JANUARY 2018

Cybersecurity Best Practices for Users of Radioactive Sources

ORS
Office of Radiological Security
Protect · Remove · Reduce

National Nuclear Security Administration

Cybersecurity Best Practices for Users of Radioactive Sources

January 2018

The National Nuclear Security Administration's (NNSA) Office of Radiological Security (ORS) works with governments, law enforcement, and businesses across the globe to improve radiological security by providing world class security upgrades, expertise, training, source recovery, and alternative technology strategies to users of radioactive sources. ORS has both domestic and international programs and is working in all 50 states and collaborating with over 80 countries.

The Office of Radiological Security (ORS) works to enhance global security by preventing high-activity radioactive materials from use in acts of terrorism.

ORS employs the following three strategies:

PROTECT radioactive sources used for vital medical, research, and commercial purposes.

REMOVE and dispose of disused radioactive sources.

REDUCE the global reliance on radioactive sources by facilitating replacement with viable alternative technologies.

ORS provides industry, government, and law enforcement with training, services and security upgrades that provide enhanced security of high-activity radioactive sources used for vital medical, research and commercial purposes.

ORS
Office of Radiological Security
Protect · Remove · Reduce

National Nuclear Security Administration

TABLE OF CONTENTS

Cybersecurity Best Practices for Users of Radioactive Sources

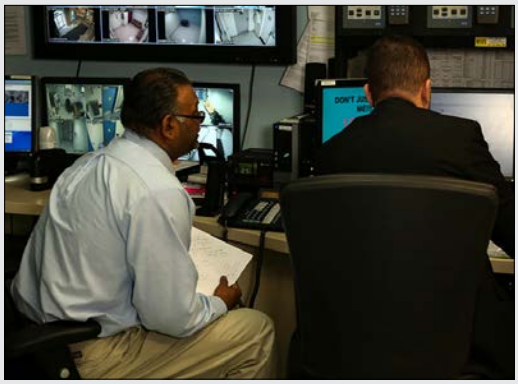
Background

1. OVERVIEW

Radioactive sources play an important role in commercial, medical and research applications — but to ensure global security, the benefits of these materials must be balanced with security. ORS collaborates worldwide with a broad range of partners including government regulatory authorities, responders, industry, and international organizations to enhance the security of high-risk radioactive sources. This first line of defense initiative helps prevent unauthorized access to materials that could be used in a radiological dispersal device ("dirty bomb"). ORS focuses its resources on the security of high activity sources including cesium-137, cobalt-60, americium-141, and iridium-192 used in facilities such as hospitals, universities, sterilization facilities, and industry.

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

Users of radioactive sources that are part of large organizations such as research institutes, universities, medical facilities, or large companies may have cybersecurity programs. Smaller organizations may rely on IT staff, contractors, or perhaps may have to perform these duties themselves. Regardless of your particular situation, this best practices guide provides you with information to counter potential cyber threats to your radioactive sources.



Boston Marathon Bombings.
Area of the first blast a few minutes after explosion. Photo by Dave Bowman

THE THREAT

Recent events such as the Boston Marathon bombing, the San Bernadino, California attacks, the attacks in Paris and Brussels, and arrests of "Lone Wolf" individuals plotting to commit acts of terrorism demonstrate the continued and evolving threat of terrorism. Cyberattacks are an emerging threat vector for radiological security as burglar alarm, video, and access control systems migrate to using networks for their communications.

Below are examples of evolving cyber threats to operational technologies* (OT). Although these examples may not directly involve a theft of radioactive sources by using cyber methods, they do illustrate the attack methods and areas of weakness that could be potentially exploited.

EXAMPLES OF EVOLVING CYBER THREATS TO OPERATIONAL TECHNOLOGIES (OT)		
Event	OT Cyber Threat Examples	Threat
Global 2017	Worldwide cyberattack by WannaCry ransomware targeting the Microsoft Windows operating system, encrypting data and demanding ransom payments. The attack has been described as unprecedented in scale infecting more than 230,000 computers in over 150 countries. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack	Ransomware
Global 2016	Internet of Things (IoT) devices have been used to create large-scale botnets — networks of devices infected with self-propagating malware — that can execute crippling distributed denial-of-service (DDoS) attacks. The IoT devices affected in the latest Mirai incidents were primarily home routers, network-enabled cameras, and digital video recorders. https://www.us-cert.gov/ncas/alerts/TA16-288A.	DDoS
United States Feb 2016	Hollywood Presbyterian Medical Center was off-line for more than a week as a ransomware attack disabled networked computers for 10 days until the ransom was paid. Barbara Hollingsworth, February 25, 2016. http://cnsnews.com/blog/barbara-hollingsworth/la-hospital-attacked-ransomware-paid-hackers-unlock-system.	Ransomware
United States 2015	TrapX Security found attackers had compromised a C-ARM X-Ray system via email and then pivoted off of the X-Ray device to each Hospital sub-network that it was connected to as it was moved around to various patient locations throughout the facility acting as a host for the advanced persistent threat, immune to regular IT security deployments. https://trapx.com/wp-content/uploads/2017/08/Case_Study_TrapX_Healthcare_MEDJACK_X-RAY.pdf	Protocol
Global 2014	Scottish firm Future Technology Devices International (FTDI) pushed an updated driver for devices that use the FT232 chipset, which converts RS-232 (UART) to USB. The update leaves devices that use counterfeit FTDI chips in an unusable & unrecoverable state. James Sanders, October 25, 2014, Tech Republic.	Supply Chain Risk Management (SCRM)
Belgium Antwerp 2013	During a two-year period, drug gangs concealed heroin inside legitimate shipping cargoes. The gang infiltrates IT systems controlling the movement and location of containers. They were then able to identify which containers contained the drugs and send in lorry drivers to steal them. http://www.ship-technology.com/features/feature-cybersecurity-port-computer-hackers-us-belgium/	Protocol

* Operational technology is defined as hardware and software that monitors and controls how physical devices perform. Physical security and surveillance systems can be considered operational technologies.

The IBM X-Force Threat Intelligence Index 2017 looked at publicly disclosed security events in 2016, finding that the industries experiencing the highest number of incidents and reported records breached were information and communications, and government. It is worth noting that the healthcare industry, which fell just outside the top five in terms of records breached, continued to be beleaguered by a high number of incidents. However, attackers focused on smaller targets, resulting in a lower number of leaked records in that industry, https://securityintelligence.com/media/ibm-x-force-threat-intelligence-index-2017/.

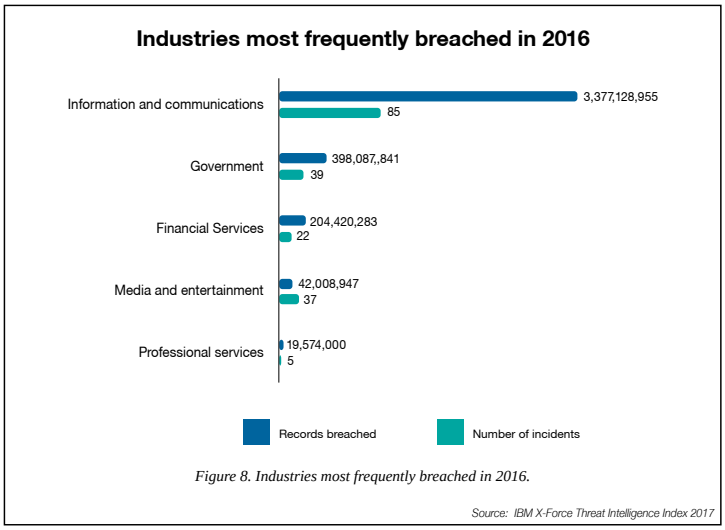
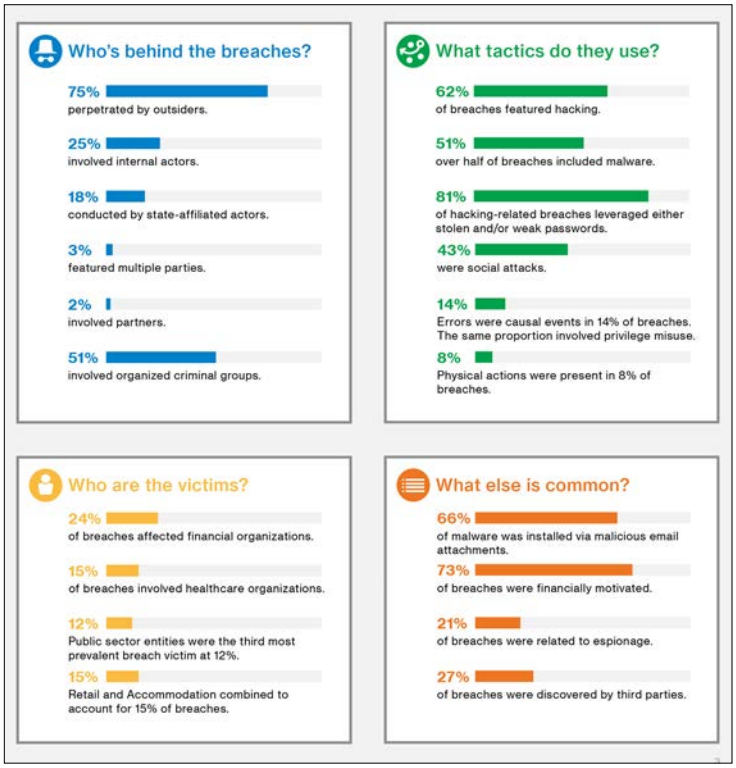


Figure 8. Industries most frequently breached in 2016.

Source: *IBM X-Force Threat Intelligence Index 2017*



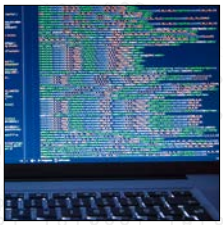
The Verizon 2017 Data Breach Investigations Report describes trends in data breaches researched by Verizon and its DBIR partners. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

WHAT IS THE CONCERN?

The primary cybersecurity concern is an adversary who could use a cyberattack to override a facility's existing network controls and security measures, allowing them to facilitate a physical attack, which could result in unauthorized and/or undetected access to radioactive sources.

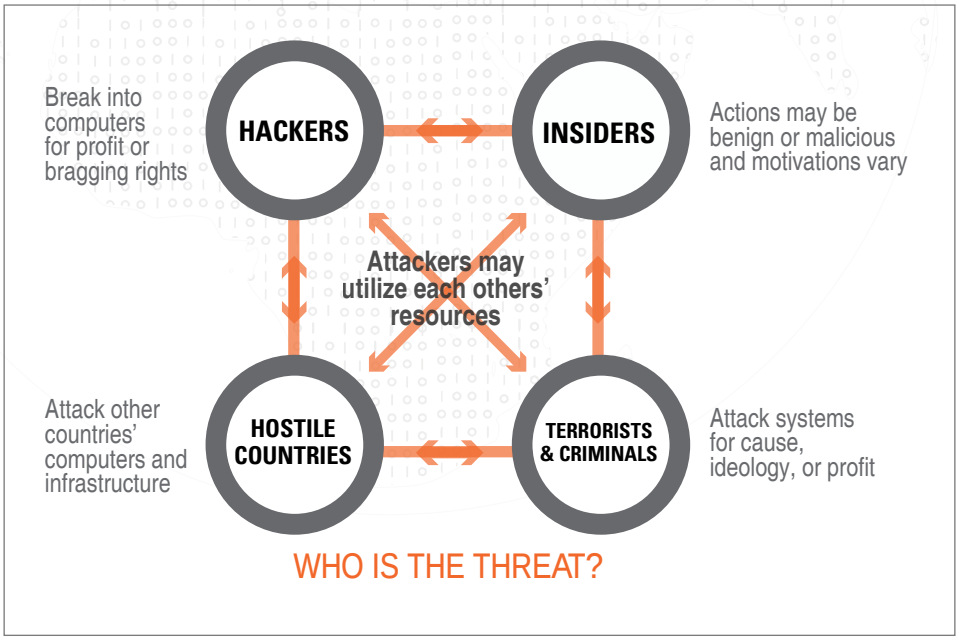
CONCERNS ALSO INCLUDE:

An adversary exploiting security equipment to gain access to a site's network(s) to carry out a cyberattack such as installing ransomware or stealing proprietary or other sensitive information.



Cyberattacks could be used to manipulate or sabotage equipment and processes that use radioactive sources.

Social engineering could be used to exploit insiders to gain access to physical security systems, networks, and related subsystems without the need to hack or conduct a cyberattack using cyber tools.



WHO IS THE THREAT?

BASIC CYBERSECURITY PRINCIPLES

Security is a process

Every system has vunerabilities

Impossible to eliminate all of them

SYSTEMS CHANGE OVER TIME
- Security requirements change over time
- Systems change over time

SYSTEMS REQUIRE MAINTENANCE
- Check for defunct users
- Update virus software
- Patch security holes
- Test firewalls

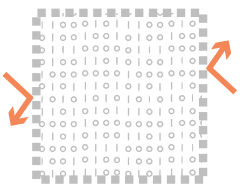
GOAL: ASSURANCE

ICA

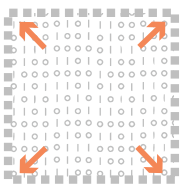
INTEGRITY
CONFIDENTIALITY
AVAILABILITY

Different kinds of security are required for different types of problems and data

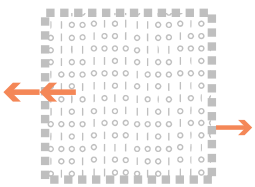
The principle of ALARA, "as low as reasonably achievable," applies to cybersecurity as well as radiation safety by limiting exposure.



INTEGRITY
- No improper modification of data
- Is data reliable?
- Enforcement is access control, digital signatures, etc.



CONFIDENTIALITY
- Protect information from improper release
- Who is authorized to see the data?
- Hard to enforce after being penetrated
- Enforcement is through cryptographic methods



AVAILABILITY
- Is the system available as designed to meet requirements?
- Can the system respond to requests?
- Enforcement is through authentication and authorization

Cybersecurity Recommendations

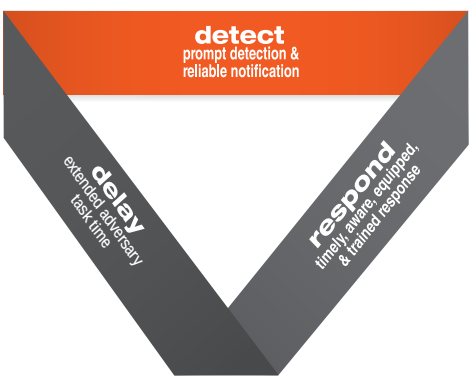
2. COMMON DESIGN AND IMPLEMENTATION CONSIDERATIONS

Designing and implementing effective security of radioactive sources requires security, response, administrative, and management elements work together in order to have a successful security program that prevents the theft of radioactive sources. Increasingly, security systems are moving to Internet Protocol (IP)-based components which means that cybersecurity must be considered when implementing physical security programs.

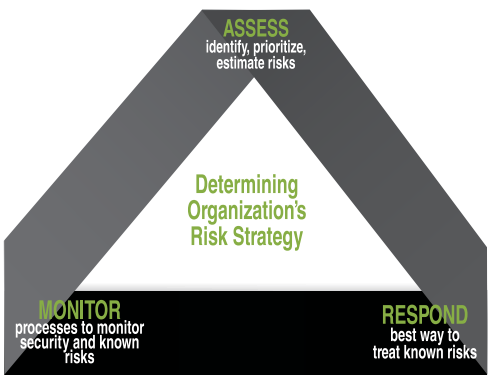
2.1. PHYSICAL AND CYBERSECURITY DESIGN AND PROTECTION ELEMENTS

Physical security consists of measures that are designed to deny or impede unauthorized personnel from physically accessing specific assets, in this case radioactive sources. Designing, implementing, and sustaining the physical security program for radioactive sources are critical steps in ensuring their protection from malicious use. An effective physical security program requires the integration of people, procedures, and equipment to protect sources from theft or other malevolent attacks. This integration should include cybersecurity controls to ensure that security protection elements are not compromised through a cyberattack.

The required elements for an effective physical security 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. "Response" refers to technical and administrative measures taken following the detection of an unauthorized access to protected radiological materials such as response by law enforcement.



Security Protection Elements



NIST Risk Management Process

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

Similarities between Physical Security Measures and Cybersecurity Controls		
Security Function	Physical Security Measures	Cybersecurity Controls
Detection	Intrusion Detection Systems — Motion Sensors — Balanced Magnetic Switches Access Controls Video Surveillance Systems Onsite Security Staff Observation Searches Material inventories Tamper indicating devices	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
Delay	Locks Doors Walls Barriers In Device Delay Tie-downs	Cybersecurity staff Hardware firewalls Software firewalls Demilitarized Zones (DMZs) https://en.wikipedia.org/wiki/DMZ_(computing) Bastion Hosts https://en.wikipedia.org/wiki/Bastion_host Honeypots/Honeynets/Tarpits https://en.wikipedia.org/wiki/Honeypot_(computing); https://en.wikipedia.org/wiki/Tarpit_(networking) Sandboxes https://en.wikipedia.org/wiki/Sandbox_(computer_security) Digital system hardening
Response	Onsite security response Alarm monitoring Law enforcement response Investigations	Cybersecurity staff Alarm monitoring Intrusion Prevention Systems Forensic investigations Cybersecurity Incident Response

These security elements must be implemented in a manner such that adequate response arrives within a period of time that is less than the time required for the adversary to complete their objective (i.e., theft of the source).

2.2. PHYSICAL SECURITY DEVICES WITH POTENTIAL CYBERSECURITY CONCERNS

The blending of physical protection systems with information technology is advancing at such a rapid pace that the two can no longer be viewed independently or separately. Security systems are evolving from stand-alone hardwired devices to network-based devices where both power and data may be provided by a single Ethernet cable. This is the same type of evolution of phone systems moving from landline copper wires to Voice over Internet Protocol (VoIP) that is common in many offices today.

The following physical security devices increasingly use network-based communications that can increase a site's potential for a cybersecurity attack. IT and/or cybersecurity staff can help you identify which of your physical security devices use site networks or other IP-based communications and could potentially be an attack surface for an adversary. Isolation and segmentation of security systems on site networks through measures such as Virtual Local Area Networks (VLANS) can address many potential security issues and is highly recommended.

Security cameras

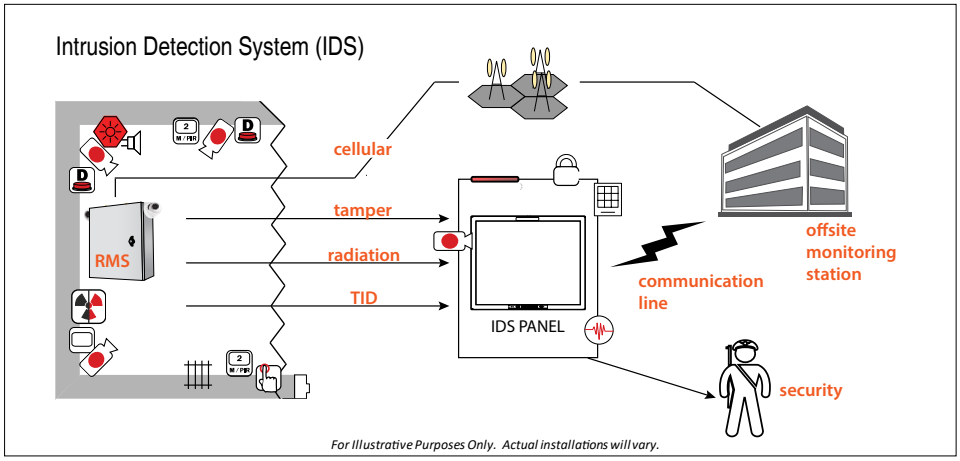
Siren and camera

Access Control

Access control measures enable facilities to implement systems and procedures to deny access to unauthorized persons to target rooms while allowing access by authorized individuals. A biometric access control device on the access door(s) to the device room is recommended to prevent an authorized person from providing their access credentials (e.g., badge and PIN code) to an unauthorized person. Common biometric systems include fingerprint or handprint readers, hand geometry readers, iris readers, retinal readers, and hand vascular pattern recognition readers. Other access control options such as using a PIN, proximity card, or PIN and a proximity card may be appropriate instead of a biometric device depending on the site's security needs.

Intrusion Detection System

An Intrusion Detection System is designed to detect an adversary before they reach the radioactive source. Security vendors can recommend the best types of alarm sensors for inclusion in an Intrusion Detection System, but sensors should be commercial quality like



what would be used in a bank or other facility with high value assets. The typical home burglar alarm sensors should be avoided. Tamper indicating devices such as Radio-frequency identification (RFID) tags could be included as components of an intrusion detection system.

Cybersecurity concerns include the method of signal communication between the IDS alarm panel and monitoring stations.

Video Surveillance System

The main purpose of the video surveillance system is to assess the alarm and have sufficient camera resolution and lighting that provides a clear enough picture to the monitoring station that shows that there is unauthorized activity occurring with the source device or sources. Video surveillance systems are increasingly network-based and therefore vulnerable to cyberattack.

The Remote Monitoring System and cameras

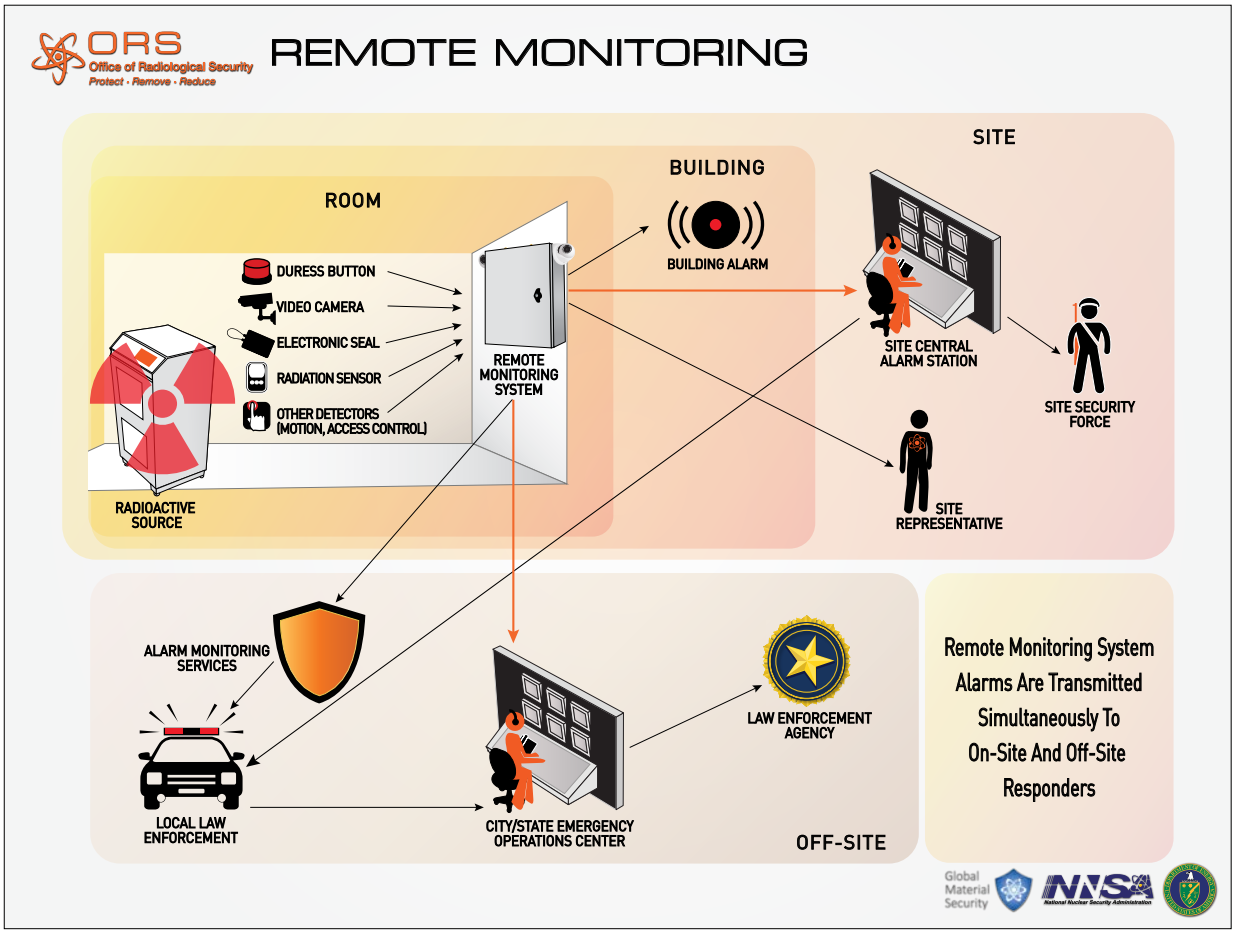
Remote Monitoring System (RMS)

An RMS is a separate Intrusion Detection System that incorporates an active tamper indicating device (TID) on the asset and a radiation detector used for security purposes. The system

Seal receiver installed inside the RMS

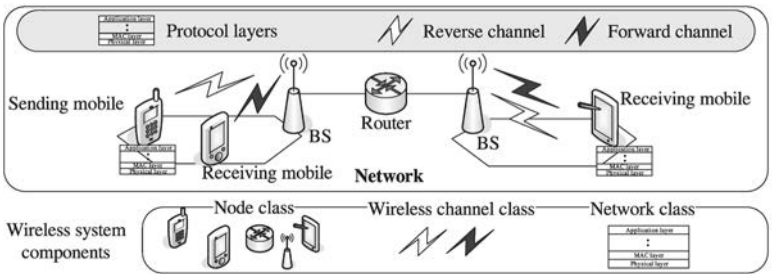
ORS provides the Sentry Remote Monitoring System for U.S. domestic sites. Remote Monitoring System equivalents that include the same functionality are installed at international sites.

should have redundant video surveillance focused on the device. This provides protection against the insider threat as these alarms and video are always on except for authorized maintenance and testing; i.e., the device user cannot disable these alarms. The RMS should provide the capability for remote (offsite) alarm and video monitoring of critical alarms and video in order to rapidly provide information to armed responders that will assist them in responding to a theft event. In most cases, the method of communication will be over the Internet. To ensure ORS-developed security equipment does not introduce new cyber vulnerabilities to sites, ORS conducted thorough cybersecurity testing on the Sentry RMS.



Data Communications to Offsite Monitoring Station

The selection of the technical means of transmitting RMS data from a building/site to an alarm monitoring station is dependent on a number of factors including state of the communications infrastructure, reliability of phone systems, capability and availability of cellular data networks such as GSM, GPRS, 3G, 4G, RF capability, etc. The use of phone lines with auto-dialers is not recommended as this method does not provide frequent enough polling to ensure the continuous monitoring of alarm data transmission or that loss of communications is detected in a timely manner. In some instances, two means of alarm transmission such as internet and cellular may be required to ensure reliable alarm transmission with polling capability and detection of loss of communications in a timely manner.



Kyungtae Kang, Min-Young Nam, Lui Sha, "Model-Based Analysis of Wireless System Architectures for Real-Time Applications", IEEE Transactions on Mobile Computing, vol. 12, no. , pp. 219-232, Feb. 2013, doi:10.1109/TMC.2011.260

Onsite Alarm Monitoring Station

A site may choose to provide or significantly enhance an onsite alarm monitoring station based on the role the station plays in the initiation of a response and its role in implementation of the site protection strategy. In most cases, a site can build upon existing onsite monitoring capabilities already established at a site. Since a site should also have offsite alarm monitoring, small sites with a limited onsite guard force (e.g., unarmed) might not warrant expenditure of resources on the construction of a new monitoring station. Sites with highly attractive radioactive material, a capable onsite armed response force, short adversary timelines, or when the onsite alarm monitoring station is critical to implementing the site protection strategy should consider establishment of a hardened/protected onsite monitoring station. The method of alarm communication will often be over site networks.

2.3. IMPLEMENTATION RECOMMENDATIONS FOR CYBERSECURITY CONTROLS TO SUPPORT PHYSICAL SECURITY SYSTEMS

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. Increasingly, system components should be reviewed by cybersecurity professionals for vulnerabilities including hardwired and proprietary code, IP-based communications, and non-prioprietary protocols. Users of radioactive sources should review their security systems to see what parts of the systems have IP-based communications and services (e.g., security cameras in public spaces with USB ports or other interfaces), as these are potential cyber adversary pathways. 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.

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 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 (e.g., motion sensors, BMS) 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.

The following diagram depicts a typical configuration of physical protection equipment and related technologies and equipment to communicate alarm signals to an alarm monitoring station. For the site in Figure 1, the network diagram represents a middle-sized facility such as a small university or hospital and demonstrates the potential cyber complexities of a relatively simple single target room site. The diagram shows a typical security configuration with the ORS-provided RMS connected to the burglar alarm panel for redundancy and with the RMS signals going to an onsite alarm monitoring station and an offsite alarm monitoring station.

Figure 1 shows a representative network layout recognizing that there are endless varieties of how networks could be laid out, e.g., firewall before router, router before firewall, router/firewall combinations, network components can be geographically far apart, services could be cloud-based such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), etc., and management of site networks could be outsourced to third parties.

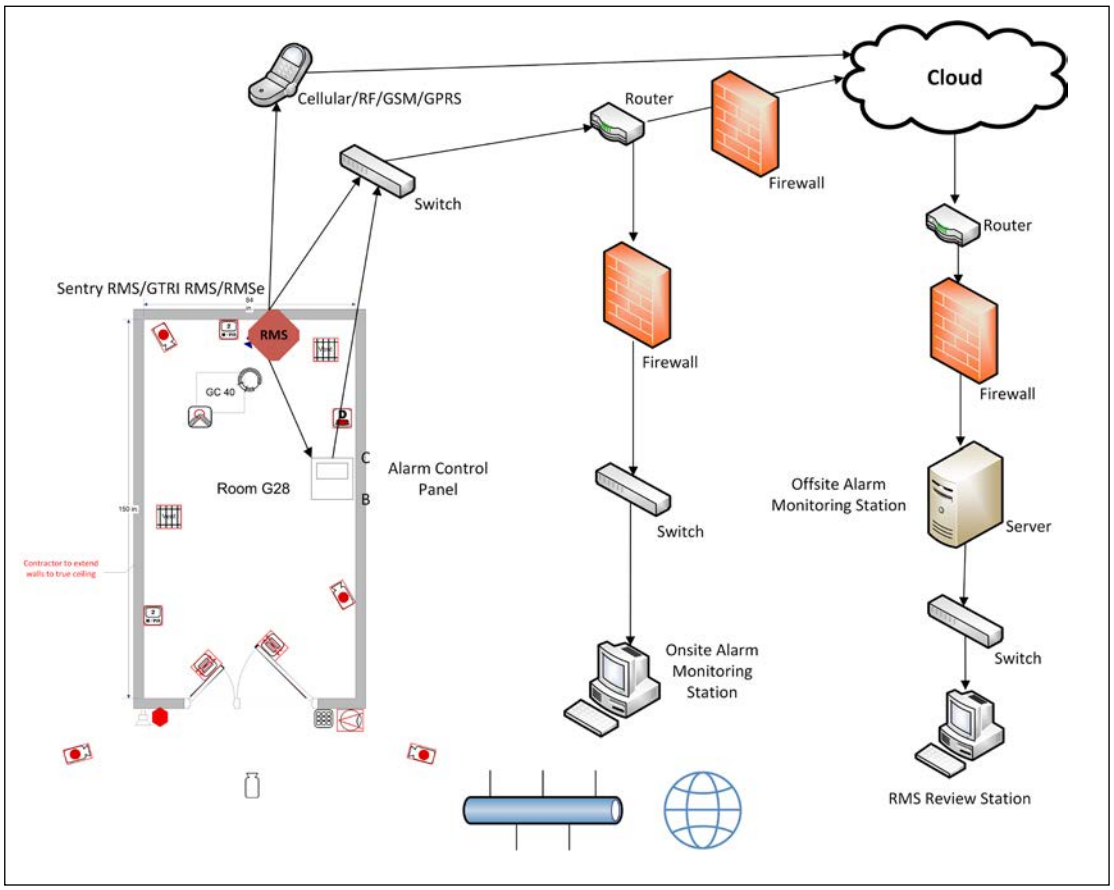


Figure 1. Example of Security System Communications

2.4. STARTING A CYBERSECURITY PROGRAM

A cybersecurity program is a necessity to ensure vulnerabilities are not introduced into a physical security program protecting radioactive sources. The integration of IP-based security system components will continue to increase making cybersecurity even more essential. Site IT staff can help you with the basics of a cybersecurity program, but professional cybersecurity support may be needed to develop a comprehensive program.

DEVELOPING A CYBERSECURITY PROGRAM STARTING POINT	
✓	
	Evaluate overall cybersecurity hygiene, posture, culture, and awareness level. https://www.dhs.gov/stopthinkconnect-toolkit
	Map out all interconnectivities/dependencies including interconnections to other systems
	Determine if protection system components are configured into logical security zones with minimum required traffic flows between zones, and are they enforced
	Determine if network-level access controls are implemented on the internal network infrastructure that interconnects protection system components
	Use a system discovery tool to conduct an inventory of what devices are connected to the protection system, and determine if only those authorized devices consistent with the security plan are connected. https://www.techtalk.gfi.com/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/
	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.
	Conduct a best practices evaluation for secure router and switches configuration, management, and operation. https://www.insights.sei.cmu.edu/sei_blog/2017/05/best-practices-for-network-border-protection.html
	Identify potential attack paths that can lead to potential compromise of the protection system, especially from connections permitted through the perimeter or from permitted remote access and management connections
	Review overall attack surface, attack paths, and attack vectors
	When performing the review keep in mind such items as:
	• Network terminals vs. workstations
	• Restricted connectivity using distributed firewall security zones vs. unrestricted internal network connectivity
	• Hardened centralized server configuration vs. distributed server and software implementation
	Use a vulnerability assessment tool to determine if server systems contain potential vulnerabilities and require patching or other security measures to mitigate potential risk
	Conduct penetration testing to validate perimeter security design and implementations

2.5. CYBERSECURITY BEST PRACTICES

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 because they are beyond the skill set expected of a layperson. These activities are included because they are recommended components of a comprehensive cybersecurity program.

CYBERSECURITY BEST PRACTICES	
✓	
	Site designates a person/staff member responsible for cybersecurity
	Enforce strict user accounts with limited role based permissions. Use the "least privilege" model for access to systems.
	Strong, complex password management and no longer than 6 months aging policies
	• Minimum of 8 characters, including special characters
	• May also use phrase password
	In addition to strong, complex password management, employ additional login authentication (e.g., RSA tokens)
	Remove unnecessary accounts, software, and processes
	Install Anti-Malware software and ensure it is kept current. http://www.searchsecurity.techtarget.com/definition/antimalware
	Ensure cybersecurity is included in Site Security Plan with ongoing review and updated following upgrades
	Ensure site has an acceptable use policy for employees using company cyber resources. Example policy: https://www.usaid.gov/sites/default/files/documents/1868/545mam.pdf
	Establish baseline to identify all equipment, cabling, and circuits and update documentation to match the physical implementation of the system and implement configuration management process for reviewing, approving, and documenting equipment and software changes, patches, etc.
	Ensure patches and firmware are derived from authorized vendors
	Network switches, alarm panels, access control devices, computer bios, digital cameras, and other components need to be patched to the current firmware version
	Purchase and use "enterprise" class hardware instead of consumer class components meant for home or small office use
	All software and firmware upgrades should be limited to authorized system administrators/managers
	Web browsers and dedicated e-mail accounts are often required by alarm management software, but recommend browser be configured to limit access to non-system related sites
	Physical hardening IDS/ACS of host computer locations, workstations, wiring closets, and on-site central monitoring stations
	Port scanning of all physical protection system (PPS) components that connect to the network and communication infrastructure
	Patch vulnerabilities on all ports and associated services

CYBERSECURITY BEST PRACTICES	
	Disable all unnecessary ports and associated services through hardware and software hardening
	Use Mobile Device Management (MDM) for the administration of mobile devices accessing company networks
	Ensure site 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
	Ensure site has an active security awareness program to potentially include phishing campaigns to test employee security awareness
	Enable built-in firewall attack detection, logging, and alerting features that should already exist in most modern firewalls
	Enforce network traffic flows in existing firewalls
	Utilize existing firewall DMZ as applicable (e.g., drop boxes, DNS, Web server). https://www.en.wikipedia.org/wiki/DMZ_(computing)
	Enable port security on network switches, disable unused interface ports, and restrict administrative access
	Create ACLs (access control lists) and restrict administrative access
	Air gap the system if possible or at least minimize the number of perimeter interconnections to provide network isolation where feasible
	Configure multi-zone network security architecture to isolate security protection components into logical groups. Add new transparent-mode firewalls where needed while enforcing the minimum required traffic flows between the zones
	Utilize thin-client network terminals instead of Windows workstations where possible to reduce attack surface, patching requirements, and total cost of ownership
	Incorporate traffic encryption for communication over any external networks or telecommunications circuits
	Employ redundant non-routable, static-IP dedicated networks in the core design
	Add intrusion detection capability to analyze network traffic and identify and alert attempted cyberattacks or suspicious packets and payloads
	Use multifactor authentication:
	• Type 1) Something a user possesses such as a badge;
	• Type 2) Something a user knows such as a PIN or password;
	• Type 3) Biological characteristics of a user such as their fingerprint or iris pattern.
	Recommend that prior to deployment new equipment/components be thoroughly tested for cyber vulnerabilities

2.6. SUSTAINABILITY

The following are best practices recommendations to sustain cyber protection.

SUSTAINABILITY CHECKLIST	
✓	
	Implement a configuration management plan
	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
	Security Plans (update periodically, and after upgrades)
	Approved equipment lists including hardware, operating systems, application software, firmware, etc., and associated revision levels
	Update mapping of interdependencies (hardware, software, hosts, and subsystems)
	End-to-end testing performed prior to incorporating new code or technologies
	Procedures for upgrades to include comprehensive checklists
	License management (e.g., some legacy software won't run on new platforms or may introduce cyber vulnerabilities)
	Automate virus scans and patches
	Documentation control (make sure its kept current and secure)
	System management of the network infrastructure and the interconnected components
	Examine current methods and capabilities of performing secure access, administration, and system management
	Perform penetration testing conducted to ensure the effectiveness of the hardening and architecture measures implemented during the remediation period. Tests can be tailored to the specific PPS protection system requirements
	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
	Implement a recovery plan that includes contingency planning and backups

CYBER RESOURCES

ICS-CERT - The Industrial Control Systems Cyber Emergency Response Team
https://ics-cert.us-cert.gov/alerts

National Cybersecurity Institute (NCI)
http://www.nationalcybersecurityinstitute.org/

Center for Internet Security (CIS)
https://www.cisecurity.org/

NIST Cybersecurity Framework
http://www.nist.gov/cyberframework/

Department of Homeland Security
https://www.dhs.gov/topic/cybersecurity

UK Center for the Protection of National Infrastructure
http://www.cpni.gov.uk/advice/cyber/

CIS Critical Security Controls
https://www.sans.org/critical-security-controls

CWE/SANS Top 25 Most Dangerous Software Errors
http://cwe.mitre.org/top25/

World Institute for Nuclear Security, Security of IT and IC Systems at Nuclear Facilities
https://www.wins.org/

IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities
http://www-pub.iaea.org/books/IAEABooks/8691/Computer-Security-at-Nuclear-Facilities

IAEA Computer Security for Nuclear Security (NST045) Draft Implementing Guide, http://www-ns.iaea.org/downloads/security/security-series-drafts/implem-guides/nst045.pdf

NRC Backgrounder on Cyber Security
https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html#require

IEEE Technology Policy Community White Papers, Internet Of Things (IOT) Security Best Practices, http:// http://internetinitiative.ieee.org

Note: ORS is planning a “Cybersecurity Best Practices for Transportation” as a future release.

For more information, contact ORS at ORSinfo@nnsa.doe.gov

ORS

Office of Radiological Security

Protect · Remove · Reduce