EXAMINING CYBERSECURITY VULNERABILITIES

AND COUNTER-MEASURES TO COMBAT

THE INSIDER THREAT

IN RADIOLOGICAL SECURITY

J. WISE

Pacific Northwest National Laboratory

Richland, WA, United States of America

Email: jaime.wise@pnnl.gov

B. GORTON

Pacific Northwest National Laboratory

Richland, WA, United States of America

M. HAZEL

Pacific Northwest National Laboratory

Richland, WA, United States of America

B. HIGGINS

Pacific Northwest National Laboratory

Richland, WA, United States of America

**Abstract**

The U.S. Department of Energy/National Nuclear Security Administration’s Office of Radiological Security (ORS) collaborates with partner countries throughout the world to enhance the security of radioactive sources used for legitimate purposes [1]. The partner stakeholders’ environments consist of operators using ionizing radiation for medical, industrial, and research applications. In each of those domains, the risk of an insider is ever-present within the spectrum of threats and threat agents. With the continued advancement of security technology and the proliferation of networked security components, security practitioners are using new capabilities to greatly enhance detection, assessment, and response security functions. However, as systems increase in the level of integration and complexity, such as those either connected to or riding directly on a site’s information -technology (IT) network, those same security practitioners must remain vigilant of the associated risks to the confidentiality, integrity, and availability of the data being communicated. IAEA Nuclear Security Series No. 11, Security of Radioactive Sources, outlines security objectives for the various security functions of detection, delay, and response [2]. NSS-11 also emphasizes the importance of understanding the threat environment including the threats proliferated by insiders with intent to acquire radiological material. As the security systems continue to evolve, satisfying the recommendations of NSS-11 necessitates placing a greater emphasis on insider mitigation through the strategic identification, selection, and implementation of administrative, technical, and physical controls to address the cyber vulnerabilities. One solution being explored by ORS is the development of a cloud-hosted architecture to streamline IT communications, ensure delivery of critical alarm notifications, and ultimately optimize the response timeline of interrupting the adversary. The paper explores the challenges posed by the cyber vulnerabilities present in such an architecture and proposes security controls to mitigate targeted risks.

## INTRODUCTION

The Office of Radiological Security (ORS), an organization within the US Department of Energy’s National Nuclear Security Administration Office of Global Material Security, assists partner countries in implementing their security commitments under the International Atomic Energy Agency (IAEA) Code of Conduct on the Safety and Security of Radioactive Sources. One of the greatest challenges ORS and its partners face in radiological security is that of the insider threat. Radiological sources are often used at medical facilities, research laboratories, or industrial installations where access control is exceptionally difficult. ORS has previously implemented a network-based Remote Monitoring System (RMS) to mitigate the insider threat at facilities it protects.

Off-site monitoring of security alarms provides some assurance that an insider’s attempts to gain unauthorized access to the source will be detected and a response initiated. A persistent challenge with off-site monitoring is that it is heavily dependent upon reliable communications. Limitations of the underlying system’s infrastructure – public switched telephone network, Internet, and cloud-based options, as examples currently available in industry – may limit the confidentiality, integrity, and availability of the data being communicated across those systems. As a result, the modern, networked security system must consider physical security from a cyber-security perspective and vice versa. Key first steps include policy and procedural measures to close fundamental gaps in cyber security and enable the successful implementation of networked security systems to detect and respond to malicious acts.

While certain aspects of security are immutable, technological advances have driven both security system designers and adversaries to modify their respective approaches. With the continued advancement of security technology and the proliferation of networked security components, security practitioners are using new capabilities to greatly enhance detection, assessment, and response security functions. However, as systems increase in the level of integration and complexity, such as those either connected to or riding directly on a site’s information-technology (IT) network, those same security practitioners must also remain vigilant of the associated risks.

The paper will examine a cloud-based mechanism for augmenting detection and response capabilities within a security system and will also examine the considerations for addressing cyber vulnerabilities which are introduced concurrently with network-based security solutions.

## DETECTION AND RESPONSE: CHALLENGES AND SOLUTIONS

Radiological source security presents unique challenges when it comes to designing and implementing a system to perform the key security functions of detection, delay and response. Many facilities where radiological sources are used require frequent, if not constant, access to the radiological source. Whether treating patients, facilitating research, or performing high through-put industrial irradiation activities, the number and frequency of operational tasks makes it difficult to confidently and effectively implement access controls, detect adversaries, or delay an adversary from advancing along their attack pathway leading to a radiological source target. This problem is dramatically compounded when attempting to mitigate the insider. As ORS grappled with this reality, it developed a network-based security enhancement known as the Remote Monitoring System (RMS) to neutralize the game-changing impact of an insider on the adversary timeline [3]. The RMS provides tamper-resistant detection of unauthorized access and responds by sending an automated alarm notification directly to identified staff, such as an off-site alarm monitoring station. This is an effective means of reducing the risk that an insider may disable or bypass detection components of the physical protection system. Similarly, the RMS provides redundant alarm prompts to ensure off-site responders are informed of the developing situation. An example of an RMS is shown in Fig. 1[3].



FIG. 1. Sentry-RMS

With the maturation of the ORS program and its experience in integrating off-site responders with the on-site physical security systems that guard radiological sources, a persistent gap became evident. Analyses of physical security systems revealed a very brief adversary task timeline. Efforts to avoid adversely impacting operational requirements limit the methods by which physical security systems can be augmented to improve the detection and delay capabilities necessary to guarantee a sufficiently timely and adequate response by off-site responders. In its effort to solve this problem, ORS, has turned to technology for part of the answer.

If a physical security system performs three functions, and the first two of those functions – detection and delay – are subject to inherent limitations in the radiological security domain, the effectiveness of the security system depends heavily upon successful improvement of the third function – response. With the intent of improving the speed that law enforcement responders can effectively interrupt a malicious act, ORS is pursuing a cloud-based application called, Sentry-RMS Communications and Response Platform, or “Sentry-SECURE.” Sentry-SECURE is intended to enhance existing alarm monitoring strategies at a facility by transmitting high-priority alarms associated to malicious acts involving radiological sources directly to law enforcement agencies [4]. This capability, operating concurrently with established alarm adjudication procedures at the facility, streamlines the transmission of alarm signals by eliminating exclusive reliance on an emergency operations center or alarm monitoring station to process, adjudicate, and transmit alarm signals to responders.

In a further effort to afford responders every possible advantage, Sentry-SECURE will also provide the capability for alarm and video signals to be sent directly to a responder’s mobile platform, whether it is a vehicle-mounted device, a tablet, or a mobile telephone. This will further reduce the time necessary to communicate key alarm information to responders in the field and will simultaneously ensure real-time situational updates regarding the adversary and the ongoing malicious act. An architecture diagram for Sentry-SECURE is shown in Fig. 2 [5].



## TECHNOLOGY SOLUTIONS AND RELATED TECHNOLOGY VULNERABILITIES

Both the Remote Monitoring System (RMS) and Sentry-SECURE use modern technology to combat the insider threat and to maximize the effectiveness of off-site response resources. Like other technological improvements that enhance security, the maturation of IT and the use of networked systems simultaneously pose the risk of introducing new vulnerabilities. Such vulnerabilities may yield unconventional adversary pathways that mandate controls be implemented to mitigate the risk. Neither the RMS nor Sentry-SECURE represent the genesis of this challenge; rather, their deployment simply serves to further underscore the need to address vulnerabilities related to information technologies and networked systems that may undermine perceived security for radiological sources.

### The cyber-physical nexus for security

Traditional physical security continues to merge with information technology, often resulting in a cycle of implementation, innovation, redesign, and additional implementation. This is represented in Fig. 3 below as a cyclical process that is consistent with and occurs in parallel to other industry norms. Specific examples include continuous improvement for risk management and as low as reasonably achievable for exposure to radioactive substances.

*FIG 3. Implementation, innovation, and redesign as a cyclical process*

As a result, physical protection systems are becoming part of the broader classification of hardware and software known as “operational technology.” Many of the ORS security upgrades such as access controls, intrusion detection, and video assessment systems, and the RMS, are increasingly dependent on the networks and cybersecurity capabilities of the underlying infrastructure. This predictably leads to concern that an adversary could use a cyberattack to override a facility’s existing network controls and physical security measures, facilitating a physical attack resulting in unauthorized and/or undetected access to radioactive sources. Both the RMS and Sentry-SECURE effectively mitigate this concern. If not properly implemented and maintained, however, both capabilities may also present opportunities for cyber-savvy adversaries to exploit new vulnerabilities in the security architecture. Consequences of such an attack may degrade critical detection, assessment, or response elements such that an attack pathway previously confirmed to be unlikely is made more attractive to the adversary.

### Tackling cyber-security vulnerabilities

Information technology and networked systems have significantly evolved the range of tools available to effectively detect, assess, and respond to the threat posed by an insider in the radiological source security context. Security professionals and site operators cannot, however, simply rest on their current, near term success. In the ongoing evolution of the security domain, as complicated by the influence of cybersecurity vulnerabilities, ORS has turned its attention to addressing those gaps.

As one component of the programmatic initiative, ORS developed guidance for its implementation teams to identify and clearly communicate the objectives in the area of cybersecurity. Among the resources deployed by the program are three resources highlighted below – the Cybersecurity Best Practices for Users of Radioactive Sources, Cybersecurity Procurement Requirements for ORS-Provided Security Systems, and the Physical Protection Specialists’ Cybersecurity Pocket Guide (Fig. 4). A brief description of each identified resource has been included below.

* **Cybersecurity Best Practices for Users of Radioactive Sources [6]**

*Identifies and characterizes cybersecurity best practices that are applicable to the radiological security domain. Accounts for the unique and challenging environments that ORS-partner stakeholders operate in.*

* **Cybersecurity Procurement Requirements for ORS-Provided Security Systems [7]**

*Provides an initial collection of cybersecurity enhancements that may be applicable. While valid to initially consider, not all enhancements are appropriate for all sites. Specific enhancement implementation is contingent upon a security assessment to evaluate the unique site and asset pairing.*

* **Physical Protection Specialists’ Cybersecurity Pocket Guide [8]**

*Enumerates specific subtasks found within the Procurement Requirements document to explore possible steps that the contractor and regional team may use to assure and verify the scope has been completed correctly. Specific enhancement implementation assurance is contingent upon site-specific details.*



*FIG. 4. Cybersecurity resources available to implementation teams*

Through the development and deployment of these resources, two primary objectives stewarded the process - reduce the attack surface and ensure the integrity of security-related devices and communications. Reducing the attack surface involves decreasing the cumulative vulnerability that an adversary may be able to exploit relative to a given asset. From a cybersecurity perspective, this may include removing unnecessary software from a workstation, closing excess ports on a network appliance, or implementing network segmentation and isolation. Complementing this objective, it is critical that alarm and video signals are transmitted without a loss of data whether due to nefarious intent or accidental data corruption. This enables effective alarm adjudication and, if necessary, the dispatch of a response force. Success in these objectives requires that enhancements be made to the physical security, cybersecurity, and information technology domains as well as those that span the traditionally separate topical areas.

In order to meet the identified objectives, twelve cybersecurity topical areas were characterized. Each plays an important role in mitigating a blended, cyber-enabled physical attack that may facilitate nefarious acts. While all the domains do not apply universally to security at all sites, these are the areas identified for specific attention when developing and evaluating a site’s physical protection system:

1. Software and Services
2. Access Control
3. Account Management
4. Session Management
5. Authentication (and Password) Policy and Management
6. Logging and Auditing
7. Communication Restrictions
8. Malware Detection and Protection
9. Reliability and Adherence to Standards
10. Vulnerabilities
11. Network Intrusion Detection
12. Wireless Technology Provisions

For each domain, ORS has identified a range of specific measures to be implemented by operators to help mitigate the cyber risks inherent in the physical protection system that often depend on IT networks for effective implementation, operations, and maintenance.

## CHALLENGES IN ADDRESSING CYBER VULNERABILITIES

Success in the cybersecurity domain is both challenging to achieve and difficult to confirm. Challenging in that the adversary likely has infinite resources, primarily time, to carry out passive forms of reconnaissance, often waiting for a single misstep to yield a critical piece of information. Success is also difficult to confirm because a bad actor who is committed to carrying out illicit activity may be intent on remaining covert or undetected, taking steps to cover their tracks to slow or even prevent detection, investigation, and attribution. Nonetheless, should successful security be achieved, maintaining it is embattled by factors such as staff attrition, a dynamic threat environment, and complacency, the latter being the greatest source of risk. In this predicament, the best mitigation strategy is to design and implement a multidisciplinary, layered architecture of security controls that spans multiple security domains. Starting with the most critical security domain, physical security must be robust in order to realize success in the complementary domains. Once physical security is established and maintained, the overall security posture may be further enhanced by making enhancements within domains such as cybersecurity, information security, information technology, and operational security, among others.

If designed correctly, a single failure of any one security sensor, policy, procedure, or related resource should not permit an unauthorized individual from gaining access to radiological material. Rather, the concentric layers of administrative, technical, and physical security controls work together to compensate for vulnerabilities at the individual component level. This approach may also mitigate the effects of limited resources by shifting emphasis from a constrained element of the physical protection system to one capable of carrying the additional importance. A specific example would be a site constrained by a shortage of monetary funds, thus substantially limiting access to advanced physical security systems. In this case, a more robust architecture of policies, procedures, and staff training may be pursued to reach an equal level of security. From another perspective, this same example may shift emphasis from expensive technical controls, such as an advanced alarm management system, to more administrative controls, such as a robust insider threat detection program and a two-person requirement.

## cONCluSION

Ultimately, an approach to realizing sustainable success with cybersecurity and the insider threat in the radiological security domain requires, at a minimum, two elements – time and saturation. There are many elements working against a site that maintains radiological material. At a fundamental level, change is not easy. In fact, it is often met with overt opposition. Software updates may be released monthly, new capabilities or features may be desired, or products may reach the end of their lifecycle and need to be replaced. Simply put, the cybersecurity domain requires a constant, unyielding ability to adapt to change over time. This, combined with the fact that cybersecurity largely consists of intangible and unintuitive attributes defined by strings of 1s and 0s, makes both immediate and long-term success challenging. However, through an appropriate balance of technology, policies and procedures, and training, cybersecurity vulnerabilities can be effectively mitigated to thwart the insider threat.

References

[1] ORS Staff, Office of Radiological Security (ORS) National Nuclear Security Administration (2019),

<https://www.energy.gov/nnsa/office-radiological-security-ors>

[2] International Atomic Energy Agency, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[3] ORS Staff, “Section 5.7 Remote Monitoring System,” Implementation Guidelines, Office of Radiological Security (2018).

[4] WISE, J. and B. GORTON. Sentry-SECURE Conceptual Proposal, internal report, Pacific Northwest National Laboratory, 2019.

[5] WISE, J. and B. GORTON. Sentry-SECURE Outreach Flier, internal report, Pacific Northwest National Laboratory, 2019.

[6] ORS Staff, Cybersecurity Best Practices for Users of Radioactive Sources, Office of Radiological Security (2018).

[7] ORS Staff, Cybersecurity Procurement Requirements for ORS-Provided Security Systems, Office of Radiological Security (2018).

[8] ORS Staff, Physical Protection Specialists’ Cybersecurity Pocket Guide, Office of Radiological Security (2018).

PNNL-SA-149452