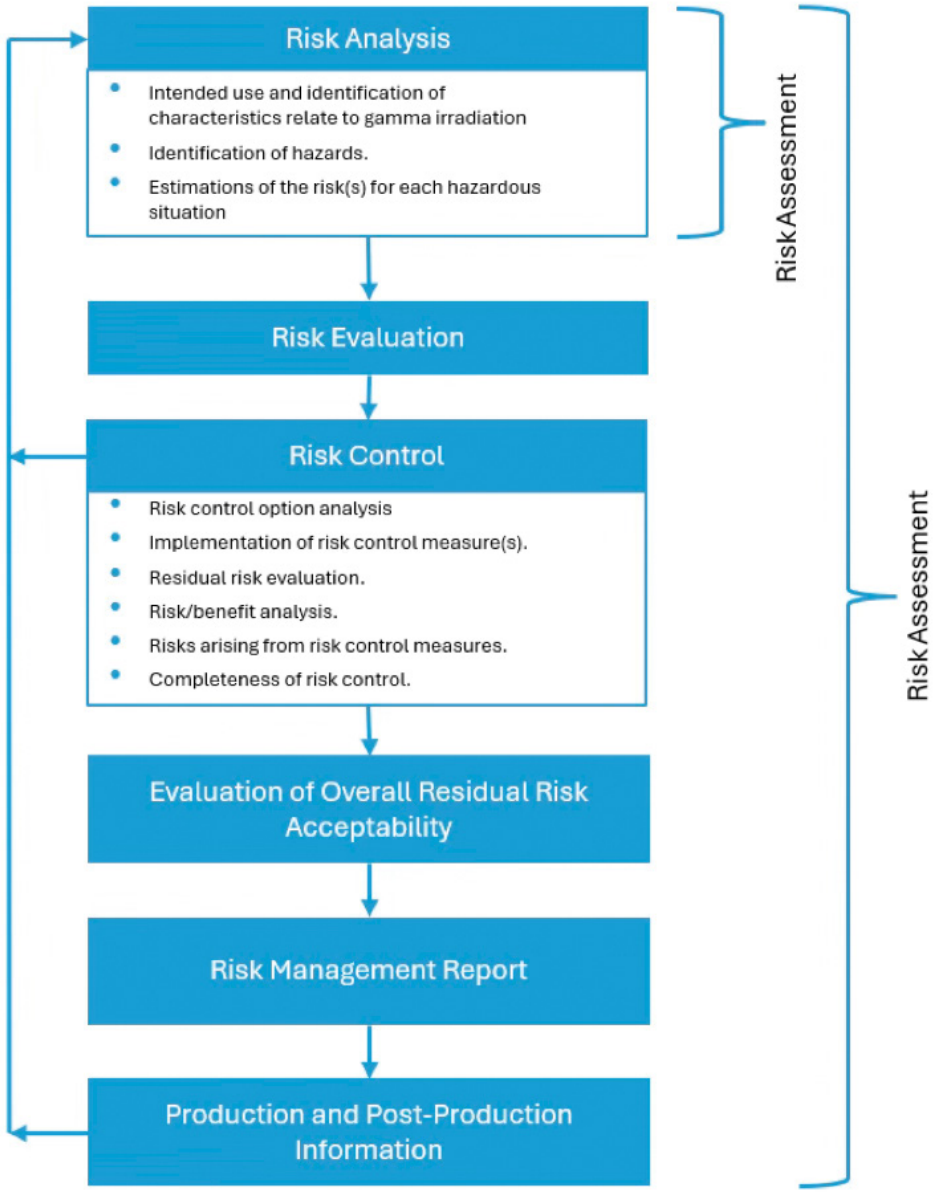
Cybersecurity controls cannot eliminate all threats from inside or outside a facility's network, and establishing an integrated, graded approach to mitigating cyber-based insider threats is challenging but not impossible.

2 Phishing through Baiting sourced from ORS, "Cybersecurity Best Practices for Users of Radioactive Sources," ORS, 2022.
3 In November 2024, the Cybersecurity & Infrastructure Security Agency (CISA) published a report on phishing-resistant multi-factor authentication (MFA) that was successfully implemented by the U.S. Department of Agriculture (USDA) [22].

3. Risk Management

A planned and systematic approach to risk management is necessary to create an effective cybersecurity program. Risk management is informed by policy and organizational risk tolerance. A risk management process should lead to the application of a graded approach and implementation of defense in depth. The objective is to minimize the financial and human resource costs while maximizing security benefits. A risk management framework is depicted in Figure 3 below.

Figure 3: Risk Management Framework



3.1 Potential Cybersecurity Risks to Gamma Irradiation Facilities

Risk management is necessary to ensure that limited resources are directed towards the most significant risks. The overall security consequence is associated with the theft of Cobalt-60 or Cesium-137 source at the facility either within the vault, storage, or during transport. Risks associated with cybersecurity scenarios are listed below. Some significant risks include but are not limited to:

1. The theft of sensitive information, such as credentials, access control lists, and personnel Personally Identifiable Information (PII) that could facilitate access to the sources or planning of a potential future attack. Ransomware attacks commonly exfiltrate this type of information that could be sold to a third party with motivation to attack the facility.

2. The compromise of Physical Protection Systems (PPS) can degrade security provided to the sources or locations. This risk increases in instances where (1) above has already occurred.

3. The compromise other important systems such as the compromise of Operational Technology (OT) or control system(s) that prevents normal use of the source, thereby causing an incident that could distract personnel and reduce security/situational awareness.

4. The compromise of supporting network infrastructure: disable communication of alarms to security staff or off-site responders. This may result in degrading the Physical Protection System, resulting in Risk (2) above.

3.2 Holistic Risk Management

Cybersecurity risks need to be incorporated into a facility's overall risk. Cybersecurity, as with digital technology and IT, is a key enabler of safety, security and operations. However, cybersecurity can also impact administrative functions, financial functions, and organization reputation. Given the rising incidences of cyberattacks, it is increasingly likely that gamma irradiation organizations will be targeted for cyberattacks. Risk management is necessary to reduce the potential for successful attacks, and if successful, reduce the impacts and enhance quick recovery.

Cybersecurity risk management needs to also consider the following challenges:

1. **Financial Resources – Funding for cybersecurity programs is limited**
   Cybersecurity for gamma irradiators has increasing importance as there are many unmitigated risks associated with the convergence of IT, Internet of Things (IoT), and OT. This demands investments to establish a cybersecurity program, purchase and integrate protective measures (e.g., firewall, intrusion detection/protection systems), and ongoing monitoring and sustainment.

2. **Human Resources – The availability, or lack, of trained personnel**
   There is an increasing shortage of cybersecurity professionals in the U.S. and internationally. This shortage is compounded by the specific needs and demands of industrial irradiators.

3. **User Expectations - Public Wi-Fi, interconnectivity, and expediency are prioritized**
   There are expectations for industrial irradiators to provide high-speed, reliable, remote access to insiders such as employees and contractors. Trends to increasingly integrate logistics shipping and customer management systems between industrial irradiators, their customers, and suppliers has increased the exposure of the organization's networks to remote-based ransomware cyberattacks. Internally, increased interconnectivity for business reasons of logistics systems, operational control, quality control systems to the industrial irradiator controller (i.e., OT) increases the risk of an attack having wide impact on many systems of the industrial irradiator. These expectations, including laws and regulations on privacy, may resist the application of strict controls or bypass these controls.

4. **Supply Chain Risk**
   Supply chain risk is strongly correlated to the (1) convergence and adoption of ICT, IoT, and OT within networks and systems and (2) the lack of vendor support to cover the lifetime of the irradiation device. These devices are highly dependent on out-of-support Legacy Systems (running Operating Systems such as Windows XP, Windows 7). Historically, security relied upon a physical "air" gap to isolate these devices from external "untrusted" networks. However, convergence trends are resulting in devices that demand external network connections for tasks such as monitoring, maintenance, or licensing by suppliers.

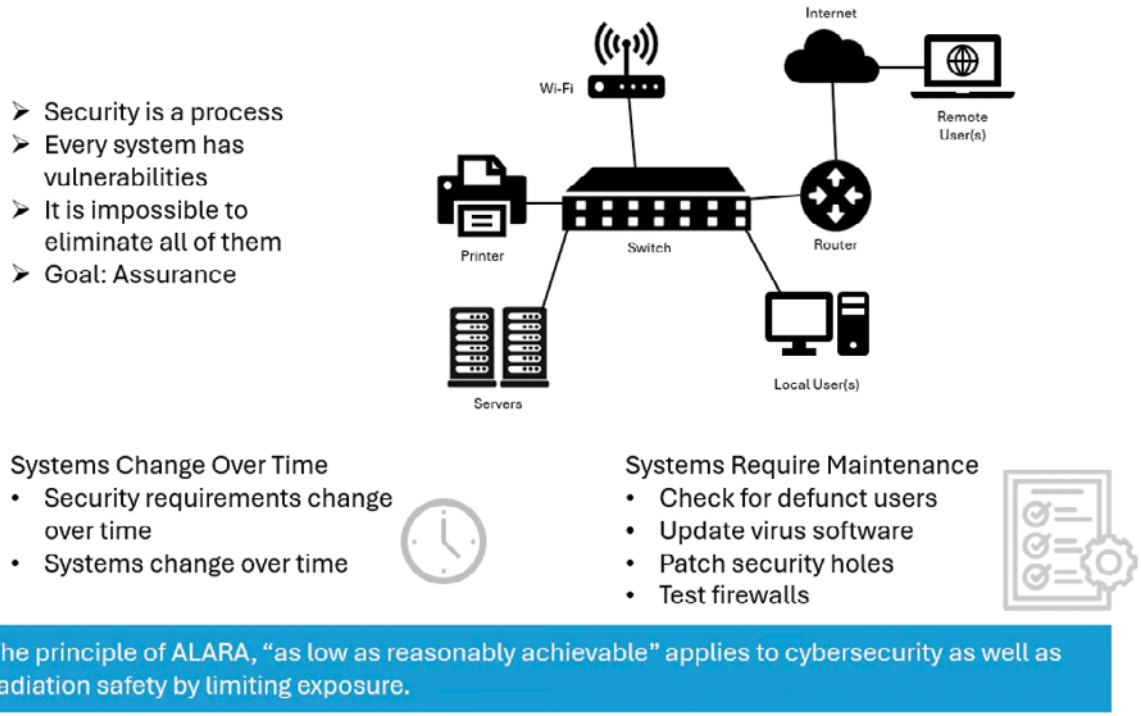
4. Cybersecurity Principles

In the realm of cybersecurity, it is essential to recognize that effective security is the result of a continual process and not a one-and-done effort.

With the emergence of modern technology, operational environments have begun to evolve in response. However, the risks and cybersecurity requirements with these systems evolve too. This dynamic nature necessitates regular maintenance and updates to ensure robust cybersecurity measures are in place. Some key maintenance activities can, and should, include:

- Updating software and firmware periodically.
- Regularly reviewing and removing inactive user accounts to prevent unauthorized access.
- Keeping antivirus software up to date and regularly patching systems to protect against current threats.
- Routinely scanning for vulnerabilities and testing firewalls and intrusion detection systems, if applicable, to verify they remain effective in safeguarding against potential breaches.

Figure 4: Basic Cybersecurity Principles



The basic cybersecurity principles depicted in Figure 4 can further the principle of "as low as reasonably achievable" (ALARA). This principle applies not only to radiation safety within an irradiator but also to cybersecurity. ALARA emphasizes the importance of minimizing exposure to risks while also balancing operational needs and resource constraints. By adopting a proactive, systematic approach to cybersecurity, gamma irradiators can enhance their resilience against threats and ensure the safety and integrity of their irradiation systems. Every facility, even gamma irradiators, possesses inherent physical and cybersecurity vulnerabilities. While it is impossible to eliminate all potential threats, the primary goal should always be to manage risk to as low as reasonably achievable with sufficient assurance.

Cybersecurity risks are inherently linked to sensitive digital information. The confidentiality, integrity, and availability (CIA) triad must be properly protected to ensure that risks are kept ALARA.

- **Confidentiality** – The protection of information from improper release. One thing to consider when protecting the confidentiality of information is who is authorized to see the information. Confidentiality is typically enforced through cryptographic methods and is often hard to enforce once confidential information is revealed.
- **Integrity** – This principle focuses on protecting data, or systems, from being improperly modified to address the concern of whether data is reliable. Integrity is generally enforced through measures such as access control or the use of digital signatures.
- **Availability** – This concept addresses the concern of whether a system is working as intended and if it is available to users as designed and if it can respond to requests. Availability is generally enforced through authentication and authorization.

Information properly secured against cyberattacks targeting digital information can lessen the likelihood of disclosure (confidentiality), alteration (integrity), or destruction or denial of use (availability); any of which could compromise nuclear security. Concepts that support the CIA triad are detailed in the following section [23].

4.1 A Graded Approach and Defense in Depth

Key security principles that simplify establishing, implementing, and sustaining a cybersecurity program are a graded approach and defense in depth (DiD). A graded approach simplifies the application of cybersecurity requirements and their associated controls.

4.2 Graded Approach

The objective of a graded approach is to ensure that resources are optimized to provide sufficient cybersecurity to systems and functions associated with unacceptable risks.

An example of graded application of access requirements to categories of computer systems could be a common office system with access to no sensitive information. In this case, a valid username and password may be sufficient, and a physical protection system protecting common office systems would be less robust. An office system with access to sensitive information would require a username, password, and other authentication factors to gain access. The office system would also be in an area with physical protection.

For systems associated with greater risk, such as physical protection access control system protecting Co-60 sources, authorized users would be strictly limited to those that have successfully completed a trustworthiness evaluation, such as a background check; have a need to access the system; and possess a username, password, and strong multifactor authentication.

4.3 Defense in Depth (DiD)

However, no cybersecurity program is perfect, and to further ensure that risks are effectively managed, a DiD strategy for cybersecurity needs to be implemented. For cybersecurity, DiD is implemented through the establishment of a Defensive Cybersecurity architecture (DCSA). The DCSA ensures that functions associated with unacceptable risks are afforded protection through multiple independent layers of protection.

DiD is based upon an integrated set of Fortification, Access Control, and Choke point strategies [24].

a. Fortification is a defensive barrier or other reinforcement built to strengthen a function, system, or zone against a malicious act. Physical examples of fortification may include walls, hardened doors, or fences. Technical examples of fortification include cryptographic modules, sandboxes, or network segmentation. Fortification can be enhanced via system hardening like blocking unused ports or removing unnecessary services from a computer. Removing, or disabling, unnecessary system services can subsequently remove vulnerabilities as well.

b. Choke points are traditionally a strategic narrow route or gateway linking one zone, area, or network to another and are intended to control either the flow of people or information. Cybersecurity examples of choke points can include wired conduits between networked islands, whereas physical examples include entry control points to protected areas. Choke points are only effective when all traffic is first forced to pass through them as they provide a key location to deploy both authentication and detection technical measures.

c. Area or Access Control is the specific granting or denial of access to a place or resource. Access control is designed to prevent adversaries from having easy, unlimited access to physical locations or digital components. Access control can be passive, such as physical USB port blockers, walls, or locked doors. Network traffic filtering can be active, such as intrusion protection systems, or transition to more defensive modes of operations.

DiD demands a DCSA that supports key security functions to prevent, detect, delay, respond, and recover. Fortifications, such as encryption, help mitigate attacks and prevent widespread disclosure of sensitive information. Access Control is necessary to ensure that adversaries cannot leverage authorized entry points to bypass or overcome the fortifications. Detection demands key bottlenecks or choke points that provide key points whereby adversary access can be detected. Choke points can also be severed by an effective response after detection, resulting in islanding of key subnetworks thereby providing a potential to delay or disrupt adversary scenario progression; thereby limiting the extent of compromise.

Risk management, a graded approach, and DiD need to consider the stages of an attack. While prevention is key to reduce effort in response, it cannot be assured. A DCSA that supports detection, delay, and response is critical to minimize impacts of successful attacks.

5. Cybersecurity By design

Cybersecurity by design (or "Secure-by-design) means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure" [25]. Increasingly, security systems are moving to Internet Protocol (IP)-based components increasing exposure to malicious cyber-actors, which means that cybersecurity design must be considered when implementing physical protection systems (PPS).

Generally, PPS networks are interconnected to a gamma irradiator's larger enterprise IT network. This interconnection has the potential to provide access to malicious threats (adversaries) that have access to the enterprise IT network. Therefore, a Defensive Cybersecurity Architecture (DCSA) is necessary to provide defense in depth (DiD) against attacks aimed at degrading or comprising the PPS. The DCSA is a key design element that provides cybersecurity by design.

5.1 Defensive Cybersecurity Architecture

DCSA is a key cybersecurity concept that provides DiD against cyberattacks. Similar to how physical protection measures achieve Detection, Delay, and Response, DCSA achieves DiD through overlapping barriers of protection to: (i) prevent adversaries from accessing critical PPS components; (ii) increase the likelihood of detection for cyberattacks; (iii) delay the attacker; and (iv) support response to cyberattacks, including zero-day vulnerabilities.

The DCSA specification must consider all digital systems and components that either provide or support the security of radioactive material, which includes both security access and control, intrusion detection, and radiation monitoring systems. As physical protection systems evolve from stand-alone hardwired devices to network-based devices, the integration of physical protection devices with information technology becomes increasingly important. This shift entails that both power and data may be provided by a single ethernet cable; like the transition from landline phone systems to Voice over Internet Protocol (VoIP).

DCSA consists of two key parts. First is a specification consisting of graded sets of design requirements, constraints, and measures in security levels. Second, an implementation that installs and integrates cybersecurity measures to protect key PPS functions in security islands. These protections implement digital controls, network boundaries, and access controls to digital components that protect radioactive material by reducing or limiting access to adversaries and providing key choke points to improve detection and support response.

The DCSA specification and implementation demands an understanding of four fundamental concepts of cybersecurity—facility function, security level, security zone, and system. In physical protections systems, the protected area is a physical area (security zone) to which security requirements are applied (security level).

There are four major elements from which a DCSA is designed:

1. Facility Function: A purpose that needs to be achieved and a performance objective. For example, physical protection against theft of the gamma source would be a function.

2. System: An integrated set of equipment or components used to perform a facility function. A system likely performs many functions. For example, a physical protection system would protect against theft, but also provide the sub-functions of Detect, Delay, and Response.

3. Security Level: The strength of security protection required for a facility function and consequently for the system that performs that function. Each security level has a distinct set of requirements that are necessary to protect the safe and secure performance of the facility function. There will also be a base set of requirements common to all security levels ranging from high, medium, or low.

4. Security Zone (or Island): A group of systems having common physical and virtual (logical) boundaries. The same computer security requirements are applied to all systems within a zone.

Functions are overall objectives that an organization operating a gamma irradiation facility needs to achieve. The loss or malperformance of a function generally results in consequences and therefore is highly correlated with risk. The following are key steps in developing a DCSA:

1. Identify and describe facility (or system) functions. For PPS, this involves securing Detection, Delay, a nd Response sub functions. Based on the needs of the industrial irradiator, functions can be high-level, abstract, or detailed. Functions that can be islanded from one another should be prioritized for identification.

2. Assign each function to a security level. The number of security levels are generally aligned with level of risk associated with each function such as high, medium, or low would lead to three security levels corresponding to high, medium, and low risk. A security level consists of a set of requirements. There may also be "generic" or baseline security requirements which consist of common requirements for all security levels. A common requirement would be mandatory cybersecurity training for all staff or use of multi-factor authentication.

3. Identify systems (or parts of the system) that perform a facility function. These systems are then assigned a security level based upon the risk associated with that function.

4. Identify an island (i.e., zones) and establish logical and physical boundaries in which systems are contained. Boundaries need to be fortified, and communications between islands need to minimize interconnections through implement choke points and enforce effective access control. Boundaries need to meet the requirements of the associated security level.

5. Develop sets of requirements for arrangement of islands, inter-island computer security measures, and restrictions on interzone communications. These are unique requirements based upon the DCSA strategy which ensures that DiD is implemented whereby the functions associated with the highest risk are provided the greatest protection.

Evaluate interdependencies between islands: informational, engineering, physical resource, policy, procedural, or proximity. Based on these interdependencies, the DCSA requirements may be revised based on operational, organizational, or safety considerations.

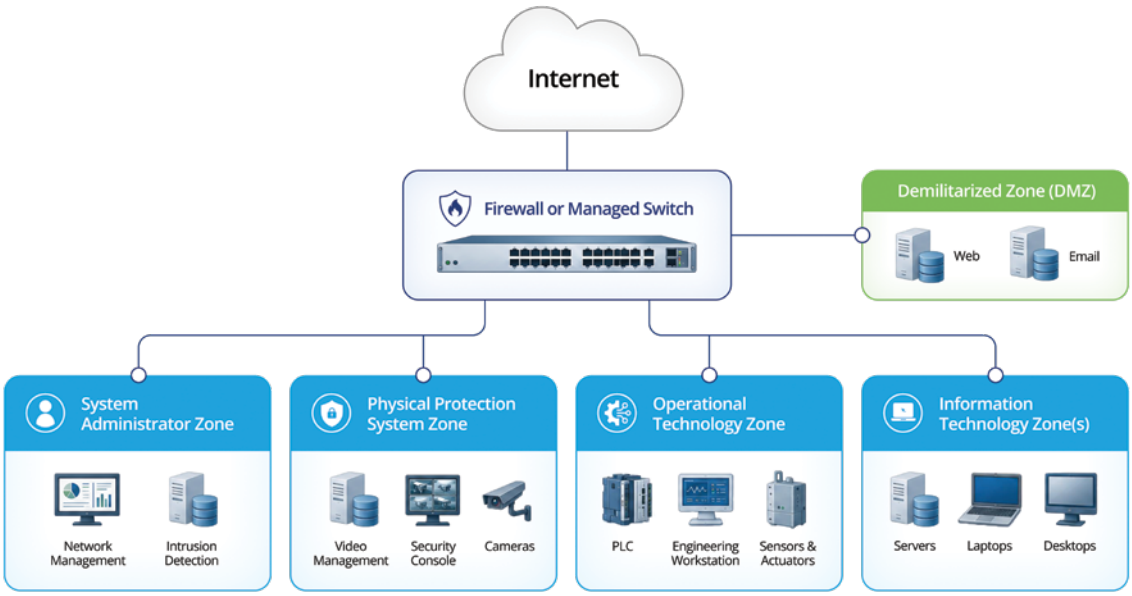
5.1.1 DCSA Template

The following DCSA Template focuses on a simple application of the key concepts above. Functions are isolated on islands which are interconnected via choke point connections that can be disconnected during an attack to isolate, delay, or stop attack progress and simplify recovery operations.

This template utilizes two operational configurations: (i) interconnected during normal operations and (ii) isolated or islanded configuration (during attack mitigation and recovery operations). The islanded network architecture is particularly vital for enhancing an irradiator's overall security posture and supporting business continuity management.

This architecture focuses on prevention, through fortification, by separating functions and systems into distinct islands (i.e., zones) such as System Administrator, PPS, OT, and IT with each island connected to firewalls and isolated from the internet by a demilitarized zone (DMZ). In the cybersecurity realm, a DMZ is intended to separate publicly accessible services, like the internet, from an organization's internal, protected network. This separation minimizes the interdependencies between islands while also reinforcing logical and physical boundaries. By removing entry points, facilities can significantly reduce the risk of unauthorized access and decrease an attacker's ability to move from one network to another. An interconnected and fully operational network is depicted in Figure 5 below.

Figure 5: Interconnected Configuration[4,5]



To bolster defenses further, access control supported by intrusion detection systems can be implemented in a manner that provide alerts (or alarms) indicating potential cyberattacks. These alerts may be supplemented with response procedures that can transition the DCSA to a hardened configuration, known as islanded operations, see Figure 6. In the event of a cyberattack, the ability to detect, assess, and initiate a switch to an islanded operation will contain potential threats and prevent adversaries from exploiting vulnerabilities on one network and then traversing into more critical networks. Isolation and segmentation of security systems using administrative tools such as Virtual Local Area Networks (VLANS) that can virtually separate network traffic can address many potential security issues and is highly recommended. By effectively creating islands, this proactive strategy not only shortens recovery time in the event of a cybersecurity attack but also ensures that compromised systems do not negatively impact other critical assets.

4 The terms 'island' and 'zones' are interchangeable. While the IAEA guidance references 'zones', this guide uses islands to highlight that each zone is easily separated from each other allowing easier transition to 'Islanded Configuration', see Figure 6.
5 The method of alarm communication will often be over secure site networks to the internet using a wired network connection or there may be a wireless connection such as cellular (not shown).

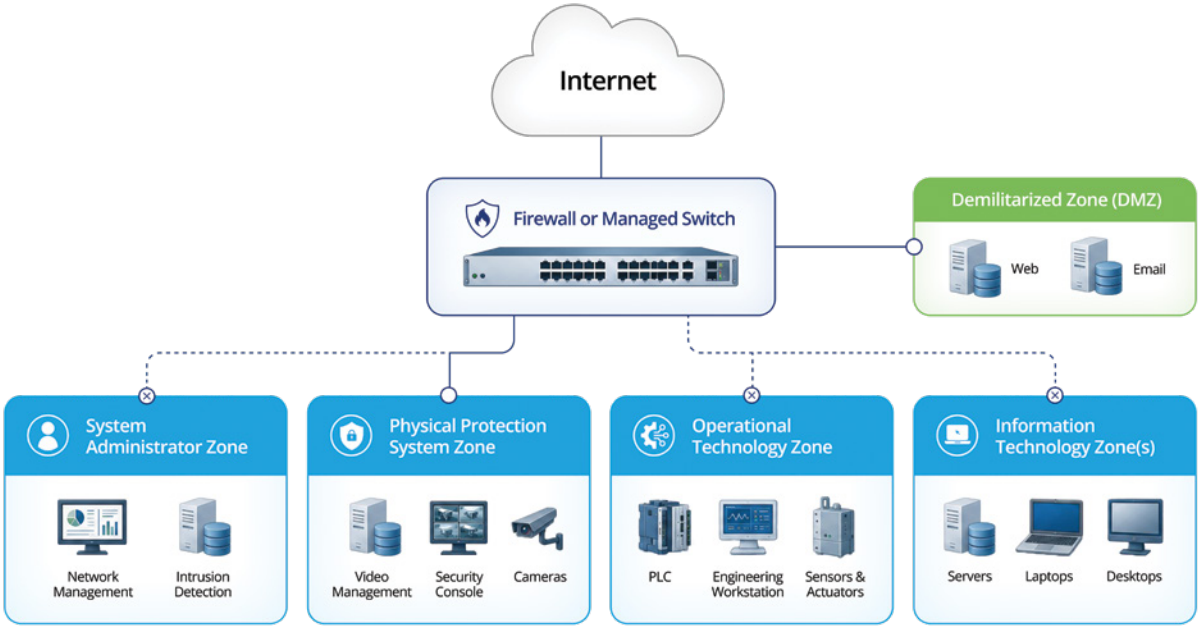
This DCSA template aims at enhancing operational resilience. For a gamma irradiator, where precise control and safety are paramount, the implementation of an alternate, hardened configuration of the firewall[6] is crucial in maintaining secure communication between networks, thus safeguarding the integrity of the entire system.

In addition to prevention, detection mechanisms within a DCSA with an islanded architecture can include:

- Choke points: Monitoring access control behavior to identify potential brute force attacks. Should a breach occur, a cybersecurity incident response plan emphasizes the isolation of non-compromised networks–effectively securing compromised connections–and triaging critical islands to prioritize recovery efforts.
- Incident response: By preparing for incidents with backups, established procedures, and trained personnel, operations can continue smoothly, even in the event of disruptions (malicious or otherwise). A robust framework is created that fortifies defenses against evolving cyber threats while ensuring the safety and reliability of operations.

The concept of an islanded network and fortified by firewalls is depicted in Figure 6 below as noted by the fact that each island is not interconnected as they are in Figure 5. The PPS island retains its connection to the Internet to ensure transmission of alarms to off-site monitoring and response agencies. Any allowed connection to the Internet during a cyberattack needs to be evaluated and strictly controlled.

Figure 6: Islanded Configuration



6 A redundant, fail-over firewall with the alternate configuration is another acceptable approach.

5.1.2 Case Study - Key Benefits of the DCSA Template

The DCSA template was implemented at a Gamma Irradiation Facility, and a follow up self-assessment leveraging a framework published by the iia [26] noted the following key benefits:

1. **Reduction in exposure of overall networks to malicious attack(s)**
   The removal of network branches with significant exposure to external threats reduces the attack surface. This architectural change enhances the protection of workstations responsible for managing sensitive operations, minimizing their exposure by design and reducing risk of attacks having a large impact on the overall organization.

2. **Focused Monitoring of Critical Network Segments**
   The new design enables streamlined and precise monitoring of traffic to and from critical zones. Human and computer resources are no longer wasted analyzing traffic from devices that should not interact with sensitive subnets, improving both performance and security visibility.

3. **Improved Incident Response Capability**
   The segmentation strategy and associated procedures allows targeted response actions during security incidents, minimizing disruption to unaffected operational areas. The response capability that contains attacks by quarantining compromised networks and devices strengthens resilience and shortens recovery time, while keeping the core business running.

4. **Clear Segregation of Networks and Zones**
   The separation of roles and services across distinct VLANs and subnets allows for a clearer overview and more efficient enforcement of security policies simplifying monitoring and sustainment activities. This structured layout also facilitates the design and implementation of effective incident response and disaster recovery plans.

5. **Strategic Placement of Choke Points**
   The introduction of hardened control point at key interconnection nodes enables granular control and continuous monitoring of inter-zone traffic. These choke points serve as security enforcement boundaries and are optimized for logging, alerting, and inspection.

5.2 Physical and Cybersecurity Design Elements

Physical protection consists of measures that are designed to deny or impede unauthorized personnel from physically accessing specific assets, or in this case, radioactive sources. Designing, implementing, and sustaining the physical protection program for radioactive sources are critical steps in ensuring their protection from the required elements for an effective physical protection program are Detection, Delay, } and Response.

"Detect" security enhancements refer to technical measures that are designed to alert personnel that an unauthorized access is occurring. "Delay" security enhancements refer to technical measures that increase the time required for an adversary to enter and gain access to the protected radiological material. For cybersecurity, Delay is generally thought of in terms of the strength of encryption mechanisms because the timeline for an adversary to conduct a cyberattack is probably unknown. "Response" refers to the technical and administrative measures taken following the detection of an unauthorized access to protected radiological materials, such as response of law enforcement. An effective physical protection program requires the integration of people, procedures, and equipment to protect sources from theft or other malevolent attacks to include situational awareness and a strong security culture. This integration should include cybersecurity controls to ensure that security protection elements are not compromised through a cyberattack.

The following table compares typical physical protection measures that are implemented for the protection of radioactive sources to corresponding cybersecurity controls that perform a similar function. Facilities may not need to implement all these measures or controls, but they illustrate their similarities.

Table 5.1: Physical Protection Measures Mapped to Cybersecurity Controls

Similarities Between Physical Protection Measures and Cybersecurity Controls		
Security Function	**Physical Protection Measures**	**Cybersecurity Controls**
Detection	Intrusion Detection Systems • Motion Sensors • Balanced Magnetic Switches Access Controls Video Surveillance Systems On-Site Security Staff Observation Searches Material Inventories Tamper-Indicating Devices Policies, Plans, and Procedures	Cybersecurity Staff Network Intrusion Detection Systems Host Intrusion Detection Systems Anti-Malware Software Security Information and Event Management Systems Critical Alert Emails and Texts Log Files Honeypots/ Sandboxes/Jails Defensive Computer Security Architecture
Delay	Locks Doors Walls Barriers In-Device Delay Tie-Downs Policies, Plans, and Procedures	Cybersecurity Staff Hardware Firewalls Software Firewalls Demilitarized Zone (DMZs)[7] Bastion Hosts[8] Honeypots[9], Honeynets[10], Tarpits[11] Sandboxes[12] Digital system hardening Defensive Computer Security Architecture
Response	On-Site Security Response Alarm Monitoring Law-Enforcement Response Investigations Policies, Plans, and Procedures	Cybersecurity Staff Alarm Monitoring Intrusion Prevention Systems Forensic Investigations Cybersecurity Incident Response Defensive Computer Security Architecture

7 https://csrc.nist.gov/glossary/term/demilitarized_zone
8 https://csrc.nist.gov/glossary/term/bastion_host
9 https://csrc.nist.gov/glossary/term/honeypot
10 https://www.okta.com/identity-101/honeynet/#:~:text=A%20honeynet%20is%20a%20network,contains%20plenty%20of%20monitoring%20tools.
11 https://nordvpn.com/cybersecurity/glossary/tarpitting/?srsltid=AfmBOopGdSnNUBAJIG0Qy6DBNKAj-lF-DHmhhehSWJYM9nf600vIxEJ8
12 https://csrc.nist.gov/glossary/term/sandbox

6. Cybersecurity Program

Establishing, monitoring, and sustaining effective security of radioactive sources requires security, response, administrative, and management elements to work together to create a successful security program that prevents the theft of radioactive sources.

6.1 Program Considerations for PPS

Security enhancements comprise all security system elements (Detection, Delay, and Response) as well as plans, procedures, and training required to operate and sustain security system enhancements. Users of radioactive sources should review their security systems to see what parts of the systems possess IP-based communications and services, as these are potential cyber adversary pathways. Also, facilities should consider attack vectors such as wireless networks, portable interfaces, physical location of devices, and the supply chain. Hardware and software hardening by removing unnecessary programs and blocking unnecessary access ports, such as USB drives and firewall ports, can reduce these potential adversary pathways.

6.2 Security System and Cybersecurity Integration

All security systems contain some form of Intrusion Detection System (IDS), Access Control Systems (ACS), and a method for monitoring alarm states either on-site, off-site, or in many cases, both. The main security system and network-related components and capabilities that are potentially vulnerable to cyberattacks include:

- Alarm concentrators/panels, which communicate to the host using various communications protocols over ethernet, cellular, or a combination of communications means.
- Where very little infrastructure exists, or additional communication channels are desired, alarms can be transmitted via Global System for Mobile Communications/ General Packet Radio Service (GSM/GPRS) or Radio Frequency (RF).
- Analog cameras are giving way to IP cameras, where Power over Ethernet (PoE) is becoming even more commonplace.
- Network infrastructure mainly comprising of switches, midspans (PoE injectors or switches), repeaters, routers (wired and wireless), and firewalls, and in some installations, Wireless Access Points (WAP).
- IP addressable access control/alarm keypads (biometrics, proximity card, pin keypads).
- Application servers' Cloud-based services, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS), etc.
- Remote Access.

Domestic and international systems use security software from multiple vendors that use proprietary protocols and standards that often introduce risks and vulnerabilities into the operating environment. Moreover, software applications are not always compatible, and/or developers do not consider constraints when security software applications are built. All of which increases the potential for system and/or process compromise.

Most alarm sensor devices are currently not IP-addressable and are hard wired into alarm panels; but the security industry is quickly moving to IP-addressable devices and in some cases offering wireless

connectivity. A move to IP-addressable sensor devices will broaden the cyberattack surface by including security system components. In addition, current systems generally use existing telephones or radios for communication that are not integrated into the security system. As current and future systems are built to take advantage of the cost-savings provided by IP networks (such as the use of VoIP to route voice calls), the use of these converged mediums introduce other attack surfaces for adversaries to target that must be addressed through the application of a DCSA.

Examples of controls that are considered industry best practices are detailed in the following sections. Best practices that can be directly tied to developing, maintaining, or sustaining a DCSA are noted with an "x" in the neighboring column within each table.

6.3 Developing a Cybersecurity Program

A cybersecurity program is a necessity to ensure vulnerabilities are not introduced into a physical protection 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 assist with the basics of a cybersecurity program, but professional cybersecurity support may be needed for some of the more technical tasks in developing a comprehensive program.

Table 6.1: Developing a Cybersecurity Program

ORS Best Practice Number	ORS Best Practice Description	Design Relevant
D.1	Designate a person/staff member responsible for cybersecurity with sufficient authority to implement the site cybersecurity program.	
D.2	Evaluate overall cybersecurity hygiene, posture, culture, and awareness level.	
D.3	Develop a defensive cybersecurity architecture – how many levels (unique sets of requirements) and islands (segmented networks and devices)	
D.4	Conduct risk assessment and develop recovery plan	
D.5	Map out all interconnectivities/dependencies including interconnections to other systems.	x
D.6	Determine if physical protection system components are configured into logical security zone with minimum required traffic flows between zones (i.e., islands).	x
D.7	Determine if network-level access controls are implemented on the internal network infrastructure that interconnects physical protection system components.	x
D.8	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.	
D.9	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. The references at the end of this guide can provide further information.	x
D.10	Conduct a best practices evaluation for secure router and switches configuration, management, and operation	
D.11	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.	
D.12	Review overall attack surface, attack vectors, and firewall rules	
D.13	When performing the review keep in mind such items as: • Network terminals vs. workstations. • Restricted connectivity using distributed firewall security zone vs. unrestricted internal network connectivity. • Hardened centralized server configuration vs. distributed server and software implementation	
D.14	Use a vulnerability assessment tool to determine if server systems 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.	
D.15	Conduct penetration testing to validate perimeter security design and implementations. The use of cybersecurity experts is recommended for this activity.	

6.4 Implementing Cybersecurity 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 relatively quick and inexpensive manner. Some of these activities may require support from your IT department, cybersecurity staff, or contracted service provider to implement as they are beyond the skill set expected of a layperson. These activities are included because they are recommended components of a comprehensive cybersecurity program and are activities which can provide business continuity in the aftermath of a cyberattack.

Table 6.2: Implementing Cybersecurity Controls

ORS Best Practice Number	ORS Best Practice Description	Design Relevant
M.1	Enforce strict user accounts with limited role-based permissions. Use the "least privilege" model for access to systems.	x
M.2	Use strong, complex password management and no longer than 6 months aging policies; or use a passphrase. Passphrases are becoming the recommended control instead of passwords. • Minimum of 8 characters, including special characters or use a passphrase	
M.3	Remove unnecessary accounts, software, and processes	x
M.4	Install Anti-Malware software and ensure it is kept current. Be aware that legacy software such as Windows XP or Windows 7 will not be getting updates because these operating systems are no longer freely supported by the vendor.	
M.5	Don't use software that is beyond end-of-life (for instance, Windows XP and 7). New vulnerabilities are often found in this software, but the manufacturer is no longer providing patches.	
M.6	Ensure cybersecurity is included in Site Security Plan with ongoing reviews and is updated following upgrades	
M.7	Ensure facility has an acceptable use policy for employees using company cyber resources. Example policy: https://www.usaid.gov/sites/default/files/documents/1868/545mam.pdf	
M.8	Establish a baseline to identify all equipment, cabling, and circuits. 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.	x
M.9	Ensure patches and firmware are derived from authorized vendors.	
M.10	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	x
M.11	Purchase and use "enterprise" class hardware instead of consumer class components meant for home or small office use.	
M.12	Restrict software and firmware upgrades to authorized system administrators/managers.	x
M.13	Configure web browsers and dedicated e-mail accounts required by alarm management software to limit access to non-system related sites.	x
M.14	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.	x
M.15	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.	
M.16	Disable all unnecessary ports and associated services through hardware and software hardening.	x
M.17	Use Mobile Device Management (MDM) for the administration of mobile devices accessing company networks.	
M.18	Ensure facility has a strategy for the development and implementation of plans, processes, and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber event.	x
M.19	Ensure facility has an active employee security awareness program to potentially include phishing campaigns to test employee security awareness.	x
M.20	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, or at least some means to get the alert to the responsible staff in a timely manner.	x

ORS Best Practice Number	ORS Best Practice Description	Design Relevant
M.21	Enforce network traffic flows in existing firewalls	x
M.22	Utilize existing firewall DMZ as applicable (e.g., drop boxes, DNS, Web server).	x
M.23	Enable port security on network switches, disable unused interface ports, and restrict administrative access.	
M.24	Create ACLs (access control lists) and restrict administrative access.	
M.25	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.	
M.26	Configure multi-zone network security architecture to isolate security protection components into logical layers and zone (i.e., island) as appropriate.	
M.27	Utilize thin-client network terminals instead of Windows workstations where possible to reduce the attack surface, patching requirements, and total cost of ownership.	
M.28	Incorporate traffic encryption for communication over any external networks or telecommunications circuits.	
M.29	Add an intrusion detection system to analyze network traffic. This analysis will identify and alert personnel for attempted cyberattacks via suspicious packets and payloads.	
M.30	Use multifactor authentication (that is phishing resistant, ideally) [22]: • 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.	
M.31	Recommend that prior to deployment any new equipment/components be thoroughly tested for cyber vulnerabilities.	
M.32	Ensure excess computers and media are properly sanitized when disposed.	
M.33	Implement DCSA and controls that support the recovery plan. Verify that recovery processes achieve their objectives and facilitate faster triaging and restoration of PPS(s) without disrupting critical operations.	x

6.5 Sustaining a Cybersecurity Program

The following table provides a checklist for industry best practices that are recommended to sustain an effective cybersecurity program.

Table 6.3: Sustaining a Cybersecurity Program

ORS Best Practice Number	ORS Best Practice Description	Design Relevant
S.1	Implement a configuration management plan and update it regularly.	
S.2	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.	
S.3	Update security plans periodically and after significant changes in your systems or networks.	
S.4	Maintain approved equipment lists including hardware, operating systems, application software, firmware, etc., and their associated revision levels.	
S.5	Update mapping of interdependencies (hardware, software, hosts, and subsystems).	x
S.6	Conduct end-to-end testing performed prior to incorporating new code or technologies.	x
S.7	Implement procedures for upgrades to include comprehensive checklists	
S.8	Manage and maintain software licenses (e.g., some legacy software won't run on new platforms or may introduce cyber vulnerabilities).	
S.9	Regularly update software and ensure that it continues to be supported by the software vendor. This will minimize software cyber vulnerabilities.	
S.10	Run virus scans and update patches on a frequent basis. Automated scans and update may be used but be aware they may impact system performance.	x
S.11	Perform penetration testing to ensure the effectiveness of the hardening and architecture measures implemented during the remediation period. Tests can be tailored to the specific PPS requirements. These tests should be performed by qualified cybersecurity experts and should confirm that networks go into islanded modes in the event of a cyberattack.	x
S.12	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.	x
S.13	Periodically test the recovery plan, which should include contingency planning and backups.	

References

[1] CrowdStrike, "2025 Global Threat Report," CrowdStrike, 2025.

[2] Verizon, "2025 Data Breach Investigations Report," Verizon, 2025.

[3] ORS, "Cybersecurity Best Practices for Users of Radioactive Sources," ORS, 2022.

[4] ISO, "ISO 31000:2018 | Risk Management - Guidelines," International Organization for Standardization, Geneva, 2018.

[5] Unit 42, "Network Threat Trends Research Report (Vol 2.)," Palo Alto Networks, Santa Clara, CA, USA, 2023.

[6] Mandiant, "M-Trends 2023 | Mandiant Special Report," Mandiant, Reston, VA, USA, 2023.

[7] Verizon, "Verizon 2023 Data Breach Investigations Report," Verizon, 2023.

[8] Center for Strategic & International Studies, "Significant Cyber Incidents Since 2006," CSIS, 2024. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[9] R. Forno, "What exactly is Salt Typhoon?," The Center for Internet and Society at Stanford Law School , 7 December 2024. [Online]. Available: https://cyberlaw.stanford.edu/what-exactly-is-salt-typhoon-2/.

[10] L. M. Chang, T. Chen, L. Bermejo and T. Lee, "Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions," Trend Micro, 25 November 2024. [Online]. Available: https://www.trendmicro.com/en_us/research/24/k/earth-estries.html?ref=cyberlaw.stanford.edu.

[11] Government Technology, "Back to Basics: A Deeper Look at the Colonial Pipeline Hack," Government Technology, 8 July 2021. [Online]. Available: https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack.

[12] K. Wood, "Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack," The Georgetown Environmental Law Review, 7 March 2023. [Online]. Available: https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/#:~:text=Colonial%20Pipeline%20shut%20down%20its,work%20to%20restart%20the%20pipeline.

[13] A. Waldman, "10 of the biggest ransomware attacks in 2024," Tech Target, 30 December 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/news/366617564/10-of-the-biggest-ransomware-attacks-in-2024.

[14] U.S. Energy & Commerce Committee, "What We Learned: Change Healthcare Cyber Attack," U.S. Energy & Commerce | Chairman Guthrie, 3 May 2024. [Online]. Available: https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack.

[15] D. Zakreski, "Ransomware attack on eHealth forces 31 cancer patients to re-schedule radiation treatment," CBC, 15 January 2020. [Online]. Available: https://www.cbc.ca/news/canada/saskatoon/ransomware-attack-ehealth-cancer-patients-1.5428346.

[16] K. Randolph and M. Hunt, "Summary: March 9, 2021 Security Incident Report," Verkada, 21 May 2021. [Online]. Available: https://www.verkada.com/security-update/report/.

[17] K. Lafalaise, "FTC Says Surveillance Camera Company Verkada Has A Lotta Explaining To Do After Lax Data Security Practices and More," FTC, 30 August 2024. [Online]. Available: https://www.ftc.gov/business-guidance/blog/2024/08/ftc-says-surveillance-camera-company-verkada-has-lotta-explaining-do-after-lax-data-security.

[18] President of the United States, "Transnational Organized Crime: A Growing Threat to National and International Security," U.S. National Security Council, Washington, DC, USA, 2011.

[19] L. Frye, S. Lohmann, P. J. Milas, M. W. Parrott, S. Sim, S. S. Sin and K. J. Wheaton, Emerging Technologies and Terrorism: An American Perspective, S. Sim, E. Hartunian and P. J. Milas, Eds., Carlisle, PA: US Army War College Press, 2024.

[20] IAEA, "NSS No. 8-G - Preventive and Protective Measures Against Insider Threats," IAEA, Vienna, 2020.

[21] M. Kosinski, "What is smishing?," IBM, 10 June 2024. [Online]. Available: https://www.ibm.com/think/topics/smishing.

[22] Cybersecurity & Infrastructure Security Agency, "Phishing-Resistant Multi-Factor Authentication (MFA) Success Story: USDA's Fast IDentity Online (FIDO) Implementation," CISA, Washington, DC, USA, 2024.

[23] IAEA, "NSS No. 20 - Objective and Essential Elements of a State's Nuclear Security Regime," IAEA, Vienna, 2013.

[24] L. Maccarone, M. Rowland, R. Brulles and A. Hahn, "Advanced Reactor Safeguards & Security: Design of Defensive Cybersecurity Architectures for High Temperature, Gas-Cooled Reactors (SAND2024-11449R)," Sandia National Laboratories, Albuquerque, NM, USA, 2024.

[25] CISA, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and – Default," Cybersecurity and Infrastructure Security Agency, Washington, DC, USA, 2023.

[26] International Irradiation Association, "Guide for Assessing Cybersecurity Programs at Gamma Irradiation Facilities," iia, Ludlow, England, 2025.

[27] IAEA, "NSS No. 17-T (Rev. 1) - Computer Security Techniques for Nuclear Facilities," IAEA, Vienna, 2021.

[28] IAEA, "NSS No. 33-T - Computer Security of Instrumentation and Control Systems at Nuclear Facilities," IAEA, Vienna, 2018.

[29] IAEA, "NSS No. 42-G - Computer Security for Nuclear Security," IAEA, Vienna, 2021.

[30] ISA, "ISA/IEC 62443 Series of Standards," International Society of Automation, [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[31] ISO, "ISO/IEC 27000 Family - Information Security Managment," International Organization for Standardization, [Online]. Available: https://www.iso.org/standard/iso-iec-27000-family.

Appendix A

The following sources have been provided for additional reading and are listed in no specific order.

1. ICS-CERT—The Industrial Control Systems Cyber Emergency Response Team. https://www.cisa.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jul-Aug2011.pdf
2. National Cybersecurity Institute (NCI). http://www.nationalcybersecurityinstitute.org/
3. Center for Internet Security (CIS). https://www.cisecurity.org/
4. NIST Cybersecurity Framework. (2.0) http://www.nist.gov/cyberframework/
5. Department of Homeland Security. https://www.dhs.gov/topic/cybersecurity
6. UK National Protective Security Authority. https://www.npsa.gov.uk/
7. CIS Critical Security Controls. https://www.cisecurity.org/controls
8. CWE Top 25 Most Dangerous Software Errors. https://www.sans.org/top25-software-errors/
9. World Institute for Nuclear Security, Cybersecurity in the Nuclear Industry. https://www.wins.org/document/cybersecurity-in-the-nuclear-industry/
10. IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf
11. NRC Backgrounder on Cyber Security.
12. https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html
13. International Atomic Energy Agency. (2016). Computer Security for Nuclear Security NSS No. 42-G, Implementing Guide. https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf
14. International Atomic Energy Agency. (2020). Preventive and Protective Measures Against Insider Threats, Implementing Guide. Nuclear Security Series, No. 8-G (Rev. 1). https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858_web.pdf
15. International Atomic Energy Agency. (2018). Computer Security of Instrumentation and Control Systems at Nuclear Facilities NSS-33T. https://www.iaea.org/publications/11184/computer-security-of-instrumentation-and-control-systems-at-nuclear-facilities

iiaglobal.com