Funded by the European Union

CBRN Centres of Excellence
An initiative of the European Union

Information Security Best Practices for CBRN Facilities

With the support of

unicri
United Nations Interregional Crime and Justice Research Institute

Action Implemented by

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Funded by the European Union

CBRN Centres of Excellence
An initiative of the European Union

UNICRI Project 19

Information Security Best Practices for CBRN Facilities

Prepared by the Pacific Northwest National Laboratory within the framework of the Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative (EU CBRN CoE) entitled:

"Development of procedures and guidelines to crate and improve security information management systems and data exchange mechanisms for CBRN materials under regulatory control."

December 2015

With the support of

unicri
United Nations Interregional Crime and Justice Research Institute

Action Implemented by

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Pacific Northwest National Laboratory
Richland, WA 99352 USA

© UNICRI, 2015

All rights reserved. This document or parts thereof may be reproduced provided the source is referenced.

The document has been produced with the assistance of the EU. The information and views set out in this document are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

The contents of this document do not necessarily reflect the views or policies of the United Nations, UNICRI or contributory organizations, or do they imply any endorsement. While reasonable efforts have been made to ensure that the contents of this document are factually correct and properly referenced, UNICRI does not accept responsibility for the accuracy or completeness of the contents, and shall not be liable for any loss or damage that may be occasioned directly or indirectly through the use of, or reliance on, the contents of this publication. The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI concerning the legal status of any country, territory or boundaries. This publication has not been formally edited by UNICRI.

Summary

Information assets, including data and information systems, need to be protected from security threats. To protect their information assets, chemical, biological, radiological, and nuclear (CBRN) facilities need to design, implement, and maintain an information security program.

The general principles of information security are the same for CBRN facilities as they are for any other critical infrastructure or industry. The type of threats, attack tools and technologies, vulnerabilities, and types and capabilities of security controls are roughly similar for all types of facilities. What differs for CBRN facilities are the source of threats (i.e., who might want to attack a CBRN facility) and the consequence of the loss of information security. The sensitive nature of CBRN materials, the safety and health threats involved in the potential theft or sabotage at CBRN facilities, and the high public visibility of CBRN facilities often generate higher risks for the loss of information security than at other facilities.

This document provides management and workers at CBRN facilities, parent organization managers responsible for those facilities, and regulatory agencies (governmental and nongovernmental) with guidance on the best practices for protecting information security. The security mitigation approaches presented in this document were chosen because they present generally accepted guidance in an easy-to-understand manner, making it easier for facility personnel to grasp key concepts and envision how security controls could be implemented by the facility.

This guidance is presented from a risk management perspective. Not all facilities can afford to purchase, install, operate, and maintain expensive security systems; therefore decisions on information security have to balance considerations of security risk and resource constraints. When resources are limited, information security investments should focus on what provides the greatest risk reduction for the available resources.

This document is the first in a series of three documents produced by Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative. The second document in the series, *Information Security Management System Planning for CBRN Facilities*[1] focuses on information security planning. It describes a risk-based approach for planning information security programs based on the sensitivity of the data developed, processed, communicated, and stored on facility information systems. The third document in the series, *How to Implement Security Controls for an Information Security Program at CBRN Facilities*[2], provides risk-based guidance on selecting security controls to implement the ISMS.

[1] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015a. *Information Security Management System Planning for CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute, Turin, Italy.

[2] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015b. *How to Implement Security Controls for an Information Security Program at CBRN Facilities.* United Nations Interregional Criminal Justice Research Institute, Turin, Italy.

Acknowledgments

This document was prepared by a team of cyber and information security researchers from the Pacific Northwest National Laboratory in the United States, the National Nuclear Laboratory in the United Kingdom, and the University of Glasgow in the United Kingdom. The U.S.-based members of the team are:

Joseph Lenaeus
Pacific Northwest National Laboratory

Lori Ross O'Neil
Pacific Northwest National Laboratory

Rosalyn Leitch
Pacific Northwest National Laboratory

Cliff Glantz
Pacific Northwest National Laboratory

Guy Landine
Pacific Northwest National Laboratory

Janet Bryant
Pacific Northwest National Laboratory

The European-based members of the team are:

John Lewis
National Nuclear Laboratory

Gemma Mathers
National Nuclear Laboratory

Robert Rogers
National Nuclear Laboratory

Christopher Johnson
University of Glasgow

The document's technical editor was Cornelia Brim (Pacific Northwest National Laboratory). Administrative and management support was provided by Emily Davis, Josh Byrd, Monica Chavez, Keith Freier (all of Pacific Northwest National Laboratory), and other members of the authors' organizations.

This document was produced within the scope of Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative. The initiative is implemented in cooperation with the United Nations Interregional Crime and Justice Research Institute and the European Commission Joint Research Center. The initiative is developed with the technical support of relevant international and regional organizations, the European Union Member States, and other stakeholders, through coherent and effective cooperation at the national, regional, and international level.

Special thanks to Odhran McCarthy and the staff at the United Nations Interregional Crime and Justice Research Institute for their support, patience, and technical guidance during this project.

Acronyms and Abbreviations

ANSI	American National Standards Institute
ASD	Australian Signals Directorate
AV	anti-virus
BSI	Federal Office for Information Security *(German translation abbreviated BSI)*
CBRN	chemical, biological, radiological, and/or nuclear
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CIRT	Critical Incident Response Teams
COTS	commercial off-the-shelf
DNS	domain name system
ENISA	European Union Agency for Network and Information Security
EU	European Union
HART	Highway Addressable Remote Transducer
HIDS/HIPS	host intrusion detection and prevention systems
I&W	indication and warning
ICS	industrial control system
IDS	intrusion detection system
IEC	International Electrotechnical Commission
IACS	Industrial Automation and Control Systems
ISMS	Information Security Management System
ISA	International Society of Automation
ISO	International Organization for Standardization.
IT	information technology
ITL	Information Technology Laboratory
LAN	local area network
NIDS/NIPS	network intrusion detection and prevention systems
NIST	U.S. National Institute of Standards
NERC	North American Electric Reliability Corporation
OT	operations technology
PID	proportional integral derivative (controller)
PNNL	Pacific Northwest National Laboratory
SANS	System Administrators Networking and Security Institute
SIEM	Security Information and Event Management
SOP	standard operational procedure
SP	special publication

TTP	tools, tactics, and procedures
US-CERT	United States Computer Emergency Readiness Team

Contents

Summary iii
Acknowledgments v
Acronyms and Abbreviations vii
1.0 Introduction 1.1
1.1 Context of this Document 1.1
1.2 Background Information 1.2
1.3 Consequences to CBRN Information Security 1.5
1.4 Threats to CBRN Information Security 1.5
1.5 The Threat Agent 1.7
1.6 How to Use this Best Practices Document 1.10
2.0 PERFORMANCE AREAS FOR INFORMATION SECURITY MANAGEMENT SYSTEMS 2.1
2.1 Context of Organization 2.1
2.2 Leadership 2.3
2.3 Planning (Plan) 2.4
2.4 Support (Plan) 2.8
2.5 Operation (Do) 2.9
2.6 Performance Evaluation (Check) 2.10
2.7 Improvement (Act) 2.10
3.0 BEST PRACTICE RECOMMENDATIONS FOR INFORMATION SECURITY PROGRAMS 3.1
3.1 Recommendation: Implement a Graded Approach to Protect Critical Systems 3.1
3.2 Recommendation: Integrate Physical and Cybersecurity 3.1
3.3 Recommendation: Secure the Data Center 3.2
3.4 Recommendation: Secure the Human 3.3
3.5 Recommendation: Secure Data Exchange 3.3
3.6 Recommendations: Adopt Information Security Policies, Standards, and Procedures 3.4
3.7 Recommendation: Identify Credible Threats and Vectors of Attack 3.5
3.8 Recommendation: Identify, Eliminate, and Mitigate Vulnerabilities 3.8
3.9 Recommendation: Implement Defense-in-Depth Principles 3.10
3.10 Recommendation: Implement Life Cycle Security 3.13
3.11 Recommendation: Implement an Information Security Incident Forensic Response and Recovery Capability 3.14
3.11.1 Preparation 3.15
3.11.2 Identification 3.16
3.11.3 Containment 3.16
3.11.4 Eradication 3.17

3.11.5 Recovery 3.17
3.11.6 Post-incident Analysis 3.17
3.11.7 Forensics Activities 3.18
3.12 Recommendation: Information Security Awareness Training 3.19
3.13 Recommendation: Analyze and Select Security Controls 3.21
3.13.1 System Environment Analyses 3.22
3.13.2 Analyses of Threat, Threat Agents, and Attack Vectors 3.22
3.13.3 Development of Strategic Information Security Objectives 3.23
3.13.4 Selection of Security Controls 3.23
3.14 Recommendation: Perform Security Monitoring 3.24
3.14.1 Event Logging Systems 3.24
3.14.2 Security Logging and Event Manager 3.25
3.14.3 Other Issues 3.26
3.14.4 Human Interface 3.26
4.0 HIGH-VALUE SECURITY CONTROLS 4.1
4.1 The Top Four Strategies 4.1
4.1.1 Application Whitelisting 4.2
4.1.2 Application Patching 4.3
4.1.3 Operating System Patching 4.3
4.1.4 Minimize Administrative Privileges 4.4
4.2 The Critical Security Controls 4.5
4.2.1 Inventory of Authorized and Unauthorized Devices 4.7
4.2.2 Inventory of Authorized and Unauthorized Software 4.8
4.2.3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers 4.9
4.2.4 Continuous Vulnerability Assessment and Remediation 4.10
4.2.5 Malware Defenses 4.11
4.2.6 Application Software Security 4.12
4.2.7 Wireless Device Control 4.13
4.2.8 Data Recovery Capability 4.14
4.2.9 Security Skills Assessment and Appropriate Training to Fill Gaps 4.15
4.2.10 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches 4.16
4.2.11 Limitation and Control of Network Ports, Protocols, and Services 4.16
4.2.12 Controlled Use of Administrative Privileges 4.18
4.2.13 Boundary Defense 4.18
4.2.14 Maintenance, Monitoring, and Analysis of Audit Logs 4.20
4.2.15 Controlled Access Based on the Need to Know 4.21
4.2.16 Account Monitoring and Control 4.22

4.2.17 Data Loss Prevention 4.22
4.2.18 Incident Response and Management 4.23
4.2.19 Secure Network Engineering 4.25
4.2.20 Penetration Tests and Team Exercises 4.26
5.0 COMMON DEFICIENCIES/PROBLEMS OBSERVED IN EXISTING INFORMATION SECURITY PROGRAMS 5.1
6.0 SOURCES OF INFORMATION 6.1
6.1 International Organization for Standardization 27000 Series 6.1
6.2 National Institute of Standards and Technology Special Publication 800 Series 6.2
6.3 International Society for Automation/International Electrotechnical Commission Standards 6.3
6.4 German Federal Office for Information Security Standards 6.4
6.5 National Information and Computer Security Strategies 6.5
6.5.1 Information and Computer Security Strategies in Australia 6.5
6.5.2 Information and Computer Security Strategies in the Czech Republic 6.5
6.5.3 Information and Computer Security Strategies in Estonia 6.6
6.5.4 Information and Computer Security Strategies in France 6.6
6.5.5 Information and Computer Security Strategies in India 6.6
6.5.6 Information and Computer Security Strategies in Japan 6.7
6.5.7 Information and Computer Security Strategies in the Russian Federation 6.7
6.5.8 Information and Computer Security Strategies in the United States 6.7
6.6 European Union Agency for Network and Information Security 6.7
7.0 REFERENCES 7.1
8.0 GLOSSARY 8.1

Figures

2.1. The Seven Performance Areas of an ISMS, and their Implementation Stages 2.2
2.2. A Simplified Flowchart for Risk Assessment 2.7
2.3. Relationships of Various Components within the Risk Management Program 2.8
3.1. Simplified Attack Tree..... 3.7
3.2. Computer Vulnerabilities Reported to the U.S. NIST National Vulnerability Database..... 3.9
3.3. Defense in Depth 3.10
3.4. Multiple Layers of Security..... 3.11
3.5. Defense Data Flow Model 3.12
3.6. Analyze and Select Security Controls..... 3.22

Tables

1.1. Simple Qualitative Risk Chart Showing Risk as a Function of Likelihood and Consequences1.4
2.1. Example Set of Key Information Security Roles and Responsibilities..... 2.5
2.2. Planning the Risk Management Process 2.6

1.0 Introduction

Information security is the practice of protecting information from unauthorized access, unauthorized modification, or denial of access. Unauthorized access could lead to the disclosure, modification, deletion, or misuse of information. Severe adverse outcomes can result from the loss of information security—this is especially true for facilities that are tasked with creating, using, storing, or disposing of chemical, biological, radiological, or nuclear (CBRN) materials. Outcomes may involve safety or health impacts to workers and members of the public, disruption of facility operations, loss of revenue, compromise of facility security information, loss of sensitive inventory information, loss of intellectual property, damage to a facility's reputation, increased regulatory oversight, and loss of worker or customer personnel information, to name a few impacts.

The protection of information involves the application of security controls holistically made up of technical, physical, procedural, and required compliance. No single set of tools or technologies can safeguard information from all threats. The protection of information involves cybersecurity (i.e., computer security) as well as physical security and personnel security. It also involves protecting infrastructure resources upon which information security relies (e.g., electrical power, telecommunications, and environmental controls).

This document provides management and workers at CBRN facilities, organizational managers responsible for those facilities, and regulatory agencies (governmental and nongovernmental) with guidance on the best practices for protecting information security related to CBRN materials and facilities. This guidance is presented from a risk management perspective. Not all facilities can afford to purchase, install, operate, and maintain expensive security systems; therefore decisions on information security have to balance considerations of security risk and resource constraints. When resources are limited, information security investments should focus on what provides the greatest risk reduction for the available resources. However, we recognize the difficulties in accurately identifying potential threats and existing vulnerabilities. This document:

- provides a high-level description of the best practices that support information security and the development of an effective information security program
- identifies the critical security controls that are recommended for information systems
- covers areas of special interest to CBRN facilities, such as how to safely exchange data and how to identify specific threats that are of particular concern to CBRN facilities
- also covers key deficiencies and problems that the authors have observed during their cyber and information security inspections of CBRN facilities.

The guidance provided in this document has been developed on behalf of the European Union (EU) as part of their EU Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative.

1.1 Context of this Document

This document is the first in a series of three information security guidance documents produced within the framework of Project 19 of the European Union CBRN Risk Mitigation Centres of Excellence

Initiative. The initiative is implemented in cooperation with the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the European Commission Joint Research Center. The initiative is developed with the technical support of relevant international and regional organizations, the European Union Member States and other stakeholders, through coherent and effective cooperation at the national, regional, and international level.

The objective of Project 19 is to provide guidance on the security of information technology (IT) structures and data exchange mechanisms for CBRN facilities. This includes providing information on the management, operational, and technical security controls needed to address threats, characterize adversaries, identify vulnerabilities, and enhance defense and mitigation capabilities. The key objective of the project is to help CBRN security managers, IT/cybersecurity managers, and other decision makers typically involved in acquiring, auditing, regulating, and disposing of information to develop and implement appropriate and cost-effective information security programs. The guidance provided by Project 19 is based on international standards and best practices, the experience of the information security experts on the document writing team, and the many CBRN facility personnel and government officials from around the world who participated in the stakeholder review of this document.

The second document in the series, *Information Security Management System Planning for CBRN Facilities* (UNICRI 2015a), is referred to as the "ISMS Planning" document. It provides guidance for developing information security planning documents that establish information security roles, responsibilities, and policies. The third document in the series, *How to Implement ISMS Security Controls Using a Risk Based Approach at CBRN Facilities* (UNICRI 2015a), is referred to as the "How-to" document. It provides a guide for selecting security controls that can be used to implement information security plans and policies.

In addition to the three documents, a two-day teach-the-teacher workshop on information security for CBRN facilities has been prepared. That workshop is designed to introduce the need for information security to CBRN facility decision makers and others with oversight responsibilities for CBRN materials and facilities.

1.2 Background Information

All information held and processed by an organization is subject to threats of human attacks, including unauthorized access, theft, alteration, and denial of access. These attacks can range from deliberate and malicious actions to inadvertent and benign actions resulting from human error. The security of information may also be subject to threats from natural hazards such as floods, fires, earthquakes, and volcanoes. The goal of information systems is to provide accurate and complete information to appropriately authorized people and systems in a timely and secure manner. To do this, organizations need to develop and maintain an information security management system (ISMS). An ISMS is a set of policies, practices, and technologies that protect the security of information to maintain and achieve an acceptable level of information security risk. The ISMS needs to adopt a life cycle view on information security, providing governance over the design, acquisition, installation, operation, maintenance, evolution, and disposal of its components.

Information security risks and the effectiveness of security controls change depending on shifting circumstances. In response to this, organizations need to:

- identify emerging threats and vulnerabilities
- evaluate evolving consequences as threat, vulnerabilities, defenses, operating conditions, and other factors change
- audit, monitor, and evaluate the effectiveness of implemented management, operational, and technical security controls
- evaluate potential changes to existing security controls and the addition of new security controls. This includes an evaluation of the risk reduction benefits and the costs of making changes.
- select and implement appropriate modifications to security controls based on requirements and risk management considerations
- regularly educate staff members and raise their awareness of cybersecurity risks, prevention, and mitigations.

The three general categories of security controls are management, operational, and technical security controls.

Management controls concentrate on the management of information security. Controls within this category include activities involving certification, accreditation, security assessments, planning, risk assessment, and system or services acquisition.

Operational controls are safeguards or protective measures that are to be performed by humans rather than by automated means. Controls within this category include activities involving training, configuration management, contingency planning, incident response, maintenance, media protection, physical and environmental protection, system and information integrity, and personnel security.

Technical controls are considered to be safeguards or protective measures that are executed through mechanisms contained within the hardware, firmware, operating system, or application software. Controls within this category would include access controls, audit and accountability, identification and authentication, and system and communications protection. This classification of controls would include devices typically related to security such as routers, firewalls, intrusion detection and prevention systems, smart tokens, and logging systems, to name a few. With technical controls, actions are automatically taken in response to a triggering event.

Risk, specifically **information security risk,** is the product of the likelihood that something adverse will happen to information and the resulting consequences of that adverse event on those who need to use that information. **Likelihood** is a function of the characteristics and intentions of the threat agent and the vulnerability of the information and/or information systems.

```
Risk = Likelihood of an adverse event X Adverse Consequences
```

For example, likelihood may be measured terms of “estimated occurrences per year” and consequences may be measured in terms of “estimated monetary consequences as a result of an adverse event”. This produces a quantitative risk estimate in terms of “money per year”.

Risk may be measured in terms of anticipated money lost per year. Alternatively, risk can be measured in qualitative terms, as indicated in Table 1.1. The combination of "High" likelihood and "High" consequences produces a "Very High" risk. On the opposite end of the spectrum, a combination of "Low" likelihood and "Low" consequences produces a "Very Low" risk. This basic approach to risk gets its start from the Open Web Application Security Project (OWASP) Risk Rating Methodology**Error! Hyperlink reference not valid.** (OWASP 2014).

Table 1.1. Simple Qualitative Risk Chart Showing Risk as a Function of Likelihood and Consequences

	Consequences		
Likelihood	**Low**	**Moderate**	**High**
High	**Moderate**	**High**	**Very High**
Medium	**Low**	**Moderate**	**High**
Low	**Very Low**	**Low**	**Moderate**

Information security risk can be reduced by making it less likely that information will be compromised, or by reducing the consequences of that loss. The likelihood of an adverse event can be reduced by eliminating or reducing security vulnerabilities in the human or technological components of information systems. Consequences can be reduced by enhancing the resiliency of information systems. Resiliency involves the ability to resist adverse impacts, absorb impacts while still maintaining functionality, or quickly recover from an attack. Resiliency, like vulnerabilities, includes both human and technological components.

No situation produces zero risk, as shown in Table 1.1. In practical terms, it is not feasible to eliminate all risk, no matter how much is invested in information security. All ISMS must accept some level of acceptable risk that cannot be eliminated, given the real-world resource constraints that all programs must face.

The focus of this document is the establishment and maintenance of information security management systems at CBRN facilities; however, the general principles of information security are the same for CBRN facilities as they are for any other critical infrastructure or industry. The type of threats, attack tools and technologies, vulnerabilities, and types and capabilities of security controls are roughly similar for all facilities. What differs for CBRN facilities are the source of threats (i.e., who might want to attack a CBRN facility) and the consequence of the loss of information security. The sensitive nature of CBRN material, the safety and health threats involved in the potential theft or sabotage at CBRN facilities, and the high public visibility of CBRN facilities often generate higher risks for the loss of information security than at other facilities. Fortunately, the nature of most CBRN facilities also creates advantages for the implementation of an information security program; staff members are typically well-trained and motivated to follow security policies and procedures because of their concerns about both physical security and information security.

1.3 Consequences to CBRN Information Security

The loss of assets or reduction in value of the organization's information can occur through the loss of:

- **Confidentiality** (prevent unauthorized access). This refers to the ability or assurance to limit access to information to authorized individuals or secret systems, or otherwise prevent its unauthorized disclosure.
- **Integrity** (prevent unauthorized modification). This refers to the assurance that information has not been modified in an unauthorized manner that would affect its accuracy or reliability. This includes information used by personnel, information technology, or controls systems that operate facility processes.
- **Availability** (prevent unauthorized access restrictions). This refers to the ability or assurance that authorized individuals, information technology, or controls systems are able to access and interact with required information in an uninterrupted and timely manner.

Consequences resulting from the loss of confidentiality, integrity, or availability of information or information systems can occur in a number of areas and may involve environmental releases of hazardous or radiological materials, curtailment of facility operations, damage to facility equipment, health or safety impacts to workers or the public, loss of intellectual property, transfer of knowledge to those who might use that information for nefarious purposes, loss of confidence in a facility by its customers or funding organizations, negative impacts on reputation and public image, and regulatory impacts (e.g., new laws or increased oversight). As an example, some recent versions of malware deliberately insert themselves into anti-viral systems. Running a scan infects the system; this makes it very difficult to convince a regulator that an infected network is clean enough to resume operation.

1.4 Threats to CBRN Information Security

Threats to CBRN facilities can generally be grouped into three distinct categories:

- Nature-based. The nature-based category comprises naturally occurring events or hazards (i.e., floods, fire, tsunamis, landslides, earthquakes, hurricanes, tornadoes, major storms, and epidemics). Although these sources are not induced by human adversaries, they can nonetheless affect the overall information security of a CBRN facility. Natural events can destroy information or prevent its access, including hardcopy information and information stored on computer systems. Nature-based events can also damage or destroy physical and cybersecurity systems, allowing theft of information.
- Human-based. The human-based category consists of activities that require a human to manifest the threat. Examples include activities involving cyberattacks, theft of information, sabotage of information, espionage, terrorism, civil disorder, and acts of war.
- Infrastructure. This category includes items such as failure of necessary services for information systems (e.g., electric power, heating and cooling, and moisture control). This can occur as the result of events including equipment malfunction or failure, software and hardware failures, or communications failures. These can occur inadvertently or accidentally, or be the result of malicious acts. Attacks on infrastructure can be human- or nature-based and need to be considered when evaluating the availability of the system.

A comprehensive CBRN site security program will seek to identify the range of all credible threats that exist for a given organization and develop strategies that implement countermeasures where possible to eliminate or mitigate the threats. This includes both physical and cyber threats. A threat to an organization is a threat regardless of where it originates or the tactics that it employs.

Many organizations treat threats as though they are mutually exclusive of one another. This is somewhat understandable as cybersecurity is a relatively new issue that has only came to the forefront within the last 20 years. In comparison, the discipline and practice of physical security are time-tested concepts that have evolved over the centuries. Moreover, in most organizations, individuals responsible for addressing physical and cybersecurity issues are typically assigned to different workgroups and there may be limited or no coordination of their activities.

In reality, approaches to cybersecurity and physical security are similar. The principal difference lies in the unit of inspection. In the case of physical security, the units of inspection are human beings. In the case of cybersecurity, the units of inspection are often packets of digital information (datagrams). In both cases we are seeking to control access to some type of organizational resources by these units.

We can exercise control over the movement of individuals through the use of physical security measures such as gates, fences, doors, locks, access control systems, surveillance systems, intrusion detection systems, and checkpoints. Additionally, devices such as metal detectors or explosive detectors can be used to ensure that prohibited items are not introduced into the workplace by individuals. Staff members may also be subject to additional screening (such as drug/alcohol screens) to ensure that they are fit for duty. These security controls typically fall under the purview of a physical guard force.

We can exercise similar control over the movement of datagrams through a network using security controls such as routers, firewalls, proxies, and network access control systems. Additional inspections measure may also include the use of anti-virus systems as well as network and host-based intrusion detection systems capable of performing deep-packet inspection to ensure that malware is not introduced into the computing environment. The security controls applied within an information or control system network typically fall under the purview of cybersecurity specialists.

Additionally, because of the rapid technological advancements made in the field of physical surveillance that have occurred in the last 20 years, many organizations have upgraded their physical security systems with network-based devices that use commercial off-the-shelf (COTS) technology and operating systems and communication protocols that are identical to that of standard information technology systems. As such, many security organizations are now highly dependent upon this underlying technology in order to perform their designated functions.

It is also important to recognize that while the nature of a given cyberattack (including the methods and tools used in the conduct of an attack) may differ substantively from those used in a physical assault, the consequences can be similar. Cyberattacks conducted against certain critical digital assets of a CBRN facility can be just as debilitating as a physical attack, resulting in severe repercussions if not properly addressed. As an example, consider a safety system that might be employed to ensure that radioactive material was not inadvertently released to the environment. If strong countermeasures were implemented that ensured that no unauthorized individuals could physically access the equipment, but a communications capability existed that allowed remote access accomplished by virtual means, what is the true effect of the physical security? If the design base function of the system can be compromised

remotely, the effect is the same as if an unauthorized individual physically accessed the system and rendered it unusable.

Finally, from a threat perspective, attacks against an organization can be multifaceted, attacking a security database to permit unauthorized physical access to a site is an example. It is quite possible for an adversary to use the following forms of attack:

- physical attack
- cyberattack
- physically enabled cyberattack (blended)
- cyber-enabled physical attack (blended).

In this document, cyberattack includes a wide assortment of computer-based events that are capable of modifying, destroying, or compromising the integrity and confidentiality of data; results in the denial of access to systems, networks, services, or data; or otherwise negatively affects the proper operation or function systems, networks, and associated equipment. Cyberattacks may involve the use of computer viruses, worms, malware, false data, denial of service, or other types of exploits and may be directed or non-directed in nature. Cyberattacks also may include physical attacks involving the theft or destruction of hardware, or seek to modify environmental conditions in order to affect the functionality of a computer-based system. Cyberattacks can arise from internal sources, external sources, or a combination of the two. Entities launching or facilitating a cyberattack may have malicious intent or may be inadvertent contributors to the attack.

Although various types of cyberattack exist, the attacks themselves:

- challenge the state of a system or network
- can affect command and control
- involve both physical and logical threats to computer systems or networks
- may be directed or non-directed
- are conducted by threat agents having either malicious or non-malicious intent.

If an organization chooses to evaluate physical and cyber threats on information security exclusive from each other, unanalyzed vulnerabilities will likely exist that may provide an adversary a successful vector of attack. Unlike physical attacks, cyberattacks can be developed at relatively little cost. They can also be launched with plausible deniability, in other words, it can be hard to identify the particular source of an attack when attackers can exploit compromised servers in third-party states.

1.5 The Threat Agent

A threat represents the intent, capability, and opportunity of an adversary to attack or inflict harm. An attack is a manifestation of a threat (e.g., assault) conducted by a threat agent against a target. Threat agents carry out threats against vulnerable targets using tools, tactics, and procedures (TTP) to accomplish their objectives in response to some motivation (i.e., political ideology, religious belief, money, or challenge). A threat agent's capability refers to the knowledge, skills, and tools necessary to conduct an

attack, whereas opportunity represents the situational circumstances that would support the initiation of an attack. The relative magnitude of the threat directly corresponds to the proportional quantities of each of these elements. A threat agent with a clearly stated or well-known intent and possesses a high degree of capability and knowledge would represent a serious threat, whereas a threat agent that has an unfocused intent with little or no capabilities would represent a negligible threat.

The relative interest levels of threat agents in a given target can vary over time. In some cases this variance can be traced to a risk/effort/reward mindset (i.e., the payoff for conducting an attack is insignificant to the risk or effort involved). In other cases, the interest level of a given class of threat agent may only be limited by the capabilities of the agent to conduct an attack (i.e., the agent is limited by insufficient knowledge or tools). Conversely, it is also important to recognize that the emergence of new tools and methods that act to overcome such limitations can also act to elevate the interest in this same class of threat agent. However, a common class of sniffer programs has been developed to gather data on a wide class of critical infrastructures, including CBRN facilities. These programs gather information that is of strategic importance even if there is no immediate intention of using the data to launch an attack.

Threat agents seeking information from CBRN facilities using physical means are fairly well known. Less familiar are the attackers who may use cyberattacks or combine cyber and physical attacks. These threat agents include, but are not limited to:

- insiders or former insiders (e.g., disgruntled staff members, contractors, or vendors)
- hackers, crackers
- hacktivists
- criminal syndicates
- commercial rivals
- terrorists
- industrial or foreign espionage agents
- nation states.

Insiders including site staff members, contract employees, and vendors may have substantial access to CBRN equipment and computing resources. Because of their ability to legitimately access resources, they have the opportunity to intentionally (or in some cases unwittingly) damage digital assets or data. Many recent, well-publicized events exposed the ability of disgruntled workers to inflict damage to an organization's critical assets, including significant destruction to property or reputation. Insiders may carry out destructive physical attacks, cyberattacks, or both. The attacks leveraged by an insider could result in immediate consequence or could be designed so that adverse effects would materialize at some future time—even months or years following the initial compromise—allowing the insider to invoke plausible deniability from involvement in the incident. The ability to programmatically alter or defer the adverse impact from the time of its initiating event within a cyberattack offers a degree of separation that does not exist for most forms of physical sabotage. Unintentional acts of negligence or careless disregard for established security protocols by insiders may expose sensitive information that could enable a threat agent to advance an attack. Disgruntled insiders are typically motivated by retribution for perceived injustice suffered at the hands of their employers. However, in previous attacks it is not always possible to anticipate or identify the precise motivation for an insider attack.

A “hacker” is a person who, without authorization, uses programming skills or tools to gain access to a computer system or network. Having gained access to a system, a hacker has the potential to tamper with data or programs. Motivations for hackers are varied, but typically include elevation of social status (i.e., bragging rights), infamy, notoriety, and personal challenge.

Much confusion exists between the terms “hacker” and “cracker” within the news media and public at large. Traditionally, the term hacker has been used to describe a person who demonstrates intense interest in the deep and obscure workings of computer operating systems and applications. Most hackers possess advanced knowledge of operating systems and programming languages. They often openly report on previously undiscovered vulnerabilities and provide solutions to the problems they find. Hackers demonstrate a constant need to seek further knowledge and freely share their discoveries within the larger computing community; however, they never intentionally damage data. A cracker, on the other hand, is an individual who demonstrates malicious intent by breaking into or otherwise violating the system integrity of computers or networks without authorization. Crackers typically steal or destroy data, deny access to legitimate users, and cause problems for their targets.

Hacktivists are motivated by perceived acts of social injustice. This may cover a wide range of potential issues including, but not limited to, cultural, political, religious, gender, and environmental concerns. Hacktivists engage in cyberattacks as a form of technical protest, activism, or civil disobedience in order to force changes in social policy, business practices, or governmental behavior. *Anonymous* and *Decocidio* are examples of hacktivist organizations.

Criminal syndicates represent another potential threat agent. Cybercrime is increasing, as is the sophistication of these attacks. Cybercrime may involve attempts at extortion or blackmail of individual CBRN facility owners and operators. The primary motivation for criminal syndicates engaging in this activity is financial. Compared to other forms of criminal activity, cybercrime represents a relatively low risk to the criminal. Cybercrime is reaching epidemic proportions on a global scale. Several reports have been published on the cost of cybercrime in 2013. One of the most conservative is the 2013 edition of the Norton Cybercrime Report which calculates the direct costs associated with global consumer cybercrime at US $113 billion over the past 12 months (Norton 2014). The highest estimate comes from Intel Security (2014), *Net Losses: Estimating the Global Cost of Cybercrime* report, at US $575 billion.

Terrorism involves the unlawful or threatened use of force by an individual or organized group against people or property, with the intention of intimidating or coercing societies or governments, often for ideological or political reasons. International terrorist groups have issued threats to use cyberattacks to affect critical infrastructure targets, including disrupting systems associated with electric power generation and transmission. Terrorist activities may involve denial of service attacks, use of malicious computer viruses, or electronic commandeering of critical systems. The motivations associated with terrorist organizations are typically associated with ideological or religious beliefs. Well-funded organizations, such as Al-Qaeda, have the ability to procure cyber expertise if it is not natively available. Terrorist organizations recognize the asymmetric advantage that cyber warfare holds and have encouraged their members to engage in “cyber jihad” against its perceived enemies.

Espionage is the act or practice of spying or using spies to obtain secret or proprietary information to gain economic, technical, or strategic advantage over competitors. Espionage may be used to identify and obtain information on technological developments or to obtain information on facility personnel that may be used for nefarious purposes (e.g., to enhance efforts to socially engineer staff members).

Nation states are threat agents capable of engaging in cyber warfare where computer systems and digital communications are used to attack an opponent to deny access to, manipulate, or destroy the opponent's computer systems or the infrastructure components controlled by these digital systems. Many nations, both large and small, are investing resources to develop capabilities that would allow them to mount successful cyberattacks and to disrupt or damage an opponent's critical infrastructure. They are highly motivated to achieve superiority in computer network exploitation (CNE), computer network attack (CNA), and computer network defense (CND) in order to achieve political, economic, and militaristic advantage over other countries. For many nations, cyber warfare provides an offensive capability that they could not achieve using conventional military forces.

Intelligence experts consider the cyber threat to be credible and growing. Although capabilities may vary among the different categories of threat agents, each represents a very real cybersecurity threat. It is realistic to assume that capabilities exist for some threat agents to mount a well-planned and executed cyberattack against CBRN facilities. Threat agents mounting such an attack would likely possess:

- a working knowledge of critical systems typically used within CBRN facilities gained through employment by a domestic or foreign CBRN facility or with a vendor providing services to those facilities
- advanced hacking capabilities that would allow them to mount a skillful and stealthy cyberattack
- the time and resources to carefully research, plan, and implement an attack.

1.6 How to Use this Best Practices Document

This document consists of several sections. Section 2 provides a brief description of each of the performance areas of an information security program. Section 3 describes best practices for information security. Section 4 presents a set of high-value security controls that CBRN facilities should give the highest priority to implement in their risk-based information security programs. Section 5 describes common issues that arise in the development and implementation of an ISMS. Section 6 provides brief descriptions of information security resources. Section 7 presents the list of references and Section 8 is a glossary of terms.

Ideally, the reader would read the document sequentially to learn how to develop and maintain a high-quality information security program (Section 2). Most information security management programs should involve a risk management component in order to determine the controls that are most appropriate for the organization's security needs. However, in the real world that process is not always readily implementable. Some readers might want to focus on Section 2 (Best Practice Recommendations for Information Security Programs) and explore a set of best practices for information security. Other readers might want to focus on Section 3 (High-Value Security Controls) to concentrate on best practices. Those who wish to concentrate on the specific, high-value security controls should focus on Section 5 and its presentation of the most effective security recommendations developed by the Australian Signals Directorate and the System Administrators Networking and Security (SANS) Institute.

2.0 PERFORMANCE AREAS FOR INFORMATION SECURITY MANAGEMENT SYSTEMS

A variety of international standards and national policy documents provide guidance for developing an information security program. Some are based on laws and regulations; following a compliance approach to information security (e.g., do what the law says). Others take a risk management approach (e.g., evaluate your information security risks and manage them). The various information security guidance products overlap. The International Organization for Standardization (ISO) 270001 series (sometimes referred to as ISO27k) is one of the more popular guidance products because it is an international standard and it is applicable for a wide range of infrastructures and industries. However, it is not customized to focus on any given type of organization and can involve significant costs.

The ISO 27001 series presents a framework for an ISMS that involves seven performance areas:

1. Context of the Organization
2. Leadership
3. Planning
4. Support
5. Operation
6. Performance Evaluation
7. Improvement.

These performance areas can be divided into five stages—Governance, Plan, Do, Check, and Act. The relationship among the seven performance areas and their stages in the information security program are illustrated in Figure 2.1.

In an environment where information systems and associated processes are continually evolving, the information security threat and adversary capabilities are changing, and new information security technologies are emerging, a continuous process is needed to maintain the accuracy and performance of the ISMS. Period reassessments are required, as illustrated by the cyclic nature of the process outlined in Figure 2.1.

Each of the seven performance areas will be discussed in the following sections.

2.1 Context of Organization

The first performance area addressed in developing an ISMS involves understanding the organization and its context. The context includes both external and internal considerations (as described in ISO 31000 [ISO 2009]).

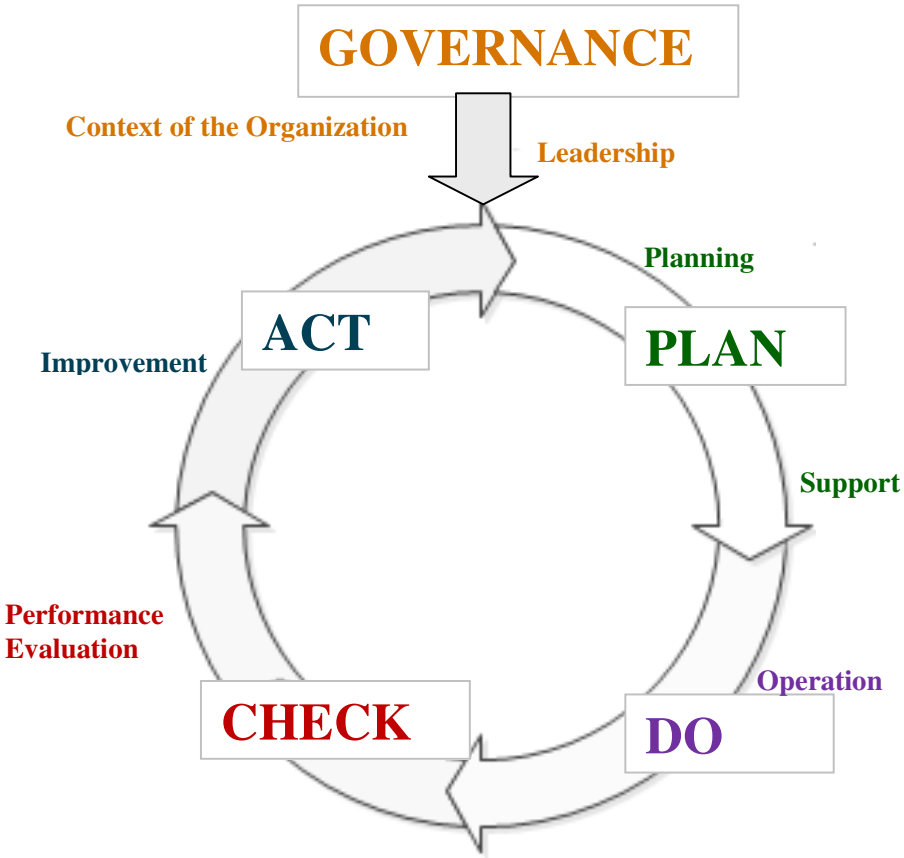

Figure 2.1. The Seven Performance Areas of an ISMS, and their Implementation Stages

Assessing the context of the organization involves identifying and characterizing:

- the legal, cultural, regulatory, financial, technological, and economic environments that affect the CBRN facility (ISO 31000). In particular this includes the identification of all applicable international, national, and local laws and regulations that pertain to information security at the facility. The identification of these laws and regulations is necessary to ensure the information security program minimizes its legal, regulatory, and financial risks associated with a failure to meet national and international requirements.
- the objectives of the organization and the "drivers" that implement these objectives. These drivers include organizational policies and structure, objectives, strategies, guidelines, procedures, current practices, and key roles and responsibilities associated with the information security program. These drivers encompass the cyber, physical, and personnel security elements of information security. A failure to comply with an organization's defined standards, policies, procedures, and responsibilities can result in substantial legal, regulatory, and financial risks—as well as personal risks (e.g., loss of employment, suspension, or demotion)—for decision makers and staff members.
- identifying external stakeholders and characterizing their interest in the CBRN facility. External stakeholders may include government agencies, international regulatory agencies, facility sponsors, industry associations, interest groups, business partners, suppliers, customers, and the general public. Of particular interest are the contractual relationships with sponsors, suppliers, developers, business

partners, and customers that may be affected by a breach in information security. A failure to consider external stakeholders can increase regulatory, financial, and public perception risks.

- existing information assets, including information technologies and systems that need information security.
- available organizational resources that can be applied to information security issues. These resources include organizational funding, available technologies, the information security expertise of decision makers and staff members, and the time decision makers and staff members have available to address information security issues.

In terms of information security, the context of the organization will vary greatly depending on what a facility does, where it is located, and what materials it contains. For example, a hospital, large chemical plant, academic institution (e.g., college or university), and a military facility provide very different organizational contexts for information security. These contexts determine applicable regulations and risk management considerations. However, regardless of the level of information security, every organization should perform a thorough assessment of its information security environment, drivers, stakeholders, assets, constraints, and resources. Appropriate risk management decisions cannot be made unless there is an adequate assessment of the organization, its needs, and the environment in which it operates.

2.2 Leadership

An effective information security program requires effective leadership. Leadership begins with the commitment of senior management to:

- establish information security objectives and policies
- establish and communicate the organization's priorities for ISM and ensure an ISMS is integrated into operations
- ensure appropriate resourcing for information security management activities
- monitor conformance with ISM policies and the effectiveness of ISMS implementation
- hold managers and staff members accountable for the implementation of the information security program
- promote the continuous improvement of information security.

Leadership also requires that senior management establish an information security program that includes clear objectives, providing a framework for information security objectives. The policy should also commit the organization to meet all applicable information security requirements and to work for the continuous improvement of its ISMS. The information security policy shall be made available within the organization and to an appropriate set of stakeholders (e.g., business partners and regulators).

The final major element of leadership is for senior management to ensure that roles and responsibilities for information security are assigned throughout the organization. This includes establishing a method for effectively communicating roles and responsibilities to all staff members and a

method for reporting on information security management implementation and performance to senior management. Some of these roles—audit, for instance—may require external support.

Clear and unambiguous roles, responsibilities, authorities, delegations, and interfaces are needed within an organization to implement and maintain an effective information security program. National Institute of Standards (NIST) Special Publication SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, (NIST 1996) is an example of a readily available guidance document for establishing appropriate roles and responsibilities to support information security. This document provides an understanding of a comprehensive set of programmatic elements that are applicable in any technology environment. Although originally authored for "securing IT systems," the guidance provided is aligned with the needs of information security.

Some key roles that should exist, the responsibilities of each role, and the organization to which each role is aligned, are identified in Table 2.1.

In addition to the roles identified in Table 2.1, responsibilities should be defined for organizations and individuals expected to interface with the acquisition, storage, use, and maintenance of information. This group might include operations personnel, engineers, technicians, users, contractors, and vendor representatives. The information security roles, responsibilities, authorities, and functional relationships should be defined, documented, and understood by all site organizations and individuals (including staff members, subcontractors, temporary employees, visiting researchers, and vendor representatives) at every level in the organization. It is also important to clarify the interface between the teams responsible for physical security and cybersecurity.

2.3 Planning (Plan)

When planning for the ISMS, the organization should determine the risks and opportunities that are needed to ensure the information security program objectives are met. A key focus is preventing information security incidents and reducing their consequences. Table 2.2 provides an overview of the risk management process.

Table 2.1. Example Set of Key Information Security Roles and Responsibilities

Role	Responsibility	Organization
Information Security Program Sponsor	• Is the senior manager responsible and accountable for the information security program • Provides resources to develop, implement, and sustain the information security program	Senior CBRN Facility Manager or organization (e.g., corporate) executive officer
Facility Security Manager	• Provides oversight for all activities being conducted by the site's security program • Has the ultimate authority over both the physical and cybersecurity programs at the site	Security Organization
Information Cybersecurity Program Manager	• Provides oversight of the information security operations • Functions as a single point of contact for all issues related to information security • Plans and coordinates incident response team activities when an information security incident is suspected • Works with regulatory and law enforcement during information security events • Oversees and approves the development and implementation of facility specific components of the ISMS • Manages the development and implementation of the information security education and training	Security Organization
Information Security Specialists	• Provide guidance to staff on how to protect systems from information security threats • Work with cyber and physical security specialists to assess the security of digital systems • Conduct information security audits and tests • Conduct information security investigations as warranted	Security, IT Organizations

CBRN = chemical, biological, radiological, and /or nuclear, ISMS = Information Security Management System; IT = information technology

Table 2.2. Planning the Risk Management Process

Develop Security Objectives	Risk Assessment
Inventory Information and Information Security Assets	
Identify Potential Threat Agents and the Likelihood of Attack	
Identify Potential Threat Vectors	
Identify Potential Vulnerabilities and Likelihood of Exploitation	
Identify Potential Consequences of a Successful Attack	
Assess Security Controls and Risks	
Identify Security Control Enhancements and Risk Reduction	Risk Treatment
Identify Costs Associated with Each Risk Treatment Option	
Make Risk Management Decisions based on Security Objectives, Risk Assessments, Risk Treatment Options, and Resources.	

An initial element of planning is to translate organizational information security objectives (as defined by senior managements) into security objectives at all levels and for all relevant processes within the CBRN facility. These information security objectives should be consistent with information security policies, resource availability, be associated with metrics (when feasible) that can be used to monitor performance, and be updated as appropriate.

In order to evaluate risks and opportunities, a facility needs to understand the information security issues it may face. This begins with identification of all:

- sensitive information products
- systems, networks, and other digital assets involved in information collection, analysis, storage, and use.

In addition, the threat and vulnerability environment should be characterized. This includes the:

- identification of potential threat agents (e.g., who might want unauthorized access to facility information)
- identification of potential threat vectors and determine which are credible
- systematic evaluation of the security vulnerabilities of systems and assets that collect, analyze, store, and use information.

For each type of attack on information security, an analysis is needed of the consequences to the facility of a successful compromise of its information security. This would include consequences that involve a loss of confidentiality, integrity, and availability.

After pulling together information on threat, vulnerabilities, and consequences, the organization should produce estimates of information security risks. This involves an assessment of the adequacy of existing security controls to determine the level of risk reduction that they achieve as part of the integrated information security program. Information security risk estimates can be prioritized for further assessment, with greater attention applied to those that represent the greatest risks to the organization. Figure 2.2 illustrates a simple example flowchart that could be used for identifying and prioritizing risks.

The next step after determining the existence of risk is to identify mitigations or security controls that can be put into place to achieve risk reduction as much as possible.

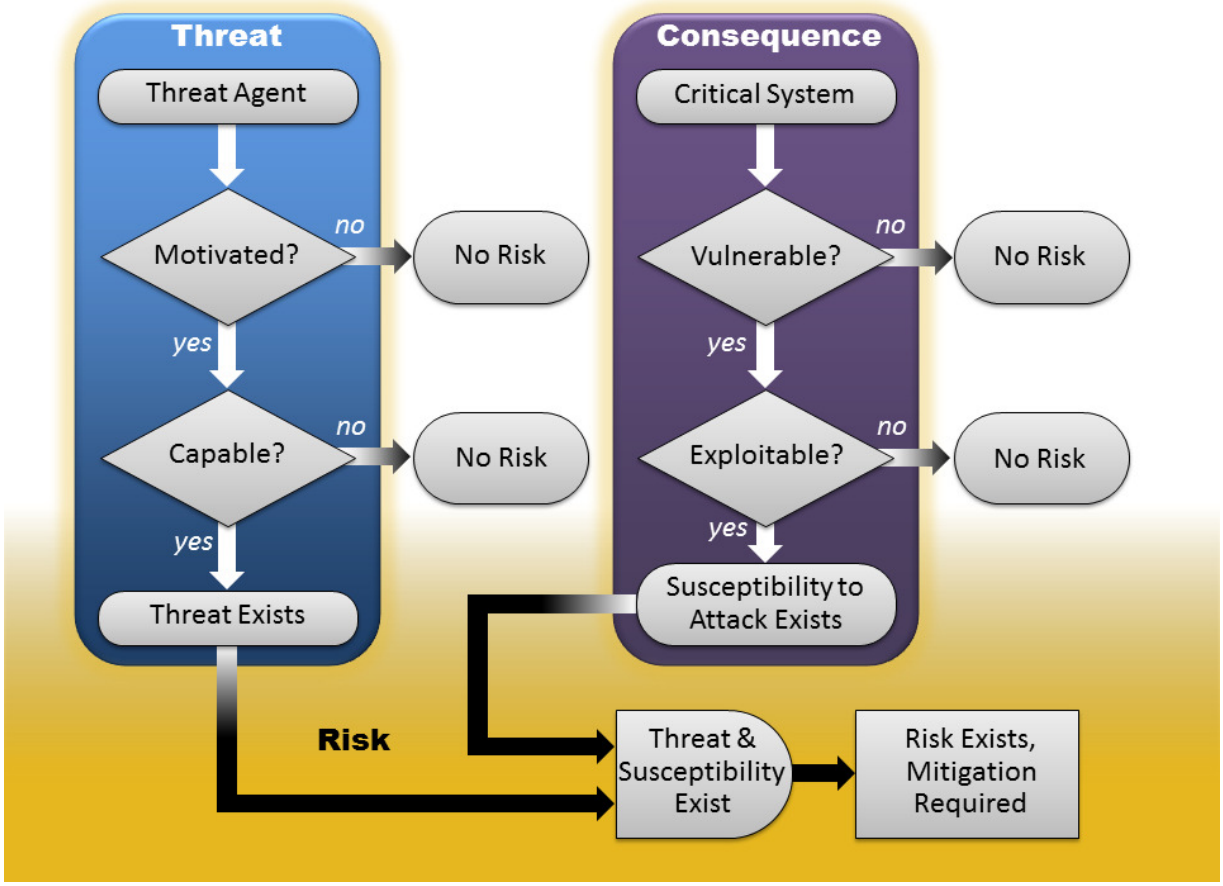

Figure 2.2. A Simplified Flowchart for Risk Assessment

Figure 2.3, which is based loosely on NIST 800-30, Figure 4.1 (NIST 2012a), illustrates the risk relationship between risk assessment and risk treatment, highlighting the importance of internal risk communication within the organizations and the role periodic reassessments play in enhancing the risk management program.

The next stage in planning is the development of a risk management program. Risk management couples the results of risk assessment with risk treatment options. The first step in determining risk treatment options is the identification of potential security controls that can be put into place to achieve risk reduction. These options may involve the implementation or modification of one or more management, operational or technical security controls. Lists of potential security controls are available from many sources. This includes ISO 27001 Annex A (ISO 2014b) and NIST 800-53 rev 4 (NIST 2013b). First, the level of risk reduction achieved from the potential enhancement to the information security program needs to be estimated.

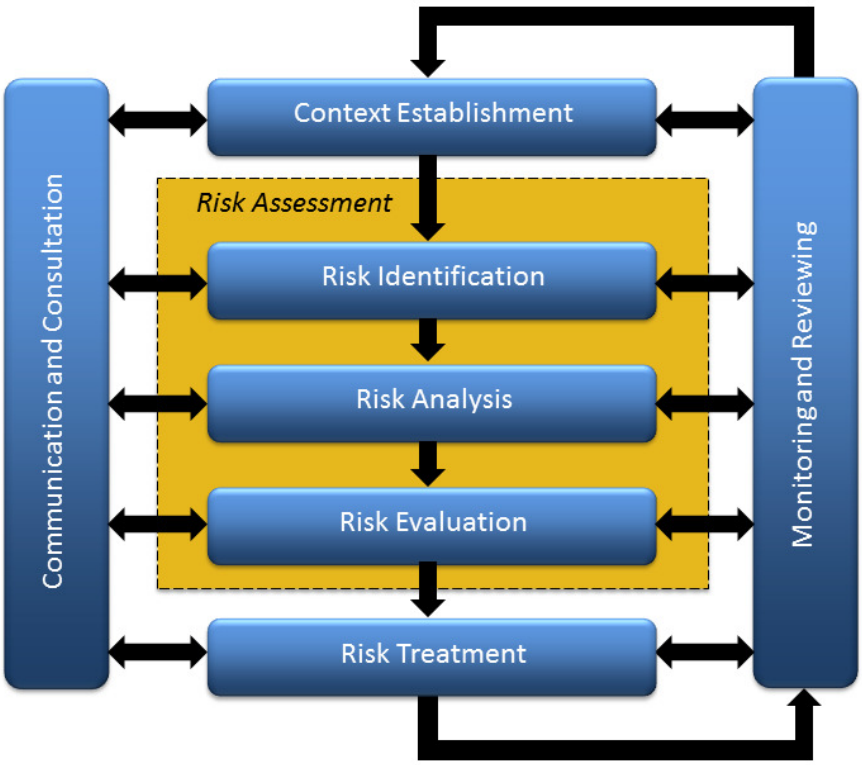

Figure 2.3. Relationships of Various Components within the Risk Management Program

The second step is to determine the cost of implementing or enhancing the set of identified security controls. Costs should include a consideration of design, acquisition, installation, implementation, operation, and maintenance costs.

The third step in the risk management process is to evaluate the risk reduction versus the cost of each potential risk treatment option. A selection can then be made based on an evaluation of legal or organizational requirements, risk reduction benefit, cost, and the acceptability of the residual risk that would remain after the selection of each viable option.

The risk assessment and management process should be clearly documented to support information security auditing and reassessment activities.

Frameworks for risk planning, assessment, and management are found in ISO 27001 and in more detail in NIST 800-39 (NIST 2011).

2.4 Support (Plan)

This performance area involves the resources the organization needs to provide for the establishment, implementation, maintenance, and continual improvement of the ISMS.

The first element in Support is for management to determine the number of personnel, the associated skill set, and time commitment needed to play key roles in the information security management program. Management needs to ensure that adequate human resources are available to meet the objective of the program.

The next element involves ensuring that an adequate information security awareness and training program is in place. The management responsible for information security needs to ensure that CBRN facility personnel (including off-site support personnel) are cognizant of the facility's information security program and policies. Each staff member needs to understand his or her role in protecting information and the implications (e.g., penalties such as suspension, reassignment, or termination) for not fulfilling their responsibilities under the information security program. To achieve an appropriate level of awareness, the organization needs to determine what they will communicate in regard to information security, when this communication will be made, who will initiate this communication, and who will be the target of this communication

The final major component in the support plan involves documentation. Documentation is a key element in maintaining an effective information security program. Documentation will differ from organization to organization, based on its internal risk management requirements. All documentation should identify its author and date and be securely stored so it is available for use and review by authorized personnel. The information security program will need to define its own controls on access to information security documentation, change control, storage, audit, and retention.

2.5 Operation (Do)

In the operations phase, the organization needs to implement, manage, and maintain its information security program. This includes implementing planned cyber, physical, and personnel security activities during the collection, analysis, storage, and use of information. It also includes the secure design, procurement, installation, operation, and maintenance of information technology assets. Adequate resources are allocated by the facility to fully implement the information security program—including security elements that defend information from attacks and resilience elements that minimize the impact of a successful attack.

Operational roles and responsibilities are carried out by senior management, facility managers, system managers, information security staff, and all other staff who have access to sensitive information or the information technology systems. This includes systematic security monitoring of information technology assets and the security controls that protect these assets, information at rest, and information in motion. Information security awareness and training is an ongoing activity for all staff members. Effective information security risk communication is maintained with internal and external stakeholders. Information security incident response capabilities are maintained and exercised.

The risk assessment and management program is maintained during the operations phase. The frequency of risk assessment and risk management activities is defined in the information security program and should be based on the needs of the organization and the speed at which its assets and the security environment are changing.

During this phase, the continuous improvement would be carried out on the steps completed in planning phase's Risk Management Process (Figure 2.3) and approaches updated based on changes in the

organization and technologies. Lessons learned during the risk assessment and risk management process should be used to support the continuous improvement of the information security program.

2.6 Performance Evaluation (Check)

The performance evaluation involves a periodic check of the implementation of the information security program charter. The organization should determine what needs to be evaluated, the method of performing the evaluation, who will conduct the evaluation, the periodicity of the evaluation, and how the evaluation results will be addressed.

At a minimum, the evaluation should survey how well the key requirements in its information security program are being followed and where requirements gaps may exist. The specific scope of the evaluation and the criteria to be used to assess the program should be defined before the evaluation begins. Qualified personnel should be assigned to conduct the evaluation and conflicts of interest should be avoided. The evaluation of security controls should include a desktop review of information assets and security controls. It should also include a field inspection of selected information assets and security controls to ensure they are configured and are operating as designed.

Evaluation results should be provided to relevant management personnel. Areas of nonconformity should be identified and management should prepare a corrective action plan to address any major issues. Lessons learned from the evaluation should be used to support the continuous improvement of the information security program.

2.7 Improvement (Act)

As part of the life cycle nature of information security, a process of continuous improvement should be included as a key component of the information security program. Results from risk assessment and risk management activities, as well as performance evaluations should be used to support continuous improvement activities. However, continuous improvements should not wait for periodic reassessments and evaluations. Over the course of routine activities, changes in threats, vulnerabilities, and security technologies will be identified and security enhancements should be made on as warranted to address changes in the information security landscape.

The improvement performance area also involves changes made to address nonconformities in the information security program and make associated corrective actions. Nonconformities should be examined to determine the cause of the problem and to determine if actions are needed to correct either the specific problem or a more systemic issue that the nonconformity might highlight.

All corrective actions and improvements should be documented as part of the information security program.

3.0 BEST PRACTICE RECOMMENDATIONS FOR INFORMATION SECURITY PROGRAMS

This section provides a set of best practice security recommendations for CBRN facilities. This guidance is based on international standards and best practices, the experience of the information security experts on the document writing team, and the many CBRN personnel and government officials from around the world who participated in the stakeholder review of this document. Each recommendation highlights a key concern for information security programs. The integration of these recommendations into an information security program should provide a foundation for a successful program.

3.1 Recommendation: Implement a Graded Approach to Protect Critical Systems

CBRN facilities contain numerous computer systems that contribute to the overall operation of the facility. Some of these systems are information technology (IT) systems that are used to create, acquire, process, communicate, or store data. Information systems support management and decision making. IT systems include data acquisition systems that act to sample, collect, and provide data in support of CBRN facility systems. Operational technology (OT) systems are hardware and software that monitor and/or control physical devices, processes and events in the enterprise. These devices are often referred to as *control systems.* Control systems consist of a device or set of devices that act to manage, command, or regulate the behavior of a process, devices, or other system. In addition to their control function in the physical world, OT systems can perform IT-like functions to create, acquire, process, and communicate data. Control systems typically employ a control loop including proportional integral derivative (PID) controllers, programmable logic controllers (PLCs), sensors, and actuators that seek to regulate a variable at a set-point or reference value.

All computers systems are made up of digital assets. If a digital asset is compromised, it could potentially affect the ability of a CBRN system or network to perform its intended function and result in a loss of confidentiality, integrity, or availability of data or system function.

It is important to recognize that all information or information systems within a CBRN facility are not of equal importance. The relative significance of a system to the overall operation of a CBRN facility is dictated by the functions it serves. While the loss of some types of information or systems may have negligible impact upon the facility, the loss of others may have more serious consequences. For example, information on the CBRN security systems or control systems that perform safety and security functions, poses greater security risks than information providing routine business functions.

Correspondingly, the level of protection afforded to information or information systems within CBRN facility should be based on the importance of the system. The use of a graded approach ensures that a disproportionate amount of security resources are to systems that represent low risk.

3.2 Recommendation: Integrate Physical and Cybersecurity

Physical security and cybersecurity are often treated as separate problems. At many CBRN facilities, physical security specialists and cybersecurity specialists may operate with little or no interaction. This

organizational disconnect can result in a failure to recognize and address significant crosscutting security vulnerabilities and underestimate the associated security risks. Crosscutting issues include cyber-enabled physical attacks and physical-enabled cyberattacks.

A cyber-enabled physical attack could be a cyberattack that involves theft of information involving facility security plans or disrupts the availability or integrity of security information (e.g., alarm systems, and video displays) needed to support the proper functioning of physical security systems. This type of cyberattack would increase the likelihood that a simultaneous or subsequent physical attack would succeed. A physical-enabled cyberattack involves unauthorized physical access to sensitive data or digital devices. This kind of cyberattack could result in the destruction, disabling, or altering of the security controls that protect sensitive information or information systems, thus increasing the likelihood that a simultaneous or subsequent cyberattack would succeed.

Strong lines of communication are needed between a facility's physical and cybersecurity programs to address blended threats. In many cases, efficiency can be increased and costs reduced by combining the physical and cybersecurity programs into a single, integrated security program that can more effectively deal with a range of threats—including those targeted against information and information systems.

In a related issue, security evaluations and force-on-force exercises at CBRN facilities often only focus on traditional types of physical attacks. Because of the added complexity and the lack of experience with cyberattacks, cyber components are often excluded from physical security training and exercise scenarios. By not training physical security forces to recognize and withstand a cyber-enabled physical attack, or evaluating their performance under such an attack, physical security forces may be inadequately prepared to deal with a cyber-enabled physical attack that can threaten sensitive information or information systems.

Security training, exercises, and evaluations should routinely include cyber elements in physical attack scenarios. This would enhance the readiness of physical security personnel to deal with the potential that well-organized attacks on information or information systems will include both cyber and physical elements.

3.3 Recommendation: Secure the Data Center

All the cyber protections in the world are insufficient if an attacker can walk into the data center and steal or destroy data. An information security manager must also consider the potential threat of natural disaster to a data center. An organization may even be bringing threats into the data center—consider the potential impact if the sprinklers malfunctioned and activated in the data center.

An organization should consider which staff members are able to access the data center. Establish requirements for who can access the data center, these requirements are ideally tied to position or role. Some very secure organizations may implement a two-person rule to get into the data center.

Questions that will need to be considered in securing the data center follow.

- How will access to the data center be granted? If using a key, who controls the spare keys?
- How are staff members prevented from making additional copies?

- If using a badging system, how do you ensure that staff members are not sharing badges? A badge and a personal identification number (PIN) with periodic reviews by the security organization may be the best fit. If the data center is within an environment that the organization cannot control, a guard is a possible solution. The data center could also be alarmed or under video surveillance with physical security response if necessary. Can the organization's data center be taken off-line by an errant piece of heavy equipment?
- If the data center's primary source of power is compromised what is the back up? Most organizations choose to use uninterruptible power supplies as a failover, but typically these will offer only a few minutes of backup power. Consider if that is sufficient for your organization's needs. A gas-powered generator is another potential solution. Remember that the data center's cooling must remain operational as well.

3.4 Recommendation: Secure the Human

Every authorized user is a potential source of unintentional or malicious data loss. IBM Global Technology Services reported that in 2013 a major retailer with millions of leaked credit cards could face more than $100 million in direct costs, including fines. A data breach caused by a trusted insider can affect the faith of consumers, customers and the reputation of the organization itself. (IBM Global Technology Services 2014). To mitigate this, an organization must train every user to threats they face and the actions they should take. The organization must also protect from users who become adversaries.

Not every position has equivalent access, and therefore does not present the same risk. Categorize users to determine who poses the greatest threat to the organization. Those users or roles that have the greatest access should receive additional background screening and auditing.

When staff members are terminated or change departments within the organization, consider how to handle the change in access. Prior to the user being notified of termination, should all access be revoked? According to the Software Engineering Institute (SEI) Computer Emergency Response Team (CERT) Insider Threat Center, 90 percent of the staff members that commit IT sabotage had some form of privileged access (CERT 2010). When users change departments, remove all access, and then grant only the new access that is needed. If necessary, consider nondisclosure agreements with sensitive staff members or users.

3.5 Recommendation: Secure Data Exchange

In 2012, the United States established a National Strategy for Information Sharing and Safeguarding. This strategy focuses on providing guidance for more effective integration and implementation of policies, processes, standards, and technologies that promote secure and responsible national security information sharing to ensure the right information is shared with the right people, at the right time (The White House 2012). Every organization finds itself sharing sensitive data with other departments spread across the region or globe or with other organizations across an untrusted medium, often the Internet. An information security manager is responsible for securing the data in transit and in storage while making the data still possible to use. The process becomes more complex because of export control laws regarding the use of encryption.

The organization should enter into agreements with third parties regarding how the data will be used and stored. The agreement will also include scope of responsibility, when does each organization accept ownership of the data. How data will be transmitted is of primary concern, ideally the organizations can use a widely available encryption tool, like Pretty Good Privacy (PGP). In some cases the most efficient solution is to store data on hard drives and ship those hard drives.

3.6 Recommendations: Adopt Information Security Policies, Standards, and Procedures

Successful security management planning relies upon the existence of properly developed policies and procedures. Effective information security policies establish the overall security objectives, goals, and practices, and provide additional detail on roles and responsibilities for cybersecurity within an organization. The policies developed should be specific to the CBRN site and clearly identify the objectives, requirements, and needed references to define the conduct of the cybersecurity program to secure and protect systems from security threats. Where possible, the developed site-specific security policies should be designed to complement existing security policies that may exist in organizations with more than one facility. When site-specific policies conflict with those of existing organizational policy, or when adherence to the organizational policy would result in an unacceptable increase in risk to the systems existing within the CBRN facility, the site-specific cybersecurity policies should take precedence.

CBRN facilities should develop procedures, based on published technical standards where applicable, to implement the developed cybersecurity policies. The developed policies and procedures need to be periodically reviewed to ensure that they are sufficient to address the risks identified for the information and information systems they are intended to protect. In addition, issues resulting from evolving threats, vulnerabilities, and security controls should be addressed.

Policies and procedures should exist to address a variety of key topical areas, such as:

- threat identification
- integration of cyber and physical security elements into an information security program information security roles and responsibilities
- assessments of information security systems, related digital assets, and networks
- identification and protection of sensitive information
- implementation of a defensive model and architecture
- identification, implementation, and management of information security controls
- life cycle security for information and information systems
- security monitoring of sensitive information and information systems
- malware protection
- incident response
- disaster recovery
- reporting/notification requirements

- cybersecurity awareness, training, and education of facility personnel.

It is recommended that CBRN staff should review ISO 27002, *Information Technology, Security Techniques, Code of Practice for Information Security Management* (ISO/IEC 2013), in addition to NIST SP 800-12, *An Introduction to Computer Security – The NIST Handbook*, (NIST 1995) for areas of applicability when developing site-specific cybersecurity policies to protect critical systems.

3.7 Recommendation: Identify Credible Threats and Vectors of Attack

A threat represents the intent, capability, and opportunity of an adversary to attack or inflict harm. The magnitude of a threat is dependent on an attacker's motivation, capability, and opportunity. Attackers carry out threats against vulnerable targets using tools, tactics, and procedures to accomplish their objectives in response to some motivation. Their capability refers to the knowledge, skills, and tools necessary to conduct an attack. Opportunity represents the situational circumstances that would support the initiation of an attack. The relative magnitude of the threat directly corresponds to the proportional quantities of each of these elements. An attacker with a clearly stated or well-known intent, a high degree of capability, and knowledge could represent a serious threat. In contrast, an attacker that has an unfocused intent, with little or no capabilities, and lacking opportunities would represent a negligible threat.

It is important to understand that the relative interest levels of threat agents in a given target can vary over time. In some cases this variance can be traced to a risk-effort-reward mindset (i.e., the payoff for conducting an attack is insignificant to the risk or effort involved). In other cases, the interest level of a given class of threat agent may only be limited by the capabilities of the agent to conduct an attack (i.e., the agent is limited by insufficient knowledge or tools). Conversely, it is also important to recognize that the emergence of new tools and methods that act to overcome such limitations can also act to elevate the interest in this same class of threat agent.

A cyberattack on an information system is a manifestation of a threat (e.g., assault) conducted by a threat agent against an IT or OT system or its supporting infrastructure. This covers a wide variety of events. Attacks may involve

- viruses
- worms
- malware
- forged data
- denial or disruption of access or service
- unauthorized access or unintended use of system assets
- theft or destruction of hardware or data
- modification of environmental conditions to negatively impact system functionality.

Cyberattacks typically involve a challenge to the state of a system. Attacks may involve physical and logical (cyber) threats to computer systems or networks, may be directed or non-directed in nature, and are conducted by threat agents (e.g., adversaries) having either malicious or non-malicious intent.

In order to develop adequate protections for a system, it is helpful to understand what actions will cause the security designed into the system to break or fail. In 1999, information security expert Bruce Schneier popularized the concept of attack trees (Schneier 1999). Schneier recognized that many organizations often misapply security solutions, incorrectly believing that by applying more security an increased security posture would result. Schneier identified that in many cases overall system security was actually reduced with the application (or rather misapplication) of additional security measures. He attributed this result to threat modeling that is performed on an *ad hoc* basis, if it is performed at all.

Attack trees are a mature security concept that provides a systematic method to describe threats that may exist for a given system. As an analytical tool, attack trees are a powerful technique because, unlike other forms of analyses, they require the analyst to adopt the mindset or perspective of the attacker. This approach also adds significant value to the identification of scenarios that attribute to an attack. Attack trees are useful in

- identifying potential vectors of attack
- understanding where critical points of vulnerability exist
- understanding the effectiveness of deployed countermeasures
- determining optimal use or placement of countermeasures
- focusing risk management efforts to address the most likely vectors of attack
- adding value to multiple phases of the system design life cycle.

Figure 3.1 illustrates an elementary example of an attack tree.

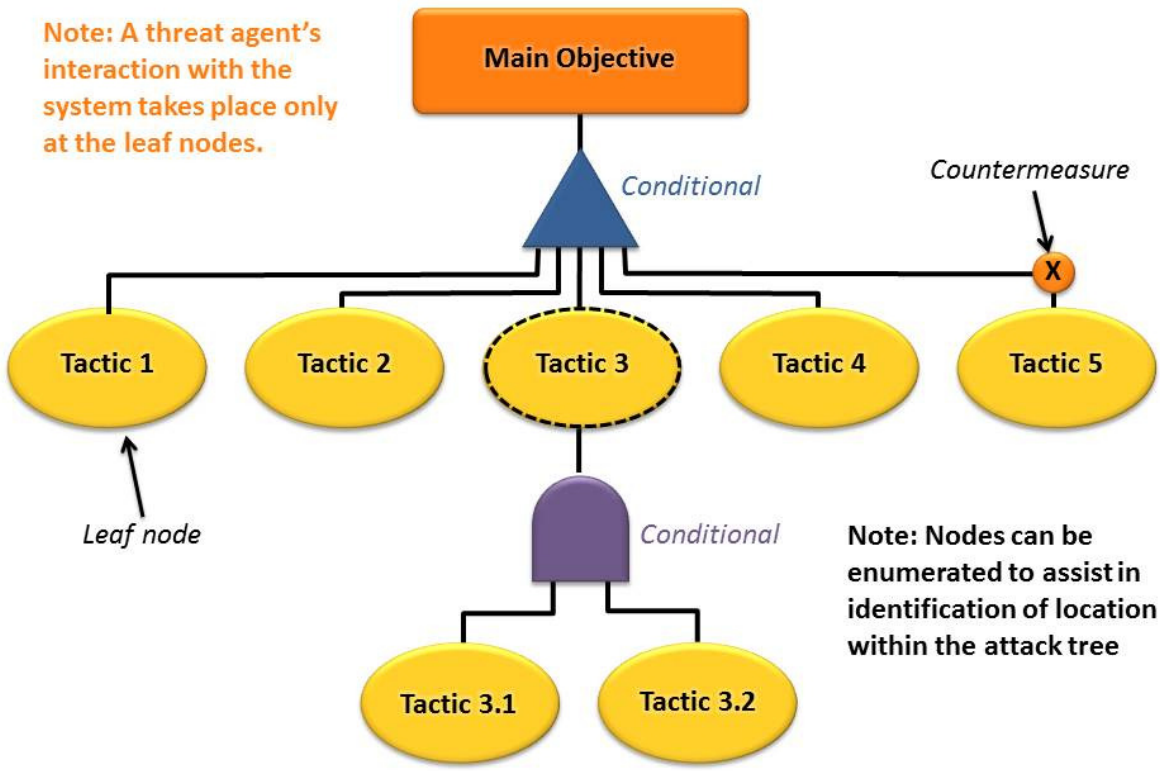

Figure 3.1. Simplified Attack Tree

The attack tree itself can be visualized as an upside-down tree with a root node that establishes the objective for the tree. Branches exist within the tree extending down from the root node to leaf nodes that identify tactics to be employed by threat agents. Conditional elements in the form of logical "OR" and "AND" gates are used to understand any relationships that may exist between the use of tactics to achieve the objective. Note that while only a single root node exists, multiple leaf nodes are possible because there may be many ways to accomplish the goal. Additionally, leaf nodes themselves are likely to contain other leaf nodes that define further actions that are required to meet the goal of the parent leaf. In Figure 3.1 it can be seen that tactics 1 OR 2 OR 3 OR 4 will result in meeting the main objective, however tactic 5 cannot be accomplished because of a deployed countermeasure. Additionally, for tactic 3 to be successful, sub-tactics 3.1 AND 3.2 must be accomplished. The dashed outline of tactic 3 identifies that a dependency relationship exists for this tactic. Enumeration of the various tactics occurring within individual branches of the tree makes for easy identification and reference, especially when dealing with trees that contain multiple, deeply nested branches that cannot be easily depicted.

Many different types of metrics can be represented in an attack tree to better understand each of the various vectors of attacks. Such metrics may include, but are not limited to

- level of difficulty
- level of intrusiveness

- physical versus logical access
- insider versus outsider
- special equipment requirements
- estimated cost for each tactic or vector of attack
- level of threat agent risk acceptance for each vector
- estimated time of completion for each vector or tactic
- estimated cost associated with a given tactic
- estimated level of skill required for a given tactic.

Metrics may be combined to ascertain the threat agent attributes that would be required to successfully exploit a given vector of attack. Some of these metrics may be Boolean in nature (i.e., Yes/No, True/False, Possible/Impossible) while others may represent values that are more continuous (i.e., probability of success, likelihood that a given attacker would choose such an attack, among others).

3.8 Recommendation: Identify, Eliminate, and Mitigate Vulnerabilities

For an attack to succeed, it must exploit some inherent weakness or vulnerability contained within the target. The term vulnerability is defined to be a weakness in the physical or electronic configuration of an asset that could allow an action that compromises the security of the asset. If the vector of attack is poorly executed or attempts to leverage an exploit that the target itself is invulnerable to, the attack will likely prove to be unsuccessful. This basic concept holds true regardless of whether the attack takes place within physical or cyber domain.

A related concept to consider is that no target is completely free from all forms of vulnerability. Thus, there is no method of achieving complete security. Regardless of the amount of money, technology, person-hours, and effort expended, the security of any system (whether digitally based, physically based, procedurally based, or a combination thereof) can at some point break down. Generally, the more complex the system is, the more likely it is to contain weaknesses. Whether it is because of failures in technology, errors in implementation, a breach of trust by a human component, or some other factor within the system, manipulation of a critical factor could result in an exploitable vulnerability.

Modern computer systems and networks are incredibly complex mechanisms that rely upon the proper implementation and execution of hardware, firmware, software, and user interaction to perform their design-based functions. The code base of contemporary operating systems and applications is staggering, often measured in millions of lines of code. The number of annual reported vulnerabilities across all operating system and application software between 2004 and 2013 is illustrated in Figure 3.2 (NIST 2014b). An important factor to consider is that the data represented in Figure 3.2 reflects the total reported vulnerabilities. Figure 3.2 does not represent nonreported vulnerabilities or those vulnerabilities that have yet to be discovered. An overwhelming number of identified security issues affecting operating system and application software can be traced to poor programming practices, insufficient development of security requirements, and ineffective implementation of security controls.

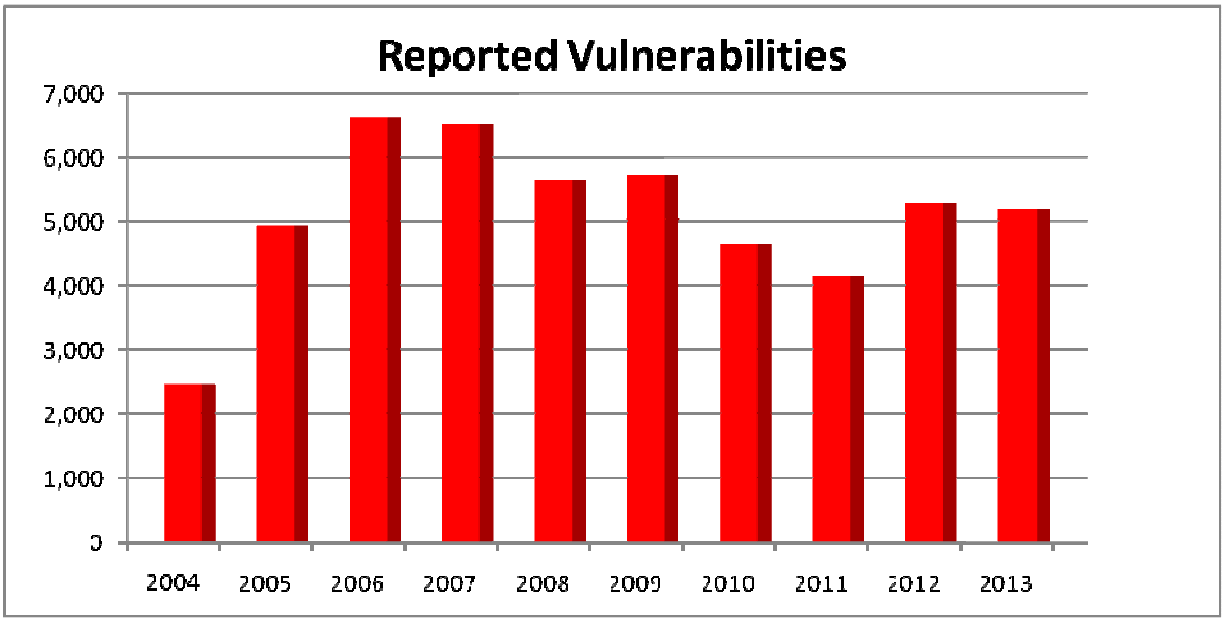

Figure 3.2. Computer Vulnerabilities Reported to the U.S. NIST National Vulnerability Database

To make a given target less susceptible to an attack, it is necessary to harden the target. Hardening of a target can be accomplished through vulnerability elimination or mitigation.

Vulnerability elimination requires reconfiguration or redesign of the system to ensure that the identified weakness no longer exists. In the case of digital systems, this could potentially involve redesign of system hardware, firmware, operating system software, or application software to remove vulnerabilities. With the known vulnerability eliminated, successful compromise cannot be achieved (at least for that particular vector of attack—other vectors may exist). The engineering costs involved with vulnerability elimination can be significant. A robust design process will take this fact into consideration, attempting to identify and eliminate security issues early in the design process rather than later, where the expense is considerably greater.

Vulnerability mitigation seeks to address the identified weakness either through reconfiguration of the system or through the application of security controls. In the case of digital systems, examples of system reconfiguration to mitigate vulnerabilities include, but are not limited to:

- removal of unnecessary user accounts
- removal of unneeded or default file shares
- removal or disablement of vulnerable operating system services and ports
- implementation of access controls on file systems, registries (if any exist), and binaries
- implementation of encryption mechanisms.

3.9 Recommendation: Implement Defense-in-Depth Principles

No information system is completely free of vulnerabilities. The more complex an information system, the more likely it is to contain weakness or vulnerabilities. To counter vulnerabilities that cannot be eliminated or mitigated, protective strategies that embrace the concept of defense-in-depth or resilience should be implemented.

Defense-in-depth represents an approach to system security where multiple layers of security are implemented to protect against failure of a single component or layer. The concept of defense-in-depth originates from a military strategy that seeks to delay, rather than prevent, the advance of an attacker by yielding space in order to buy time. The time gained during the attack allows more time for informed decision-making to counter the assault.

Defense-in-depth can be visualized as a series of concentric layers of security in which the vulnerabilities that exist for a given layer are prohibited from existing within the adjacent layers. A threat agent seeking to attack such a system would be forced to identify and exploit nonidentical vulnerabilities 1-5 existing at each successive layer, as illustrated in Figure 3.3.

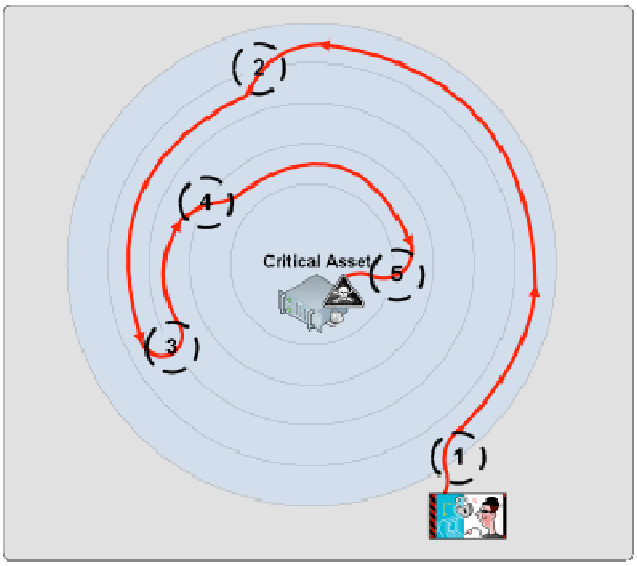

Figure 3.3. Defense in Depth

A CBRN information security program should develop, document, and implement a comprehensive and diverse set of protective strategies capable of detecting, isolating, and neutralizing unauthorized activities in a timely manner to ensure that the design-based functions and capabilities of critical systems are maintained. The protective strategies should exhibit defense-in-depth characteristics ensuring that the failure of any single element of a strategy does not result in successful compromise of a critical system by a cyberattack. The strategies developed need to protect information systems from various vectors of attack that involve both physical and logical compromise.

One example of a defensive strategy is the implementation of network architecture that uses multiple zones (or levels) of increasing security that define formal communication boundaries where defensive

measures are deployed to detect, prevent, delay, mitigate, and recover from cyberattacks, as shown in Figure 3.4.

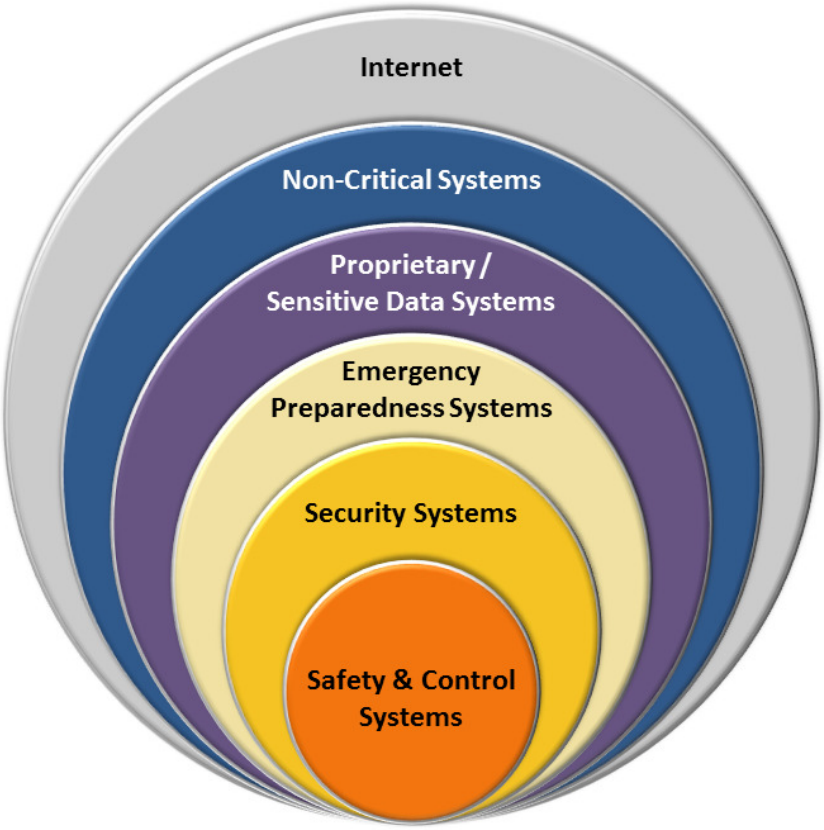

Figure 3.4. Multiple Layers of Security

The controls implemented within each layer of security need to be capable of detecting the unauthorized activity of the threat agent. Detection of unauthorized activity should trigger preplanned security response mechanisms that seek to delay or prevent the advance of the threat agent toward the target of interest. The developed strategies must consider vectors of attack involving both physical and logical compromise of protected system components.

A defensive data flow model represents a high-level abstraction of allowed data flows occurring between layers of differing security. Rules within the data flow model dictate the types of communication flows that are allowed between the layers. As an example, Figure 3.5 depicts a model with five security levels. Level 4 represents that highest level of security while Level 0 represents the least level of security.

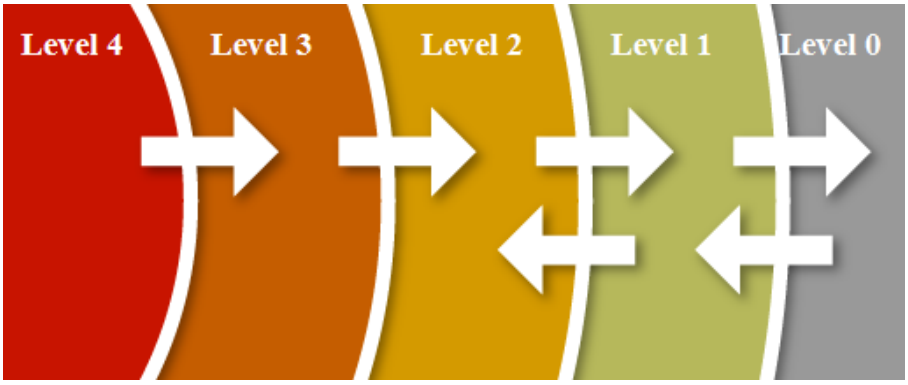

Figure 3.5. Defense Data Flow Model

The arrows between each level identify the allowed flows of data between the levels.

- Data may be passed from the Level 4 Network to the Level 3 Network.
- Data may not be passed from the Level 3 Network to the Level 4 network.
- Components within the Level 4 Network must initiate the communication with components located in the Level 3 Network.
- A dependency relationship must not exist between the Level 4 Network and the Level 3 Network that would prevent a Level 4 component from performing its design base function.
- Bidirectional data flows are permitted between Levels 2 and 1, and Levels 1 and 0.
- Data flows are allowed to occur only between adjacent levels. Data flows may not "hop" or "skip" intervening levels.

A defensive data flow model will influence the design of the network architecture used to secure information within the CBRN facility. A complete model will

- accommodate the need for both physical and logical security
- define the acceptable types of communications occurring between digital assets that are maintained at different security levels
- implement appropriate defensive security controls at the boundary between each security level so as to be able to detect, prevent, delay, mitigate, and recover from a cyberattack originating from the lower security level
- provide a method to identify the location systems, digital assets, and communication pathways existing within the defensive model
- minimize the number of allowed applications, services, and protocols needed to support the design function of the information systems.

3.10 Recommendation: Implement Life Cycle Security

The security of an information system is dependent on the level of security present throughout an asset's life cycle. A security lapse in any phase of the life cycle can affect information security. To create secure systems, the following conditions must be met:

- The design of the system's hardware and software must be secure.
- The implementation (or coding) of the design must be secure.
- Any reused components (hardware or software) must be secure.
- The security features or attributes selected must be correct.
- The implementation (or coding) of the security features must be correct.
- The environment in which the development occurs must be secure.
- It is important to prevent inadvertent disclosure of sensitive information as a side-effect of the disposal of IT systems.

Additionally, as security is an emergent property of the system, prequalification of the component code will not guarantee secure software, as it is possible to use the secure components in an insecure manner.

Security assurance testing is markedly different from that of functionality, reliability, or safety. In each of the other cases, resultant conditions are predicated upon anticipated inputs or events. Security assurance testing, however, requires the presence of unexpected input or misuse of the system as designed to cause unanticipated behavior. This often requires creativity upon the part of the software quality assurance tester to develop valid security test cases.

To ensure that modifications made to CBRN facilities that have the potential to affect the information security are appropriately analyzed, evaluated, and implemented in a controlled manner, a comprehensive and structured approach is required to address cybersecurity throughout the life cycle of the system. A typical life cycle might necessarily include the following phases and activities:

- **Concept.** During the concept phase, analyses should be conducted to identify the security capabilities of the proposed system.
- **Requirements.** During this phase, requirements are defined to address potential security issues. These may include security requirements for the system configuration, external interfaces, human factors engineering, data definitions, and documentation. The developed security requirements should be part of the overall system requirements.
- **Design.** In this phase, the security requirements identified in the requirements phase are translated into specific design configuration items in the design description.
- **Implementation.** In the implementation phase, the system design is transformed into code, database structures, and related machine executable representations. The coding of the software should be secure—including both software developed in-house and acquired software. Supply chain security issues come into play during this phase.

- **Testing.** The objective of testing security functions is to ensure that the system security requirements are validated by execution of integration, system, and acceptance tests where practical and necessary.
- **Installation, Checkout, and Acceptance Testing.** The objective of this phase is to verify and validate the correctness of the physical and logical system security features associated with the system and its operating environment.
- **Operation.** In this phase, the developed system is used by the CBRN facility in its intended operational environment. During the operations phase, the facility should ensure that the system security is intact by using techniques such as periodic testing and monitoring, review of system logs, and real-time monitoring where possible.
- **Maintenance.** The phase occurs when the operational system is accessed or modified as part of routine maintenance or enhancement activities. System modifications may be required to correct errors (corrective), to adapt to a changed operating environment (adaptive), or to respond to additional user requests or enhancements (perfective).
- **Retirement.** In this phase, the CBRN facility should assess the effect of replacing or removing the existing systems or its security controls from the operating environment. Security procedures should include cleansing the hardware and data of facility information before repurposing or disposing of the asset.

IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes," is a useful resource for addressing the software component of life cycle issues.

3.11 Recommendation: Implement an Information Security Incident Forensic Response and Recovery Capability

An incident response and recovery process is an important element for information security. If an incident involves computer systems and networks at a CBRN facility, an immediate goal is to identify the problem, implement corrective actions, and return the facility to normal operations in a timely manner. It is also important to safeguard the forensic data necessary to counter future threats.

Incident response for an information security event should be integrated with the incident response programs for cyber and physical security events; they must meet both national and international reporting requirements—for example, through Critical Incident Response Teams (CIRTs). If there is a cyber component to the compromise of information, cybersecurity incident response will come into play. If there is a physical or personnel component to the compromise, physical security incident response will be involved. For many potential events, both the cyber and physical incident response will need to coordinate operations.

An information security incident response and recovery process should include the following components:

- Preparation
- Identification
- Containment

- Eradication
- Recovery
- Post-incident analysis
- Forensics activities
- Information security awareness training.

3.11.1 Preparation

This stage involves the formation of an integrated CIRT that should have the technical skills and authority to effectively respond to a potential information security event. The CIRT may overlap with the cyber and physical incident response teams, so that it is not a separate team but a component of the cyber and physical incident response teams. The Preparation stage also should include the development of processes, procedures, and controls that the incident response team will employ upon the discovery or identification of a potential or actual information security incident. These activities would support a coordinated response and recovery effort if the event escalates into an actual information security incident. Proper forensic techniques should always be followed in case the incident is later presented to a court of law as discussed in NIST 800-86 (NIST 2006).

A CIRT will have a team leader and include various facility specialists. This may include a cybersecurity, physical security, information technology and operations technology staff member (depending on what types of systems are affected), and staff members from facility management, risk assessment, and other disciplines. Each role should be defined and staffed to support all of the activities necessary to ensure a coordinated response. Areas of responsibility and certain separation-of-duty requirements should be considered when defining the duties of each role and agreed upon by each group to document the area of responsibility. Further, each role requires levels of technical skill and authority commensurate with the activities to be performed. The CIRT should include senior facility leadership to ensure that the team can act quickly and with appropriate authority to protect facility systems and networks.

Procedures should be developed for incident response and recovery with the goal of ensuring rapid responses and recovery for any affected systems or assets. The CIRT should be prepared to provide impact assessments to directly support operational decisions. Written policy, plan, and procedures for incident response and recovery activities should cover:

- mission, strategy, and goals
- commitment and approval by senior management
- organizational structure and definition of roles, responsibilities, and levels of authority
- definition and identification of information security incident
- incident containment: notification, response, escalation, and team activation
- threat-level classification and prioritization for incidents
- metrics and performance measures

- postulated incidents or attacks, indicators, and planned responses
- incident documentation and reporting requirements
- secure communication methods to be used within the incident response team and with external law enforcement and regulatory agencies.

This list is adapted from NIST 800-61 (NIST 2012b).

3.11.2 Identification

At the Identification stage, the focus is on determining whether an information security event has occurred or is occurring, and how to classify the event. Although a report of a suspected incident can be generated by either users or automated intrusion detection systems, validation and classification of an incident generally require detailed knowledge and a variety of system experience and skills. The following actions should take place:

- Initiate a log of the incident recording all relevant facts. Proper collection, control, and dating of material will better facilitate the post-incident analysis. It is recommended that an approach such as an incident or log form be developed and used to ensure that basic information, data, or steps are not missed during the often-stressful response to an incident.
- The assessment of initial incident reporting, as documented in procedures, should determine if the event is likely to achieve the threshold that warrants the activation of the information security response team.
- Make initial notifications. The implementation of a notification tree employing electronic or handwritten forms is common practice and provides an excellent record to supporting response correlation. It also supports internal and external notification requirements. Notification tree procedures should indicate when external organizations/agencies are to be contacted.

3.11.3 Containment

The Containment stage involves taking actions to halt the further spread of an information security attack. Depending on the severity and subsequent classification of the event, various containment activities may be warranted. Containment responses may involve firewalls, intrusion prevention systems, or other technologies configured to manually or automatically employ preconfigured rules that are designed to limit the spread of an attack or the exfiltration of information. When appropriate, procedures may also call for physical isolation by automatic or manual methods that provide disconnection of affected systems or devices from the key systems or communication pathways by which the cyberattack may propagate.

Once positive containment is achieved, it should be assumed that the affected systems and networks have been compromised. Before containment is relaxed, operations and engineering should ascertain the extent of actual or potential corruption and possible damage to the system.

3.11.4 Eradication

The Eradication stage involves eliminating the current information security attack (e.g., malware, virus, unauthorized system access). For some events, the Containment and Eradication stages can be combined as steps that are taken to quickly recover a system, network, or device. Eradication requires a thorough understanding of the cyberattack.

Responses and actions performed during the Eradication stage should include the following:

- Identify the attack and determine the pathway of compromise.
- Patch or clean any affected networks and/or systems of any "hostile" code.
- Alternatively, replace affected hardware with clean disks or equipment, and reload the asset from a known good (i.e., cyber-secure) backup.
- Take steps to reintroduce the restored networks and systems that would to prevent the exploit or infection from reoccurring should eradication be challenged.
- Using security tools, perform an automated vulnerability analysis on the asset, system, or network to be restored. Search for related vulnerabilities and update software as required.

A successful eradication process should provide a detailed assessment of the attack and response actions. While all participating organizations should be involved and consulted, the incident response team should have the sole authority to determine when the cyberattack agent has been eliminated and a recovery effort can be initiated.

3.11.5 Recovery

The Recovery stage concentrates on returning the affected information system or network to a fully operational status. Prior to such restoration, the information security response team should determine that the steps taken during the Eradication stage were sufficient to prevent a repeat of the event. Recovery activities should include all of the following that are applicable:

- Restore data sets, operational software, firmware, operating systems, and configurations from known good backups.
- Alternatively, reload the entire system. Make certain that the code being restored is not itself infected.
- Reconnect systems and devices and reestablish connectivity with other subsystems or components.
- Carefully monitor the devices and network traffic to ensure a repeat compromise does not take place.
- Participate or observe while site-specific procedures provide operability assessments and determination for affected systems.

3.11.6 Post-incident Analysis

This stage involves conducting a post-incident analysis to determine the effectiveness of many components of the information security program, most important, the defensive strategy and actions taken

by the incident response team throughout the event. The analysis should determine where security controls may have been insufficient. If inadequacies are found, security controls should be reevaluated and enhanced accordingly.

Incident handling, response reports, and post-incident data may contain sensitive information. Each organization should follow its established data sensitivity processes and procedures to ensure protection of such data commensurate with the event.

During this stage an evaluation of aspects of the information security program should include the following activities:

- Evaluate the effectiveness of the defensive strategy and security controls in the wake of the incident. Identify deficiencies, identify corrective actions, and implement corrective actions.
- Evaluate the incident handling and response process to determine areas of weaknesses and strengths. Identify corrective actions for weaknesses and implement these corrective actions.
- Determine the effectiveness of communication channels and other information sharing avenues that may benefit others within your organization, region, country, or international CBRN facility community.

3.11.7 Forensics Activities

Digital forensics is defined as the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data related to the incident.

Digital evidence is acquired when data or electronic devices are secured for examination. Inappropriate handling or examination of digital evidence can cause it to be altered, damaged, or destroyed, resulting in a reduction of evidentiary value. Because of its fragile nature, the destruction of digital evidence may occur through the following:

- user activities, either malicious or accidental
- hardware failures
- normal system activity (e.g., as in the case of automated log rotations).

The failure to properly handle or examine digital evidence can lead to inaccurate conclusions that result in erroneous determinations.

When properly performed, digital forensics can aide in determining the extent or depth of a compromise and may identify the tools and methods that were used to perform or conduct an attack. Forensics can also help external agencies identify the source of the attack and support efforts to protect other CBRN facilities from similar attacks. Forensics tools and techniques are also useful for many other types of tasks, including operational troubleshooting, log monitoring, and data recovery.

Digital forensics should be integrated into incident handling and response activities. Personnel performing or assisting in forensic tasks should to be trained in forensic methodologies and forensic tools,

techniques, and procedures. Forensic analysts should be knowledgeable and possess expertise in information security, operating systems, and the applications and databases used within critical systems.

Multiple models describe the digital forensic process. However, NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response* (NIST 2006) identifies the following basic phases that are common among all models.

- Collection. The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection typically is performed in a timely manner because of the likelihood of losing dynamic data such as current network connections, as well as losing data from battery-powered devices (e.g., cell phones).
- Examination. This phase involves forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest while preserving the integrity of the data.
- Analysis. This phase involves analyzing processed information using legally justifiable methods and techniques, to derive useful information that addresses the issues and occurrences being investigated.
- Reporting. The final phase is reporting the results of the analysis, which may include describing the actions used; explaining how tools and procedures were selected; determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls); and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process.

Sufficient digital forensics capabilities are need to adequately assess, determine, and support root cause investigations for information security incidents. Information security policies and procedures should adequately address the subject of forensic analysis.

When developing policies and procedures to address forensic activities a thorough review of the recommendations presented in following documents for applicability offer excellent references.

- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response* (NIST 2006)
- U.S. Department of Justice (2004), *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*
- U.S. Department of Justice (2008), *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*.

3.12 Recommendation: Information Security Awareness Training

The information security program implemented by CBRN facilities should ensure that facility personnel, including contractors, are aware of cyber and physical security requirements associated with their assigned duties and responsibilities. The training program should

- identify information security scope, goals, and objectives
- identify training staff and other resources to support awareness training

- identify target audiences and their appropriate levels of training
- provide training updates and enhancements to support a continued quality improvement objective
- periodically evaluate program effectiveness against program goals and objectives.

The following levels of information cybersecurity awareness and training should be provided:

- General information security awareness training for all staff members and contractors that provides understanding of
  - the site-specific information security programs' objectives, management expectations, programmatic authority, roles and responsibilities, policies, procedures, and consequences for noncompliance
  - information security threats (i.e., what constitutes a threat, how they work, how they are manifested, what are the typical consequences of threats)
  - general attack methodologies including social engineering techniques
  - appropriate and inappropriate information security practices
  - organizational contacts to report violations of information security policies, procedure, or practices.
- More in-depth training on applicable information security concepts and practices for personnel involved in the development, use, or storage of sensitive information design, and personnel information in the design, configuration, implementation, and administration of information systems, component digital assets, or networks. This training should cover
  - information security and engineering procedures, practices, and technologies, including implementation methods and design requirements, which apply to the assets encountered as part of the job
  - general information on information security vulnerabilities, potential consequences to systems and networks of successful attacks, and information security risk reduction methods
  - competency in the use of tools and techniques to physically and logically harden information systems and related digital assets to reduce vulnerabilities to cyber threat.
- Advanced cybersecurity training for individuals designated as information security specialists having responsibilities to protect information systems, related assets, and networks from information security threats, and who are directly involved with the design, acquisition, installation, operation, maintenance, or administration of technical security controls; or conduct information security assessments, audits, tests, and investigations. The training should provide advanced knowledge and competency in the areas of
  - data security
  - operating system security
  - application security
  - network security
  - access controls

- intrusion analysis
- incident management and response
- digital forensics
- penetration testing.

Advanced cybersecurity training should be conducted through recognized information security training programs. The information security program should contain requirements to review appropriate information security guidance documents. NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (NIST 1998) and NIST SP-50, *Building an Information Technology Security Awareness and Training Program* (NIST 2003) are examples of applicable documents when developing and implementing an information security training program.

3.13 Recommendation: Analyze and Select Security Controls

Secure information systems are the result of careful analyses that assess the existing security posture of the system, the environment in which it resides, the types of threats that exist, the capabilities of the threat agents to carry out an attack, and the vectors of attack that they might employ. This knowledge is essential to the development of strategic security objectives. These objectives should seek to eliminate or mitigate known points of vulnerability within the system. Appropriate security controls (sometimes called countermeasures) are then selected to interrupt the previously analyzed vectors of attack. Security controls should be combined as required to meet the identified strategic objectives. To ensure that the appropriate security controls are selected for a given situation, the following process is recommended (and depicted in Figure 3.6):

1. Analyze the System Environment and Assess Threat Information
2. Perform a Threat Vector Analysis
3. Develop Strategic Objectives
4. Select Security Controls.

Figure 3.6. Analyze and Select Security Controls

A brief description of each of these steps is provided in the following sections.

3.13.1 System Environment Analyses

The environment in which a system or component exists has a direct impact upon its security posture. Systems and components under development are likely to have considerably different security environments compared to deployed systems. As such, there may be substantial differences in the types of attack vectors that exist for various information systems. When evaluating security threats to information systems, consideration should be given to the environment in which the system resides. A vulnerability assessment should consider security issues arising from physical access as well as the digital connectivity between systems or networks including direct and indirect pathways of communication. Known vulnerabilities within the system should be identified.

3.13.2 Analyses of Threat, Threat Agents, and Attack Vectors

Analyses of postulated threats for a given information system should be made relative to the environment where it is located. The assessment should consider the various types of threat agents that might seek to conduct attacks against the technology. This includes a characterization of the capabilities of identified threat agents; their objectives; and the tools, tactics, and procedures they typically employ. It is helpful to understand the system's environment, connectivity, and vulnerabilities to potential attack vectors that could be used to compromise information assets. An attack vector analysis should describe the postulated threats and identify:

- potential vectors of attack
- the actions required to conduct the attack
- the postulated threat agents
- potential vectors of attack

- any actions required to conduct the attack
- areas of system vulnerability.

3.13.3 Development of Strategic Information Security Objectives

Strategic information security objectives should be developed and documented to address the elimination or mitigation of anticipated or identified vectors of attack. In cases where vectors of attack cannot be eliminated, security controls should be selected and applied to provide appropriate mitigation.

3.13.4 Selection of Security Controls

Following the development of security objectives, security controls should be selected to mitigate identified vectors of attack. The controls selected should be appropriate to the situation and be correctly applied. Insufficient or misapplied controls may result in a failure to meet documented strategic objectives, thereby resulting in an inadequate security posture.

The controls identified in NIST Special Publication 800-53 *Security Controls and Privacy Controls for Federal Information Systems and Organizations (*NIST 2013b) and NIST Special Publication 800-82 *Guide to Industrial Control Systems (ICS) Security* (NIST 2013a) provides a catalog of security controls that can be used to mitigate vulnerabilities. These management, operational, and technical security control categories (as introduced in Section 1.1) can be subdivided into "families" each of which contains a number of individual security controls. They are presented in the following list, and cover a broad range of security activities.

- Management controls:
  - Requirements Planning – developing and maintaining documented security requirements
  - Risk Assessment Planning – developing the policies and procedures for conducting risk assessments
  - System and Service Acquisition – developing policies and procedures for acquiring resources to implement an effective cybersecurity program
  - Certification, Accreditation, and Security Assessments – developing assessment methods to determine if security controls are being correctly implemented, are operated as intended and produce the desired outcome
- Operational controls:
  - Personnel Security – including security screening, behavioral observation, hiring, and penalties for security violations
  - Physical and Environmental Protection – including the protection of physical locations, access control and monitoring, tracking of people and assets, and environmental protection (i.e., safeguarding the operating and environmental infrastructure)
  - Contingency Planning – including the restoration of operations in the event of a cybersecurity incident or emergency

- Configuration Management – covering modifications to hardware, firmware, software, and documentation
- Maintenance – including routine and preventative maintenance, repairs, use of tools, and management of maintenance personnel
- System and Information Integrity – including design testing and approval, verification testing, intrusion detection and prevention, anti-virus and anti-malware screening, and security alerting
- Media Protection - limiting access to physical and electronic media, including labeling, storage, transport, sanitization, and disposal
- Incident Response - detecting, responding to, and limiting consequences, including training, testing, monitoring, and reporting
- Security Awareness and Training – including position-specific training, communication, and an awareness of social engineering threats

- Technical controls:
  - Identification and Authentication – including verifying the identity of a person, process, or device before permitting or denying further actions. This may involve passwords, challenge/response, physical tokens, and biometric authentication.
  - Access Control – including the management of computer accounts, separation of duties, least privilege, and session management. Specific policies and procedures should be defined for different technologies (e.g., modems, wireless connections).
  - Audit and Accountability – including the generation, review, and retention of records
  - System and Communication Protection – including encryption and the use of virtual private networks.

3.14 Recommendation: Perform Security Monitoring

While security controls that are used to impede the advance of a threat agent may be deployed with the intent of deterring, delaying, detecting, or denying an attack, few are capable of achieving complete nullification of a determined threat agent. Therefore, it is imperative that CBRN networks also be adequately monitored for anomalous behavior or activity that would suggest a potential breech in security has occurred.

3.14.1 Event Logging Systems

A robust cybersecurity program will include capabilities for the collection and analysis of indication and warning (I&W) data in order to detect and respond to intrusions. I&W data can be sourced from many different devices and applications in a networked environment. Common examples would include event and logging information originating from routers, firewalls, proxies, operating system security event logs, and application logs.

Event logging systems (syslog) are a key component within any network security architecture. The data deposited in these systems are often essential from a forensics perspective when attempting to

reconstruct a timeline of events when investigating a breech in system security. Although most security devices and applications have the capability to send event information to a centralized logging server (i.e., syslog) many of these sources of security monitoring data may use proprietary reporting formats or provide cryptic messages that are not easily discernable. Many modern syslog solutions in use today have the capability to "normalize" or translate these proprietary reporting formats easing the security analyst's burden of understanding the event data being reported. The level of effort needed to quickly determine the extent of a compromise can be greatly reduced through the use of logging systems that perform such normalization functions.

A challenge that exists with the logging of event data is the vast number of events that can be generated by syslog reporting. Depending upon the types of operating systems, the reporting agents involved, and the granularity of reporting, even a relatively small network of 20 nodes is quite capable of generating in excess of 50,000 events per day. Manual inspection of this number of events is well beyond the capabilities of even a small team of cyber analysts. To effectively monitor and respond to logged events, it is necessary to use an automated logging management system that is capable of analyzing events, prioritizing each event by severity, and elevating those events which can or should be acted upon in a timely fashion. These automated logging management systems generally also provide the capabilities to aggregate event data, search on stored data, derive baselines of analyzed activity, and produce reports. Typical reports from automated logging management systems include:

- number of syslog events categorized by severity
- Top-N syslog events / unit time
- Top-N devices generating events /unit time.

3.14.2 Security Logging and Event Manager

While syslog management solutions are helpful in the evaluation of I&W data, they are by no means sufficient as a sole indicator of compromise, since many other types of data are necessary for definitive analysis to occur. Such source of data include those originating from network intrusion detection and prevention systems (NIDS/NIPS), host intrusion detection and prevention systems (HIDS/HIPS), anti-virus systems (AV), file integrity systems, and others.

Although some of these sources may also have the capability of reporting to a syslog server, the syslog events generated will not necessarily contain the same level of detail that is present within the native management tools of a given security device or application. This can create a challenge for the cybersecurity analyst as it may be necessary to interrogate several different management systems (i.e., firewall, NIDS/HIDS, AV, syslog, etc.) to correlate enough data to establish an understanding of an evolving situation or incident.

To rectify this issue, a Security Incident and Event Manager (SIEM) application is often employed. In general, a SIEM is an integrated suite of security tools used to manage multiple security applications and devices. Most SIEM applications will have the capability to interpret or normalize the various I&W logging formats originating from disparate security devices and provide the ability to present a unified view of security across a network.

SIEM applications allow the cybersecurity analyst a holistic view into the relative state of security across network or enterprise. Some SIEM applications are capable of taking automated action in response to identified security incidents. In general, most SIEM management systems are capable of generating views and reports including:

- over threat level
- security events by sensor or data source
- security events by category
- reconnaissance or probing events
- attacks and exploits
- system compromise indicators
- top-N attack sources
- top-N attack targets
- top-N alarms
- top-N events
- top-N events by risk
- vulnerability analysis.

3.14.3 Other Issues

The use of automated applications requires attention and diligence to maximize their usefulness. It is recommended that:

- network hosts, SIEM, and syslog servers should be time-synchronized to an authoritative time server to ensure that events can be properly correlated
- monitored events be forwarded to a centralized security management network that is adequately hardened and segregated from the monitored networks by a firewall
- control interfaces to security devices employ out-of-band management, where possible
- encrypted tunnels be employed to protect the transmission of sensitive security event information and authentication credentials.

3.14.4 Human Interface

Although alerting mechanisms and SIEM applications can be used to identify and flag events of interest to cybersecurity personnel, ultimately human analysis is still required to evaluate and distinguish between false positive reporting and actual security events. Periodic examinations of the results being reported by the security monitoring system should be established.

Furthermore, it is essential that cybersecurity personnel receive adequate training in the detection and logging mechanisms used to process I&W data as well as basic incident response and handling procedures.

4.0 HIGH-VALUE SECURITY CONTROLS

If an organization lacks the time or resources to fully assess all risk before implementing controls, shortcut approaches will allow defense against the most common cyber-based threats to information security. This section discusses some approaches that may give your organization a shortcut or jump-start to cybersecurity.

Organizations have the ability to procure and install a wide range of management, operational, and technical security controls (including security standards, security checklists, vulnerability databases, configuration guidance, best practices, risk management tools, firewalls, intrusion detection and prevention systems, log management tools, and security training tools). The Council on Cybersecurity (the Council) reports that there is enormous set of "good things" that a facility organization can use to improve its security, "but not always clarity on what to prioritize" (Council on CyberSecurity 2014). The Council calls this situation the "Fog of More" [1]. The set of approaches provided in this section can be used to prioritize information security decisions—how to select cybersecurity-specific types of defenses that can allow risk-based, cost-effective decisions when enhancing an information security program.

4.1 The Top Four Strategies

The Australian Signals Directorate (ASD) has a developed a set of Top Four Strategies to mitigate the effects of cyberattacks that seek to gain access to information (ASD 2013). The ASD is widely cited by cybersecurity experts and organizations as providing leadership in the development of simple strategies that can provide reasonable protection from many, but not all, cyberattacks that have the potential to compromise information systems. These top four strategies do not cover the portion of information security that is related to protection from denial of service attacks, physical attacks, or infrastructure attacks. However, the top four strategies are designed to mitigate about 85 percent of the cyber intrusion techniques that are detected by the ASD's Cyber Security Operations Centre.

These cyber intrusions often masquerade as legitimate Internet traffic (e.g., web pages and emails). They attempt to work their way onto business or other facility or company workstations and then migrate to other system on which sensitive information can be accessed. This may include security workstations, digital control systems, key databases, and other high-value targets (ASD 2013). A key focus of the top four strategies is computer systems that use the Windows operating system. This is because Windows-based machines are the most widely used and are therefore the most commonly targeted. Whitelisting tools are available for other computing environments as well.

The top four strategies are:

1. Application Whitelisting
2. Application Patching

[1] A play on term of "fog of war" that is attributed to Carl von Clausewitz (1780 – 1831). The fog of war refers to the uncertainty of the capabilities and intent of combatants during battle. The "fog of more" a similar situation, in which those defending from cyberattack are uncertain of their adversaries' capabilities and intent and uncertain about how to select among the myriad defensive options and tools available to them.

3. Patching Operating Systems
4. Minimize Administrative Privileges.

Each of these strategies is briefly summarized the following sections.

4.1.1 Application Whitelisting

Application whitelisting can be an effective tool for preventing malware on protected systems. This tool blocks malware and unauthorized programs from running on digital system by only permitting the execution of known and permitted files. While more traditional systems attempt to identify and block malicious files, application whitelisting only permits the execution of approved applications. "Whitelisting flips the antivirus model from a 'default allow' to a 'default deny' for all executable files"(Beechey 2011).

The implementation of application whitelisting involves identifying specific programs that can be permitted to run on a digital system, preventing any other programs from running, and barring routine users from changing the list of programs that can be run. Application whitelisting uses a software program to identify and approve listed executable and library files, and access control lists to prevent unauthorized changes to the list of approved files (ASD 2012).

Productivity and cultural challenges are associated with application whitelisting. Users that are accustomed to having control over their own computers may not readily accept the limitations on their computing freedom imposed by applications whitelisting (Beechey 2011). Security concerns also exist if, for instance, a whitelist prevents users from downloading and installing a more recent patch to an existing application.

As a result, whitelisting may be restricted to only those computer systems or networks that contain sensitive information or perform critical or high-risk functions. As with most security tools, errors in implementation of a whitelisting solution can result in inadequate levels of protection. Proper planning throughout the life cycle of the whitelisting products are essential for the proper functioning of the technology (ASD 2013).

Some organizations transition toward application whitelisting by identifying entire directories from which users are allowed to execute any program (e.g., C:\Program Files, even C:\Program Files\Specific_Application). This provides some measure of protection from programs executing from different locations on the computer, but it does not take into account the potential for malware to install itself on whitelisted directories. This directory-centric approach is better than not making any move toward whitelisting, but it does not offer the production of true application whitelisting (ADS 2012).

Users have become accustomed to downloading and installing the applications that they need for their work. One alternative, therefore, is for organizations to develop their own form of applications store of marketplace-list-approved software for colleagues.

An array of commercial whitelisting tools are provided by software vendors for Windows and other operating system environments. These range from tools that are provided free with their operating system to commercial products. Users need to pick the application whitelisting product that best suits their needs and digital assets.

4.1.2 Application Patching

Applications are frequently targets of cyberattacks. Unpatched applications with identified vulnerabilities are attractive targets for attackers. Attackers often take advantage of vulnerabilities in applications to "gain a foothold on a network, which can be used to attack other systems" within a network facility. In this way, a cyberattack on a low-priority system can quickly spread through network connections to higher risk targets (ASD 2013). Application patches involve the installation of updated software or supporting information to enhance performance or improve the security of software or firm ware (operating systems are covered in Section 4.1.3). Application patches often address identified security vulnerabilities, errors, or performance issues in software or firmware.

Patch management is the process of determining what to patch, when updates should be made, who should perform this work, and what testing is needed. The aim is to ensure the patched software will continue to provide adequate support for a digital system and associated processes after updates have been made. Patch management may differ depending on the computer system involved. There are often more stringent requirements for patch management for OT systems than IT systems. IT systems can typically function with periodic downtimes for patch management and other maintenance. OT systems often have to maintain continuous operation for extended periods of time, making timely patch management more challenging.

For effective risk reduction, patch management should be conducted in as timely a manner as possible. This requires facility personnel to keep a current listing of all applications present on their systems and monitor the issuance of patches by their application developers. Complicating matters, few applications permit patches to be installed at the enterprise level; instead most require some form of direct human interaction. This can be time-consuming and result in significant delays in installing patches or the failure to install some patches.

For some digital systems, particularly in the OT realm, patch installation has to be delayed until it can be determined that the patches will not interfere with the appropriate operation of the digital system. For some systems, patches have to be tested by the vendor or the owner of dedicated testing equipment, which mimic the function of the operating system. Although some delays are unavoidable, the sooner application patches are installed, the sooner the vulnerability will be mitigated.

4.1.3 Operating System Patching

The operating system is an integrated set of software that manages computer resources and provides the computers services that applications use to perform their functions. The operating system is the core around which the entire computing environment is built. If the operating system is compromised, the actions of the computer and the information it stores may no longer be safe or secure (ASD 2013). The operating system also controls networked interaction providing gateways onto other connected systems or services.

Security vulnerabilities in operating systems are a frequent target for attackers. The more commonly used a program is—and operating systems are very widely used—the bigger target it is to attackers and the more likely it is that a vulnerability will be exploited.

The time between the discovery of an operating system vulnerability and the development and deployment of a malware exploitation can be quite short. Operating system developers release patches to their products on a periodic basis. In North America, Microsoft typically releases operating system patches on the second Tuesday of every month. There is an uptick in development of exploitations after the release of each patch, as attacks analyze the patch to develop malware to exploit computers on which the patch has not yet been implemented. As a result, while delay between the discovery of a vulnerability and the release of an operating system patch is a period of heightened security risk for information systems, the security risk increases for unpatched operating systems after the developer releases a security patch. As a result, it is important to support the timely implementation of operating system patches.

There are many tools available that are capable of providing patches to operating systems as well as monitoring and auditing their patch levels. Organizations should investigate operating system patching tools and procedures to find a system and procedure that meets the operational and security requirements of their systems (ASD 2013). However, in safety-related control systems this can create new challenges when verification and validation must be completed to ensure that any patch does not cause the system to crash, endangering the safety of an application process (Johnson 2014). As with application patching, some facilities, particularly those operating control systems, may need to use a test environment to ensure that an operating system patch will not introduce a decrease in the reliability or performance of current applications.

4.1.4 Minimize Administrative Privileges

Administrative privileges grant a level of control to trusted individuals who manage and monitor computer systems. Those with administrative privileges have the ability to make any and all changes to the computer system, including the ability to access, install, remove, or modify software and data. Administrative privileges are also used to perform functions that are necessary for the operation and security of information systems and networks (e.g., set access controls for users, access, and issue passwords). The malicious or inadvertent abuse of administrative privileges may pose significant consequences to information security; therefore, attackers seek administrative privilege access on systems they are trying to compromise (ASD 2013).

Legitimate system users often desire administrative privileges because it allows them to install and use software or data without delays or prohibitions. However, it also permits users to make changes to a system that can create security vulnerabilities; for instance it can become more difficult to identify who was responsible for the introduction of malware. By limiting administrative privileges to a smaller, more security-aware and well-trained set of computer professionals, information security risks can be reduced. Additional controls and limitation on those with administrative privileges can further reduce security risks. This may include:

- granting specific administrative privileges only to designated staff, rather than granting all administrative privileges to anyone needing any type of administrative control
- permitting administrative privileges only through the use of separate administrative accounts, which would be different from that individual's routine operating account
- removing external network access privileges (e.g., email, Internet access) from administrative accounts

- requiring separate usernames and passwords for different administrative privileges
- eliminating or severely curtailing administrative privileges via remote access.

To make minimizing administrative privileges less disruptive, organizations may choose to phase in the process. Exceptions may also be granted for applications or systems for which minimizing administrative privileges may represent an unacceptable burden. In such cases, other security controls can be implemented to offset the inability to minimize administrative privileges. To make the minimizing administrative privileges less burdensome on authorized system users, operating system developers are reducing the number and type of activities that require administrative privileges, thereby permitting lower-risk operations by authorized users while reserving higher-risk modifications for those with administrative privileges (ASD 2013).

4.2 The Critical Security Controls

The "The Critical Security Controls for Effective Cyber Defense" are a set of 20 security controls that are designed to address the latest advanced targeted threats and use approaches that have been shown to work in real-world applications. These top 20 controls are developed and are maintained by the Council on Cybersecurity (the Council), an "independent, expert, not-for-profit organization with a global scope committed to the security of the open Internet" (Council on CyberSecurity 2014).

The top 20 controls grew out of public-private efforts that began in 2008. They are regularly reviewed, updated, and validated by the Council. The controls represent a powerful tool for prioritizing information security activities by concentrating on a manageable number of key security controls that have high benefit-to-cost ratios and have demonstrated real-world effectiveness. Use of these controls within a comprehensive information security program is endorsed by a wide range of organizations, including governmental agencies and private consultants.

The Council lists five critical tenets for effective cybersecurity that are captured in the top 20 controls:

1. **Offense informs defense**. Use information about real-world attacks to create effective defenses.
2. **Prioritization**. Focus on implementing security controls that provide the greatest risk reduction and are readily implementable.
3. **Metrics**. Establish easy-to-understand measures of your security controls so that their effectiveness can be readily understood by decision makers and other members of the workforce.
4. **Continuous monitoring**. Conduct continuous security monitoring to test and validate the effectiveness of your security controls.
5. **Automation**. Automate defenses to allow for a rapid assessment and response to potential attacks.

The Council provides guidance, based on real-world feedback from users, on the steps that should be followed to implement their top 20 controls:

Step 1. Perform an initial security gap assessment to determine what security controls are in place and where gaps remain.

Step 2. Develop an implementation roadmap by selecting the specific controls (and sub-controls) that need to be implemented and schedule the various implementation phases based on risk considerations.

Step 3. Implement the initial or next phase of controls by identifying existing tools and their current utilization, new tools that are needed, processes that need to be implemented or improved, and training needs.

Step 4. Integrate security controls into operations by focusing on continuous monitoring, attack mitigation, and lifecycle security.

Step 5. Report and manage progress against the implementation roadmap developed in Step 2. Repeat Steps 3-5 for the next phases outlined in the implementation roadmap to maintain an ongoing process of information security assessment and improvement.

The top 20 security controls documented by the Council are listed as follows.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

These 20 security controls will be briefly summarized in Sections 4.2.1 – 4.2.20.

The 20 controls are compatible with the ASD Top Four Strategies (Section 3.1). The Council's top 20 controls include a set of sub-controls called "first five quick wins." These subcontrols are identified as having the most immediate and cost-effective impact on preventing a compromise of information security. These include the top four strategies provided by the ASD plus one new item— "using common, secure configurations."

This "fifth strategy" involves using secure, hardened versions of operating systems and applications. These hardened systems will restrict certain activities/access control and will also provide additional tools for intrusion detection and monitoring by enhanced log generation. The versions need to be kept current and validated as operating systems and applications are updated to address security vulnerabilities.

The 20 top security controls are also compatible with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST 2013b) and other security approaches that have been mapped by SANS and the Council on Cybersecurity and are available from https://www.sans.org/media/critical-security-controls/fall-2014-poster.pdf. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards have been mapped into the top 20 security controls (The SANS Institute and the Anfield Group 2014) and are available from https://www.sans.org/media/critical-security-controls/nerc-cip-mapping-sans20-csc.pdf. The Critical Security Controls complement ongoing work in security standards and best practices such as:

- the Security Content Automation Program (SCAP) (NIST 2014c)
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* (NIST 2013b)
- the Australian Signals Directorate's "Top 35 Strategies to Mitigate Targeted Cyber Intrusions" (ASD 2014)
- the ISO/International Electrotechnical Commission (IEC) 27002:2013 Information technology — Security techniques — Code of practice for information security controls (ISO/IEC 2013).

4.2.1 Inventory of Authorized and Unauthorized Devices

This security control involves actively managing (inventory, track, and correct) all network-enabled devices so that only authorized devices are given access to the network, and unauthorized and unmanaged devices are found and prevented from gaining access.

4.2.1.1 What Is This?

Keeping a physical inventory of the organization's equipment is a well-established practice to detect and deter loss or theft. This inventory can be taken one step further into the realm of digital communications to identify which equipment is allowed access to specific networks. Knowing what equipment is actually on your computer network is key to understanding what equipment is authorized to have access and what equipment does not belong on the network. By maintaining an official inventory of network authorized equipment, it becomes possible to identify the presence of unauthorized devices and to take appropriate protective actions to either halt that unauthorized access or add that device to your list of authorized equipment.

At a minimum, all organizational assets should be inventoried annually, with ownership identification tags affixed to all equipment. Many organizations do annual physical inventories as part of their financial accounting processes. An annual inventory should identify, the characteristics of the equipment itself and the owner and other points of contact (e.g., financial responsibility and technical responsibility). The inventory should list when the equipment was put into service and record equipment as it is retired and removed from the network. For IT systems, information related to care and configuration, such as hardware, software, and system administration points of contact are also valuable.

4.2.1.2 Why Do This?

Cyberattackers can gain a foothold by looking for systems that are not being maintained or have been added to the network recently but are not yet properly configured. An inventory of authorized devices helps ensure that each device on the network belongs to a person or organization, has a business reason to be there, and is being properly maintained. Systems not being well maintained can become infected with malware, which in turn can put an entire organization's network at risk.

Through this process of referring to an organization's inventory, newly detected networked devices can be quickly identified and then authorized or blocked. If unauthorized, they can be removed from the network, which will in turn reduce the chances that a facility could be compromised or attacked through the use of that unauthorized equipment or connection. However, it is also possible to create denial of service attacks that mimic connection requests across a network—each of which then has to be notified to the security staff. There are further overheads in maintaining lists of authorized devices, especially when senior staff often want to permit "bring your own device" policies for phones and tablets.

4.2.1.3 A Question for Your Organization

Once new equipment is detected on the organization's network, how quickly can it be determined if the equipment is authorized or unauthorized?

Obviously, the more current and accessible an inventory and the more frequent the process of checking the network for unauthorized devices, the more efficient will be the identification and elimination of unauthorized devices. Rather than rely on an annual physical inventory, some organizations do continuous asset tracking via their network and compare it to known authorized equipment. This approach can greatly reduce the chances of malware outbreaks by quickly identifying unauthorized equipment and quarantining or removing until authorization can be obtained.

4.2.2 Inventory of Authorized and Unauthorized Software

4.2.2.1 What Is This?

To effectively apply the limited resources available, organizations should actively manage (inventory, track, and correct) all software on a system so that only authorized software is installed, maintained, and executed. Unauthorized or unmanaged software should be found and prevented from installation or execution. Controlling the software authorized for installation enables an organization to detect malicious software more quickly.

4.2.2.2 Why Do This?

Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets. Poorly controlled machines are more likely to be either running software that is unneeded for business purposes, introducing potential security flaws, or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many.

4.2.2.3 Questions for Your Organization

How long does it take to detect new software installed on systems in the organization?

How long does it take the scanners to alert the organization's administrators that an unauthorized software application is on a system?

If there is a vulnerability discovered on a software product, can you quickly identify the digital devices that contain that software?

The speed at which new or unauthorized software is detected can be a key factor in identifying and preventing a breach of information security. Similarly, knowing where software products are located can speed up the identification and elimination of known vulnerabilities. This too can decrease the likelihood of a successful cyberattack. Would you apply these policies across all of the systems or only in areas of greatest risk?

4.2.3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

4.2.3.1 What Is This?

Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. Having a consistent configuration of hardware and software on systems, one that fits the organizations needs and outcomes is important for reducing unnecessary work for staff members and ensuring they have the tools they need to get their work done. As part of the organization's IT life cycle, the configuration should be kept as close to the current versions of hardware and software as is feasible. Hardware and software configurations should be approved by organization and management should strongly encourage all staff members to use this standard configuration for their work. There will always be cases where staff members need a special configuration for their project or assignment, but having a consistent set of approved software allowed to be installed on a standard hardware configuration will save the organization both time and money.

4.2.3.2 Why Do This?

As delivered by manufacturers and resellers, the default configurations for operating systems and applications are normally geared to ease-of-deployment and ease-of-use. They are not typically configured for security, and as such they may be vulnerable. Having just a few approved hardware options for devices such as mobile devices, laptops, workstations, and servers allows the organization to purchase systems in larger quantities, reducing costs per unit. The same is true for software, having an approved list of software available to staff members allows for large purchases rather than purchasing small quantities or one at a time, which typically results in higher costs per unit.

For example, if the organization identifies a specific brand of word processing software, including specific versions and requires everyone to use this same brand and version, company-wide purchases can be made and distributed to staff members. If staff members are allowed to choose any brand they like and make individual purchases, the cost goes up dramatically. Likewise the time that staff members would spend converting their documents between brands or troubleshooting compatibility issues can result in many hours per person—time better spent on assigned tasks. Another benefit of keeping all staff members at the same versions is that the supporting only a few brands and versions, greatly reduces the attack surface of an adversary. The organization can focus on maintaining and protecting systems with known configurations, allowing a proactive approach rather than reacting to threats that the organization may not be aware exist in their infrastructure.

4.2.3.3 Question for Your Organization

How long does it take to detect configuration changes to a network system?

Ideally, hardware and software configurations are monitored digitally so that the organization knows current configurations, including which are current and which require updates. If that cannot be done, then as part of asset tracking, hardware and software could also be audited and tracked. Being able to refer to the most recent inventory and search to find changes since the last update using an automated process to detect changes to an organization's systems may be the difference between suffering an internal attack and being able to stop it before it spreads across all the networked systems.

4.2.4 Continuous Vulnerability Assessment and Remediation

4.2.4.1 What Is This?

Information security is not a one-time project, but must be treated as a continuous effort to defend an organization's assets. Cyber defenders must continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. Software tools can also compare vulnerability scan results over time, to enable trend analysis.

4.2.4.2 Why Do This?

Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significantly increased likelihood of having their computer systems compromised. Attackers have access to the same information, and can take advantage of gaps between the appearance of new knowledge and

remediation. For example, when new vulnerabilities are reported by researchers, a race starts among all parties, including: attackers (to weaponize—deploy an attack, and exploit); vendors (to develop and deploy patches or signatures and updates), and defenders (to assess risk, regression-test patches, and install).

4.2.4.3 Questions for Your Organization

How often do you run internal and external scans?

How long on average after identification does it take for vulnerability remediation or mitigation activities steps to be completed?

How long does it take, on average, to completely deploy operating system software updates to key information systems?

The speed at which vulnerabilities are identified and addressed is a key factor in reducing information security risks. The longer vulnerabilities go undetected and the longer it takes to eliminate or compensate for the vulnerability, the greater are your information security risks.

4.2.5 Malware Defenses

4.2.5.1 What Is This?

The purpose of malware defenses is to control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action. The use of anti-malware software is key to preventing the spread of viruses, Trojans, worms, and ransomware across organizational systems. Anti-malware software does not need to be expensive to work, in fact there are several low-cost or even free versions available.

4.2.5.2 Why Do This?

Malicious software is an integral and dangerous aspect of Internet threats, and can be designed to attack your systems, devices, or your data. Making anti-malware software part of your organization's standard configuration, required for all systems, is key to preventing loss of data such as intellectual property, trade secrets, financial information, or organization strategy. However, anti-malware software is only one part of a security management system.

Ensuring that systems are protected prevents unintentional information leakage, loss, or theft. The number of person-hours to recreate lost data can be staggering, depending on the project. In some cases it may be impossible to recreate lost data. For example, an experiment that is very complicated to run or relies on rare occurrences may be impossible to redo if the data were lost. If the integrity of information or systems across the organization was compromised because of malware, the number of person-hours to rebuild all the systems and restore them to their last known "good" state could take months.

Most organizations do not allocate funds for a large malware outbreak, and dealing with a malware outbreak means taking resources away from productive work. However, taking preventive action and having anti-malware software in place before an event occurs can save money and time in the long run.

4.2.5.3 Questions for Your Organization

How long does it take the system to identify any malicious software that is installed, attempted to be installed, executed, or attempted to be executed on a computer system?

How frequently are malware definitions updated?

Many organization wide anti-malware software installations provide high-level metrics on such things as versions installed, malware blocked, and also immediate notification of malware detected and spreading. Real-time monitoring of this information is key to detecting malware trends that may be emerging within the organization and how best to mitigate them. Of course, malware detection depends on the completeness of malware definitions. Delays in updating definitions can reduce the effectiveness of malware detection systems.

4.2.6 Application Software Security

4.2.6.1 What Is This?

The purpose of application software security is to manage the security life cycle of all software, whether developed in-house or acquired, in order to prevent, detect, and correct security weaknesses. The security of applications is a complex activity encompassing management, operational, and technical security controls. These controls may be specified in formal cybersecurity risk management frameworks or in the information security program.

4.2.6.2 Why Do This?

Attacks often take advantage of vulnerabilities found in application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions.

In just one attack, a vulnerability in widely used application compromised a million websites, including, trusted websites from government agencies and large corporations. The compromised websites were used to transfer malware to website users. Poor application software security is a large and ongoing problem.

4.2.6.3 Questions for Your Organization

Can the application system detect attacks and block in a timely manner?

Are all Internet-facing applications scanned by web application vulnerability scanners on a regular and ongoing basis?

Various tools exist to detect application security issues and block potential attacks.

4.2.7 Wireless Device Control

4.2.7.1 What Is This?

The purpose of wireless device control is to monitor, prevent, and restrict the use of wireless local area networks (LANs), access points, and wireless client systems. Wireless networks have "cut the cord" for organizations— no longer must systems rely on a wall outlet to plug in their system's network cable in order to have digital communications. The ability to wirelessly network systems can save organizations a lot of money. In the past networked systems required trenches to be dug, conduit to be installed, and cables run. Digging in the wrong place could break the conduit, quickly bringing the network down, and the organization may need to wait hours, days or weeks to get it repaired and restored. Wireless alleviates many of these problems for a greatly reduced cost. However, wireless communications introduces a new pathway for cyberattack—allowing anyone with a commercial-off-the-shelf (COTS) antenna to eavesdrop on wireless communications and attempt to access wireless connection points. This can substantially increase cybersecurity risks. In the CBRN field, there are initial attempts to secure Supervisory Control and Data Acquisition (SCADA) protocols, including wireless versions of Highway Addressable Remote Transducer (HART) to link smart sensors/controllers. Significant questions remain about the associated risks.

4.2.7.2 Why Do This?

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation via rogue wireless access points during air travel or in cyber cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization.

Unlike physical cables that the organization can control, wireless travels through the air unseen, and if not protected well, can be accessed by those without the organization's knowledge or consent, which puts the entire organization's information security at risk.

Wireless signals do not travel in a set or constant pattern and can fluctuate and overlap with signals of other organizations. Ensuring that a wireless network is protected from unauthorized access is important for reducing information security risks.

4.2.7.3 A Question for Your Organization

Are systems capable of identifying unauthorized wireless devices or configurations when they are within range of the organization's systems or connected to their networks?

Similar to the asset tracking done as part of inventory, knowing what wireless devices are expected on the network is important. These devices are allowed if they follow the organization's approved configuration for hardware and software. The user of the wireless device must also be approved and trusted with the key information needed to connect to the network. At a minimum, the wireless network should employ an appropriate method of encryption.

4.2.8 Data Recovery Capability

4.2.8.1 What Is This?

The purpose of having a data recovery capability is to provide a way to quickly recover or restore information if it is compromised. Nonexistent or unreliable backups are a common problem for many organizations. Even worse, organizations may believe they have effective backups only to find out the process is not working when the organization needs to recover sensitive information. Security managers should ensure that each information system is automatically backed up on a regular basis (e.g., daily, or weekly or more often for systems storing sensitive information). To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. However, the restoration process has to be carefully controlled for two reasons. First, the restored system may become infected—hence malware may be archived and continue to infect a network after the rollback. Second, these archives are essential resources for forensic analysis—to identify the source and extent of an attack and also to sustain any subsequent legal action.

4.2.8.2 Why Do This?

When attackers compromise information systems, they can make significant changes to system configurations, software, and data. When an attack is discovered, it is important to be able to restart systems from a known safe configuration—preferably one as close to the start of the attack as possible to minimize the loss of newer information. Performing a restart prior to the start of the attack is important to obtain a trustworthy data recovery capability that predates any presence of the attack on the system. However, as mentioned above, it can be hard to determine an appropriate starting point without also reinstalling the vulnerabilities that were already exploited by the existing attack.

4.2.8.3 Questions for Your Organization

Are all your information systems backed up on a regular basis?

How frequently are the backups recovered?

All older versions of the backup retained so that you can be sure of finding a back-up versions that pre-dates the successful attack?

A data recovery capability does not defend a system against cyberattack, but can reduce the consequence, and therefore the information security risks.

4.2.9 Security Skills Assessment and Appropriate Training to Fill Gaps

4.2.9.1 What Is This?

The purpose of security awareness training is to provide CBRN facility personnel with the skills needed to minimize information security risks. The first part of this control is to assess the current level of information security knowledge. This is used to identify knowledge gaps between what personnel do know and put into practice, and what the organization is targeting for information security practices. Knowledge of gaps is used to enhance information security design training to fill those gaps. Many organizations find it appropriate and efficient to incorporate information security with cybersecurity and physical security training because so many elements of security awareness are common to these security topics.

Information security training is needed for all functional roles in the organization—for general personnel, information system and sensitive information users and program managers, and information security specialists. This training also should be provided to vendors, contractors, corporate staff, and regulators who have a legitimate need to access the facility's information systems or sensitive information.

Information security refresher training also has to be repeated at periodic intervals to address emerging threats, technology changes, security enhancements, and consequence changes. Awareness exercises and tools are effective tools for evaluating the effectiveness of training and reinforce key lessons.

4.2.9.2 Why Do This?

Information security training is an essential part of an information security program. The best technical security controls can rendered ineffective by lapses in information security by facility staff. Empowering personnel with elevated information security awareness and adherence to information security policies can substantially reduce information security risks.

All people involved in CBRN facility activities need a basic level of information security training to avoid inadvertent actions that could increase security risks. More detailed training is needed for those with authorized access to information systems and sensitive information. Information security specialists need the highest level of training to avoid actions that could compromise information security and to understand what protective actions are needed to respond to an information security attack.

4.2.9.3 Questions for Your Organization

Is information security training provided to all CBRN facility staff?

Is the training provided appropriate for each person's level of access to information and information systems?

Are information security training records monitored to ensure that training requirements are current for all personnel?

By ensuring personnel are assigned position-appropriate information security training and tracking participation in the training, an organization can enhance its overall information security awareness and that should reduce information security risks.

4.2.10 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

4.2.10.1 What Is This?

The purpose of secure configurations for network devices is to deter, delay, detect, deny attackers who are attempting to exploit information security systems. This activity involves establishing, implementing, and actively managing the security configuration of network infrastructure devices using a rigorous configuration management and change control process.

4.2.10.2 Why Do This?

As delivered from manufacturers and resellers, the default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use. Open services and ports, default accounts (including service accounts) or passwords, support for older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state. Security-based reconfigurations are required to reduce security risks.

4.2.10.3 Questions for Your Organization

Is the security configuration of network devices reviewed and appropriately reset, as needed, prior to the network device becoming operational?

How long does it take to detect configuration changes to a network system?

Are the volatile memory devices in network equipment erased during decommissioning to avoid the inadvertent distribution of secure information at the end of the lifecycle?

Implementing secure device configurations that are actively managed and controlled, rather than left with factory default settings, reduces the risk of compromise of both the network devices and the rest of the network.

4.2.11 Limitation and Control of Network Ports, Protocols, and Services

4.2.11.1 What Is This?

The purpose of security tightening of network ports, protocols, and services is to minimize the number of vulnerabilities that attackers could attempt to exploit. This activity involves managing the ports, protocols, and services on networked devices. Categories or services of network use should be pre-defined and limited by an organization's security policy. These use policies will dictate which services are allowed to run on the organizational network.

For example, if keeping up on news and current events, watching online videos is part of the organization's focus, then allowing staff members to access video clips would be part of their regular business. If on the other hand, there is no business reason for staff members to view online videos on company time, this ability might be blocked during core business hours or all the time. An organization may go even further and allow or restrict specific sites. Network administrators should have the tools needed to monitor the organization's network continually so they know what online content or sites are being visited and then based on use, determine if services need to be added or removed. Staff members need to be notified of these policies and monitoring activities so that they understand the reasons why the policies are in place and that the staff members are expected to follow the policies—otherwise, staff members may be tempted to find workarounds that undermine security controls, such as creating their own *ad hoc* or peer-to-peer networks.

4.2.11.2 Why Do This?

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and domain name system (DNS) servers installed by default on a variety of different device types, often without a business need for the given service.

Web sites can be a source of malicious content. Unfortunately, simply by visiting the site and clicking on links, the user has given the site "permission" to share content (e.g., targeted ads), gather information about the user (e.g., identify their network), and send content back to the user, which may include malware. The first line of defense in protecting the organization's network and systems from malicious content from the Internet is by using organizational-level firewalls and web blocking, often referred to as web proxy, as well as host-based firewalls. Securely configuring network devices will stop some attempts to gain malicious access and reduce information security risks.

4.2.11.3 Questions for Your Organization

Does your organization's security program require secure configurations of network devices?

Are the security configurations of network devices part of a review process (either comprehensive or involving spot checks) by security personnel?

How long does it take to identify any new unauthorized listening network ports that are installed on network systems?

Investing in organizational-level network tools referred to as Security Information and Event Management (SIEM) systems gives the network administrator a holistic view into the network and its current alert state, similar to defense condition (DEFCON). Having this information at their fingertips gives network administrators the ability to know very quickly if the system is not functioning as expected, and if any new unauthorized listening network ports have been installed.

Unfortunately, good network hardware and software can be expensive. There are open-source or free versions of network protection software. None of the current products on the market are easy to use and should not be used by inexperienced personnel. All require learning the product and regular interaction

with it to understand what is normal and what is abnormal behavior for the organization's environment, as no two organizations function exactly the same way.

4.2.12 Controlled Use of Administrative Privileges

4.2.12.1 What Is This?

The purpose of controlling administrative privileges is to restrict the ability of attackers to use administrative privileges to gain a foothold on, or spread their attacks through, an organization's networks. Attackers seek to gain administrative privileges on computer systems they compromise, as those privileges grant the highest level of access to a system. Security managers should limit the use of administrative privileges (as described in Section 4.1.4). The most effective way to protect them is by using processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

4.2.12.2 Why Do This?

The misuse of administrative privileges is a key tool that attackers use to spread inside a target organization. As a result, attacks compromising administrative credentials can be the most damaging and the most expensive to eradicate.

4.2.12.3 Questions for Your Organization

Is there an organizational policy to limit administrative privileges on information systems?

Is monitoring conducted on information systems to log and report on the activities of those who have administrative accounts?

How long does it take for system administrators to be notified about user accounts being added to super user groups?

Given the high risk and expense of eradicating attacks that compromise administrative privileges, use of processes and tools to manage the organization's administrative privileges on computers, networks, and applications is a critical component of an effective cybersecurity program.

4.2.13 Boundary Defense

4.2.13.1 What Is This?

The purpose of boundary defenses is to restrict communications between information systems and networks at different trust levels. Just as CBRN facilities have multiple physical security zones (e.g., the publicly accessible zone, limited-access zone, and restricted-access zone) with increasing security and access restrictions around high-value assets, so should these organization have comparable zones for electronic access. For both, physical security zones—barriers such as locked doors, gates, and access control stations—restrict access to authorized individuals. For electronic security zones, digital barriers such as firewalls, and log-in screens restrict access to authorized individuals. For example, visitors with

wireless devices should not be allowed on the same range of internal networks as facility staff members. Furthermore, members of the payroll department should not have the same access to CBRN materials inventory information as do members of the security organization. As a result, an electronic boundary is needed between the plant business network and the network that contains CBRN materials information.

Network security administrators should work with facility decision makers to understand the information requirements of each facility department. In turn, they can determine how best to separate or segment the organization's information networks to allow personnel access to the information they need to do their work, while restricting access to sensitive information and information systems that they do not need to access.

4.2.13.2 Why Do This?

Attackers focus on exploiting systems that they can reach. Security boundaries and other boundary defenses act to restrict access to information and information systems that are not intended for use by others. Threat agents use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain access to an organization's computer networks. Multiple layers of boundary defenses serve to deter, delay, detect, and deny access to unauthorized individuals.

Creating network boundaries is key to segmenting the network and protecting systems from unauthorized use. Once network administrators understand the various departments and uses of the network for reaching various resources, they can best divide up the network and ensure that important network-based resources are available to those who need them. Once the rules of the network are established, they need to be reviewed regularly to ensure that the organization's structure or business need has not changed and that cybersecurity's roles have not changed, which would require adding or removing network segments. In addition to the SIEM system, having network and host-based intrusion detection systems (IDS) greatly help the network administrator maintain the configuration designed and ensure it functions as expected.

4.2.13.3 Questions for Your Organization

Does your facility use multiple boundary defenses to separate publicly accessible access zones from zones containing sensitive information and information systems?

Do all network connections to the Internet, business partners, or other third parties currently use inbound and outbound network filters, and intrusion detection systems?

Having multiple layers of boundary defenses that use inbound and outbound network filters, and IDS helps the facility limit information security risks. Boundary defenses prevent attackers with malicious intent and staff members with benign intents, from circumventing the network structure and accessing information and information systems that they should not access. Boundary defenses should be designed so that they can be modified as needed to meet evolving security threats and incorporate enhanced technologies.

4.2.14 Maintenance, Monitoring, and Analysis of Audit Logs

4.2.14.1 What Is This?

The purpose for reviewing and assessing audit logs is to help detect, understand, or recover from an attack. The collection, management, and analysis of audit logs is an important tool for detecting attacks and also for identifying appropriate recovery actions. Early detection can allow personnel to take steps to stop an attack before adverse consequences are experienced. Audit logs can also help characterize an attack, and this information can be used to decrease the time needed to recover from an attack. Many organizations gather log data, but do not analyze them or analyze them too infrequently to do much good. Effective and timely log management often involves the use of a specialized log-management tool. Time and skill are required to efficiently use most log-management tools. The skill comes into play in a number of ways, including fine-tuning the tool to minimize the number of false alarms without compromising security. Skill is often acquired as experience is gained using the tool operationally. In addition to the security benefits, tools of this nature are used by system administrators to diagnose routine problems. This dual benefit typically makes investing in a log-management system and process highly effective from a cost-benefit perspective.

4.2.14.2 Why Do This?

Deficiencies in security logging and analysis allow attackers to perform ongoing attacks without the threat of detection. Given enough time to operate without detection, many attackers can eventually find and apply a hacking tool that will break through a system's defenses. Even after systems have been compromised, without protected and complete logging records, victims are often blind to the details of the attack and to subsequent actions taken by the attackers.

Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes, but rarely look at the audit logs, so they do not know that their systems have been compromised. Because of poor or nonexistent log-analysis processes, attackers sometimes control victim machines for months or years, stealing and manipulating sensitive information without anyone in the target organization detecting evidence of the attack in unexamined log files.

4.2.14.3 Questions for Your Organization

Does the facility use a log management system?

Does it cover all pathways into sensitive information systems?

Are logs analyzed on a regular basis?

With what frequency are logs analyzed?

Are logs provided to a central log management system?

If a system fails to log properly, how long would it take for security personnel to receive the alert about this failure?

A centralized logging system allows logs from multiple systems and devices to be aggregated and analyzed in a centralized location where personnel may have in-depth log-management expertise. The use of centralized logging system can speed up the examination and assessment of logs.

4.2.15 Controlled Access Based on the Need to Know

4.2.15.1 What Is This?

The purpose of controlling access based upon the "need to know" is to restrict the number of individuals that can access sensitive information and information systems. The process begins with the formal determination of which persons, computers, and applications have a need and right to access information. A formal access control policy may be used to specify the criteria used to grant physical and electronic access privileges. Classifying information in a systematic manner allows system administrators to develop digital rules for protection. Information security personnel, often working in conjunction with system administrators, can develop access rules based on roles within an organization and the need of individual personnel to access information. These rules can be set at the organizational, department, network, or device level.

4.2.15.2 Why Do This?

Some organizations carefully identify and separate their sensitive information and information systems from nonsensitive (e.g., publicly disclosed) information on their internal networks. Just this segregation can reduce information security risks. Allowing access to sensitive information or information systems to all internal users can substantially increase information security risks. When sensitive information is used by controls systems that provide SCADA, insufficient access restrictions can compromise the function of those control systems. A key concern here will be the role of subcontractors in the installation, maintenance, and operation of network components.

In designing an organization's information security system, it is important to consider the roles and responsibilities assigned to each group or department. System administrators can map those organizational rules to digital gates and locks, as well as log monitoring systems, and alert if anyone tries to inappropriately access or tamper with sensitive information.

4.2.15.3 Questions for Your Organization

Does your organization have need-to-know access requirements on all of its information systems?

Are access requirements periodically reviewed and kept up to date?

Does your organization monitor and respond to attempts by to access information without the appropriate privileges?

Most modern operating systems allow setting rules about who should be able to access information in designated groupings (e.g., folders and directories). Operating systems can also be set to track both successful and unsuccessful access attempts. It is also important to audit and review access rules regularly as these may evolve rapidly.

4.2.16 Account Monitoring and Control

4.2.16.1 What Is This?

The purpose of account monitoring and control is to ensure that accounts on information systems are provided only to users with valid and current authorizations. Account monitoring reviews should be conducted at least annually if not more frequently. These reviews should look for idle accounts or accounts providing access to staff members who have transferred to different assignments, or left the organization entirely. Disgruntled former staff members can use old credentials to access information systems and cause the organization harm. Security organizations must actively manage the life cycle of system and application accounts— their creation, use, dormancy, deletion—in order to minimize opportunities for attackers to leverage them.

4.2.16.2 Why Do This?

Attackers could discover and exploit legitimate but inactive user accounts in order to impersonate legitimate users, thereby making it difficult for security personnel to discover an attack. The systems accounts of contractors, staff members who have transferred to other organizations, and staff members who have been terminated may be exploited in this way. Some malicious insiders or former staff members can access accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.

4.2.16.3 Questions for Your Organization

How often does your organization review the access credentials for all of its authorized users?

Does the system audit and report on valid and invalid log-ins to user accounts?

How are accounts managed when users or administrators change roles or leave the business?

Regular review and auditing of accounts assures that only current users with an identified need have access to organizational systems. This greatly reduces the opportunity for attackers to gain access via inactive accounts.

4.2.17 Data Loss Prevention

4.2.17.1 What Is This?

Data loss prevention prevents the data exfiltration of sensitive information, mitigates the effects of data loss, and ensures the privacy and integrity of sensitive information. Data loss or leak prevention is designed to detect a potential information security breach, block information exfiltration (i.e., the clandestine removal of data from the control of its rightful owners), and prevent information loss by monitoring, detecting, and blocking access to sensitive information while in use, in motion, and at rest. In data leakage incidents, sensitive data are disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. Similar to the approach discussed in Section 4.2.15, digital watermarks can be used

both to help authenticate and also to trace the distribution of digital copies and thereby help determine the chain of disclosure.

4.2.17.2 Why Do This?

An organization's sensitive information can exist in many forms. Protection of information is achieved through the application of a combination of encryption, integrity protection, and data loss prevention techniques. Information may be inappropriately disclosed via intentional or unintentional actions. Unintentional sharing can be as simple as mentioning a new project at a community event or by posting news of your latest project assignment to a social media site. Information that is inappropriately disclosed cannot be called back, and once released the task becomes one of mitigation and damage control.

It is important that rules and processes be put into place to protect sensitive information. It is also important that staff members understand how to protect information properly, through regular training and management direction. Staff members also need to work in a climate that encourages asking questions before acting, without fear of penalty. By nature, most people want to help, and sharing information to enable others to get their work done is a way to do that. The key is having protections in place to prevent unintentional information disclosures and to make it easy for staff members to handle data appropriately.

The challenge of data loss prevention is increasing as new technologies, such as cloud computing and cloud data storage, become more prevalent and cost effective. It is that when dealing with these new technologies, proper care is taken to limit the risk of information disclosure, track data exfiltration, and mitigate the effects of data compromise.

4.2.17.3 Questions for Your Organization

Does your organization have an active data loss prevention program?

Does the system identify and report on unauthorized data being exfiltrated, whether via network file transfers or removable media?

Are staff trained to support data loss prevention efforts?

Facility staff members learn how to handle data in a secure manner through regular training and education. If a mistake does occur, knowing they can self-report without retribution is key. Identifying such issues quickly may allow remediation to occur quickly and reduce the consequences for the organization.

4.2.18 Incident Response and Management

4.2.18.1 What Is This?

The purpose of incident response and management is to efficiently respond to an information security event and take steps to reduce the consequences of the event. Incident response and management

involves the detection of an information security event, the timely investigation and characterization of the event, the execution of responses to reduce the adverse consequences of the event, the rapid recovery from the event, and the incorporation of lessons learned to reduce future information security risks. Information security incident response and management are specialized forms of incident management, and to operate efficiently they need to be integrated with other incident response and management programs—particularly those involving cyber and physical security.

The efficiency and effectiveness of an information security incident response and management program can drastically reduce an organization's information security risks by reducing the consequences of an information security event and by identifying lessons learned that can lessen the likelihood of future events.

Present generations of malware will compress files and embed them within legitimate files including JPEG images. These files can still be used as normal—for instance viewed and attached to emails. Malware will send the files to an email account so that attackers can then retrieve the content at a later date. They can also be forwarded via anonymous servers that disguise the original source of the compromised information.

4.2.18.2 Why Do This?

Even large, well-funded, and technically sophisticated enterprises struggle to keep up with the frequency and complexity of information security events. When an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover from the event. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attack may have a far greater impact, causing more damage, infecting more systems, and possibly exfiltrate more sensitive information than would otherwise be possible were an effective incident response plan in place.

4.2.18.3 Questions for Your Organization

Do you have an incident response and management program in place?

Are incident response and management procedures documented and available for use during an information security event?

Is your information security incident response and management program integrated with comparable cybersecurity and physical security programs?

Is incident response practiced through the use of drilling and other training techniques?

What kind of trend analysis is performed on past cyber incidents so that security controls can be improved in the future?

Incident response and management policies, procedures, and personnel need to be available and ready whenever an information security event is detected. Incident response personnel need to have sufficient skill and practice to perform their duties in a timely manner.

4.2.19 Secure Network Engineering

4.2.19.1 What Is This?

The purpose of secure network engineering is to make information security an inherent attribute of the enterprise by specifying, designing, and building in features that allow operations while minimizing opportunities for attackers. Secure network engineering is a life cycle process. Tacking on security features after a network is designed can reduce risk, but a more effective (and cost-effective) approach is to design a network with security in mind. This includes incorporating a defensive architecture within the network design. This might include the use of demilitarized zones (DMZs) that provide a separate security level that prevents direct communication between sensitive and less-sensitive systems or networks, appropriate security segmentation, and limited visibility of internal servers and systems.

To maintain network security, it is important to protect all information about the organization's network structure and to only allow its disclosure as part of a carefully monitored, need-to-know basis.

4.2.19.2 Why Do This?

Designing networks with information security in mind can substantially reduce risks and reduce life cycle security costs. The costs of retrofitting security into systems and networks are much greater than the costs of a secure network design and implementation.

To help ensure a consistent, defensible information security network, the architecture of each network should be based on a template that describes the network's overall layout and the services it provides. Organizations should prepare diagrams for each of their networks that show network components such as routers, firewalls, and switches, along with significant servers and groups of client machines. Visual inspections should be conducted to ensure that the network configuration as-built (and as-operating) is consistent with network documentation. Knowing what currently exists on the network helps allow changes without negatively affecting the organization's ability to do work.

4.2.19.3 Questions for Your Organization

Were your information networks designed with security in mind?

Is secure network design a key objective for future network acquisition and development?

How often are network diagrams reviewed and updated?

Do the network diagrams match their as-built and as-operating configuration?

Network documentation should be kept current and under configuration management with a strict access control listing. Whenever a change occurs to the network infrastructure, the network

documentation should be updated. Software products can be used to map networks. Using an automated process allows more frequent and less costly reviews of network configurations.

4.2.20 Penetration Tests and Team Exercises

4.2.20.1 What Is This?

The purpose of penetration tests is to test the effectiveness of your information security defenses. Red team exercises are a comprehensive type of penetration test, in which a team of security experts challenges the full spectrum of an organization's information security policies, processes, security controls, and people to identify vulnerabilities. Penetration tests and red team exercises can improve organizational readiness, improve training for defensive practitioners, and inspect current performance levels. However, they need to be used with care—if the standard is set too low they can increase complacency. If it is set too high, staff may become disillusioned and resent attempts to increase levels of security to a level that may seem unattainable.

Testing by security experts from outside of the CBRN facility can provide valuable and objective insights about the existence of vulnerabilities, the efficacy of defenses and mitigating controls already in place, and the potential benefit of those planned for future implementation. These exercises can also be used to identify ineffective investments—security policies that are not being followed or outdated practices that do not reflect present threat vectors.

4.2.20.2 Why Do This?

The saying "trust, but verify" is an important element of an information security program. The verify aspect involves both self-assessments and external assessment of security performance. In a complex environment where technology is constantly evolving, and new attacker tradecraft appears regularly, organizations should periodically test their defenses to identify gaps and to assess their readiness.

4.2.20.3 Questions for Your Organization

Are information systems subject to periodic penetration tests?

When weaknesses are identified through inspection and testing, are these weaknesses documented and addressed in a timely manner?

Are red team exercises conducted on selected information systems?

Are correct actions promptly taken after a red team exercise?

Penetration test and red team exercises are not appropriate for all systems. In particular, such testing can cause operating systems to shut down, which may not be appropriate for control systems. Care must be taken for such systems to only conduct testing when the systems are off-line. For information systems, less care is required but facility staff should still ensure that appropriate backups exist to allow systems to be restored to the configuration present before the start of testing.

5.0 COMMON DEFICIENCIES/PROBLEMS OBSERVED IN EXISTING INFORMATION SECURITY PROGRAMS

Existing information security programs have a number of common deficiencies that have been observed by the authors in their cyber and information security inspections of CBRN facilities. The deficiencies are not unique to CBRN facilities, but because of the hazards associated with facilities containing CBRN materials, prompt action to address these deficiencies should be a high priority. Samples of the key deficiencies we have observed include:

- **There is no single point of responsibility and authority for information security.** Each system administrator or task lead has his or her specific systems, but no single person is looking at the organization as a whole. When security incidents occur, effort is spent in assigning blame instead of incident resolution.
- **Controls are applied without a clear understanding of risk.** Organizations may apply controls and mitigations because it is an industry best practice or a traditional practice at the organization without considering the purpose of the control. Mitigations should have a specific purpose linked to a specific risk. That link helps identify the rationale for the control as well as articulate the additional risk if a control is not properly implemented.
- **Information Security is a one-time cost.** Organization may believe that a one-time investment in information security is sufficient; however information security is here to stay, and should be planned for in an organization's annual resource plan.
- **There is no process for vulnerability and patch management.** Many organizations do not have a solid methodology for management of system and application vulnerabilities, and many organizations do not have a robust patch-management process. Identification of vulnerabilities and management of patch and fix deployment is essential in maintaining a safe and secure computing infrastructure. As it has been proven many times in the last 12 months of government and commercial computing attacks, poor patch and vulnerability management can have devastating, expensive, and long-reaching future impacts.
- **Defined and effective performance monitoring is lacking.** Performance monitoring is important in understanding the overall cybersecurity risk posture for the organization to allow management to make informed decisions for the protection of information, systems, budgets, and staffing.
- **There is no continual review of threat actors and risk determinations.** Like performance monitoring, continuous review of the threat actors and risk is important in understanding the overall cybersecurity risk posture for the organization to make information management decisions for organizational IT security.
- **Cybersecurity policies and procedure are not fully developed and implemented.** This is an important aspect of a cybersecurity program so the user community and the staff managing and securing the computing infrastructure know the security measures to implement, what the purpose of the security measures for the organization are, and to ensure they are accountable for their actions.
- **Clearly documented configuration baselines for operating systems are lacking.** The importance of having formally reviewed and agreed-upon system configuration baselines is essential to maintain

the security of information and the information systems on which it is processed, stored, and transmitted.

- **Roles and responsibilities not well documented or understood.** Staff members are an important element of the overall cybersecurity program. It is important that they know what their responsibilities are, and that they are held accountable for those responsibilities.
- **Privileged user account protection is inadequate.** The amount of power that many privileged users have is quite large. Managing who has the keys to the kingdom is important, as is the protection of the computing infrastructure, and the privileged users need to understand how to protect those accounts. Compromise of one privileged account can be very costly from a monetary, reputation, and loss-of-information perspective.

6.0 SOURCES OF INFORMATION

6.1 International Organization for Standardization 27000 Series

The ISO/IEC 27000 (ISO/IEC 2014) is a series of standards that specify the complete implementation of an ISMS. A joint committee comprising representatives from ISO and IEC is responsible for drafting and publishing the series ISO 27000.

The ISO/IEC 27000 series includes standards that define requirements for an ISMS and for those certifying such systems. The series also provides direct support, detailed guidance and interpretation for the overall Plan-Do-Check-Act (PDCA) model for continuous quality control and improvement processes and requirements. As part of this process, implementing organization are mandated to identify, analyze, and evaluate risks and reduce these to an acceptable level using various contingencies defined by the ISO/IEC 27000 standards. Finally, the series addresses sector-specific guidelines for an ISMS and address conformity assessment to show that an ISMS meets specified requirements (IT Governance 2014).

The standards contained in ISO/IEC 27000 to 27010 cover fundamental requirements of an ISMS, are applicable to any domain, and can be applied to any organization regardless of size, structure, or objectives. ISO/IEC standard documents beyond 27010, most of which have yet to be developed, focus on sector-specific implementation guidelines, such as ISO/IEC 27011 on "Information security management guideline for telecommunications organizations," for example. Abiding by ISO/IEC standards is critical for organizations because it helps them to secure their own assets, manage levels of risk, improve and ensure customer confidence, avoid loss of brand damage, loss of earnings or potential fines, and evolve their information security alongside technological developments (IT Governance 2014).

The core documents in the series include (IT Governance 2014):

- ISO/IEC 27000 - Provides an introduction and **overview** of the ISO/IEC 27000 series
- ISO/IEC 27001 - Specifies general **requirements** for establishing, implementing, maintaining, and continually improving an ISMS; also includes requirements for the assessment and treatment of information security risks
- ISO/IEC 27002 - Establishes **guidelines and practices** for implementation of an effective program using various controls to address the risk environment
- ISO/IEC 27003 - Focuses on the critical aspects needed for successful **design and implementation** of an ISMS
- ISO/IEC 27004 - Provides guidance on the development and use of **measurement** processes in order to assess the effectiveness of an ISMS and associated controls
- ISO/IEC 27005 - Provides guidelines for the satisfactory implementation of information security based on a **risk management** approach
- ISO/IEC 27006 - Provides requirements for bodies providing **audit and certification** of information security management systems

- ISO/IEC 27007 - Provides guidance on the management of an ISMS **audit program** and the conducting of the internal or external audits
- ISO/IEC 27008 - Provides guidance on reviewing an organization's information security **controls** as part of an **audit** process
- ISO/IEC 27009 - Provides help to organizations in the energy industry to interpret and apply information security management guidelines to secure their **electronic process control systems**
- ISO/IEC 27010 - Provides guidance on how to meet specified requirements **for information exchange** using established messaging and other technical methods.

This standard is available from ISO/IEC for 138 CHF in paper and ePub formats. The third edition, published in January 2014, is available for free download in PDF format only under the license agreement for standards made available through the ITTF web site (ISO 2014a).

6.2 National Institute of Standards and Technology Special Publication 800 Series

NIST is a nonregulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life (NIST 2014a).

The Information Technology Laboratory (ITL) at NIST promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems (NIST 2007, p. iii).

NIST established the Special Publication (SP) 800 series reports in 1990 to create a dedicated series of publications on information security which report on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations (NIST 2007, p. iii). The higher the SP minor number, the more current and applicable the information.

SP800 Standards comprise nearly 170 separate guidance documents and include several of the following topics, among many others (NIST 2014d):

- SP 800-12 - *An Introduction to Computer Security*, 1995. This document provides a broad overview of computer security, control areas, and the importance of the implementing security controls. While this is good baseline information, it is no longer being maintained.
- SP 800-14 - *Generally Accepted Principles and Practices for Securing Information Technology Systems,* 1996. This document provides a baseline that organizations can use to establish and review their IT security programs. While this is good baseline information, it is no longer being maintained.

- SP 800-37 - *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* This document provides guidelines for the security certification and accreditation of Information Technology (IT) systems supporting the executive branch agencies of the U.S. federal government.
- SP 800-30, *Rev. 1 - Guide for Conducting Risk Assessments.* This publication identifies risk management as an essential management function of the organization.
- SP 800-45, *Version 2: Guidelines on Electronic Mail Security.* This publication is intended to aid organizations in the installation, configuration, and maintenance of secure mail servers and mail clients.
- SP 800-50 - *Building an Information Technology Security Awareness and Training Program.* This publication presents a conceptual framework for providing information technology (IT) security training for today's distributed computing environment. Revision 1 is currently in review.
- SP 800-53 - *Security and Privacy Controls for Federal Information Systems and Organizations.* This publication provides a catalog of security and privacy controls for federal ISMS and a process for selecting controls to protect organizational operations.
- SP 800-53A - *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans.* This publication is a companion to SP 800-53 and establishes common assessment procedures to assess the effectiveness of security controls in U.S. federal information systems.
- SP 800-82 - *Guide to Industrial Control Systems (ICS) Security* (NIST 2013a). This publication provides guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions.

The NIST SP800 publications are important information security guidelines because they are designed to facilitate cost-effective security and privacy of sensitive unclassified information by providing research and insight on various computer security risks, controls, and scenarios in which each respective control mechanism might be most useful or effective. These guidelines and practices are relevant for both federal government personnel with computer security responsibilities for sensitive systems as well as private sector personnel, though risks, priorities, and legal constraints may vary between each sector and thereby influence the type of controls which might be most effective or appropriate in each scenario. All Special Publications 800 Series can be found on the NIST website http://csrc.nist.gov/publications/PubsSPs.html.

6.3 International Society for Automation/International Electrotechnical Commission Standards

The International Society of Automation (ISA)/IEC-62443 is a series of standards, technical reports, and related information that defines procedures for implementing electronically secure Industrial Automation and Control Systems (IACS) (NovaTech 2014). This guidance is directed towards those responsible for designing, implementing, or managing industrial automation and control systems as defined in the program scope. The guidance also applies to users, system integrators, security practitioners, and control systems manufacturers and vendors. The series of publications was originally

referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the ISA Committee on Industrial Automation and Control Systems Security (ISA99) and publicly released as American National Standards Institute (ANSI) documents. In 2010, the documents were renumbered to be the ISA/IEC-62443 series to align the ISA and ANSI document numbering with the corresponding IEC standards. ISA and IEC each publish separate but nearly identical documents for each corresponding document number (ISA99 2014).

The ISA99 committee's purpose is to develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance. Furthermore, the committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure control systems. Compliance with the committee's guidance will improve system electronic security and help identify and address vulnerabilities; this helps reduce the risk of compromising confidential information or causing degradation or failure of the equipment or process under control (ISA99 2014).

The ISA-62443 standards and technical reports are organized into four general categories (ISA99 2014):

- **General**: Includes foundational information such as concepts, models and terminology; also reviews security compliance metrics and security life cycles for IACS.
- **Policies and Procedures**: Addresses various aspects of creating and maintaining an effective IACS security program; this guidance is geared toward management or an asset owner.
- **System**: Provides guidance on system design and technologies as well as security levels and requirements for the secure integration of control systems.
- **Component**: Describes specific product development and technical requirements for control system products.

6.4 German Federal Office for Information Security Standards

The Federal Office for Information Security (German translation abbreviated BSI) is the German government agency in charge of managing computer and communication security for the German government. Its areas of expertise and responsibility include the security of computer applications, critical infrastructure protection, Internet security, cryptography, counter-eavesdropping, certification of security products, and the accreditation of security test laboratories (Federal Office for Information Security 2014b).

The BSI Standards, the first of which were published in 2005, contain recommendations from BSI on methods, processes, procedures, approaches, and measures relating to information security. In these publications, BSI addresses information security issues for public authorities and companies as well as issues for which practical national or international approaches have been established (Federal Office for Information Security 2014a).

While BSI Standards can be leveraged to provide technical support to users of information technology, public agencies and companies can also adapt BSI recommendations, as needed, to help

fulfill their own needs. By promoting use of trusted methods, processes, and procedures, the BIS standards help facilitate secure information technology systems. BSI standards also describe cooperative approaches that have proven effective in enhancing information technology security (Federal Office for Information Security 2014a).

BSI standards in the series are listed as follows (Federal Office for Information Security 2014a).

- BSI Standard 100-1, *Information Security Management Systems(ISMS)*: Defines general requirements for an ISMS and provides systematic instruction on how to implement these requirements; this document is completely compatible with ISO 27001
- BSI-Standard 100-2, *IT-Grundschutz Methodology*: Describes step-by-step, practical procedures for implementing and operating an information security management system
- BSI-Standard 100-3, *Risk Analysis based on IT-Grundschutz*: Describes a risk analysis method based on IT-Grundschutz, which can be used to enhance security measures without duplicating efforts already accomplished under the IT-Grundschutz Methodology
- BSI-Standard 100-4, *Business Continuity Management*: Explains a systematic way to develop, establish and maintain an agency-wide or company-wide internal business continuity management system. The goal of business continuity management is to ensure that important business processes are only interrupted temporarily or not interrupted at all, even in critical situations.

6.5 National Information and Computer Security Strategies

Cybersecurity has become an area of increasingly high priority for all aspects of international civilian nuclear development as it has become apparent that significant cybersecurity risks are likely to exist at many nuclear facilities. Many nations have made cybersecurity a top national priority and developed corresponding national strategies on how to protect their information and communications technologies from being compromised and then jeopardizing national security, economic prosperity, and social well-being. Several examples of national strategies for cybersecurity described in the following sections.

6.5.1 Information and Computer Security Strategies in Australia

The aim of the Australian Government's cybersecurity policy is the maintenance of a secure, resilient, and trusted electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy. More specifically, the key objectives of the Australian Government's cybersecurity policy are that all Australians become aware of cyber risks, secure their computers and take steps to protect their identities, privacy, and finances online; Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers; and the Australian Government ensures its information and communications technologies are secure and resilient (Commonwealth of Australia 2009, pp. v-vii).

6.5.2 Information and Computer Security Strategies in the Czech Republic

The Czech Republic established a 2011-2015 Cyber Security Strategy, which defines its interests and objectives in the field of cybersecurity. The strategy document emphasizes the need to establish a robust and credible information security infrastructure with solid legal foundations in order to facilitate secure

information exchange and processing in all sectors of society; this infrastructure will also ensure that information may be used and shared freely and safely at all times. The document highlights a number of strategic objectives and measures that will help establish a strong information security infrastructure, including establishing strong legislative frameworks; strengthening of cybersecurity of public administration and critical infrastructure information systems; establishing a national Computer Emergency Response Team (CERT) agency; promoting international cooperation; promoting cooperation of the state, private sector and academia; and promoting cybersecurity awareness (Czech Republic 2014).

6.5.3 Information and Computer Security Strategies in Estonia

In 2007, Estonian government suffered cyberattacks by hacktivists that paralyzed its ability to operate. Estonia immediately went to work reviewing, strengthening, and establishing a robust approach to cybersecurity. In May 2009, the Estonian government implemented a Cyber Security Strategy that established a large-scale system of security measures, increased competencies, improved the legal framework, bolstered international cooperation, and raised cybersecurity awareness across the country. Under this strategy a Cyber Security Council was established. The Council made the decision to more fully incorporate cyber into the National Emergency Act. In 2008 under the North Atlantic Treaty Organization (NATO), the Cooperative Cyber Defense Center of Excellence was established to research ways to increase national and international cybersecurity. In 2009 the Estonian Informatics Center, a State agency tasked with providing cybersecurity for public information services and systems, was established. In 2010 the Estonian Defense League was established and identified information security volunteers to assist in times of national crisis. Also in 2010, the Guidelines for Development of Criminal Policy until 2018 were created to direct police to prevent the spread of hacking and malware, and increase the number of law enforcement cybersecurity specialists (Jackson 2013).**Error! Hyperlink reference not valid.**

6.5.4 Information and Computer Security Strategies in France

In a 2008 White Paper on Defense and National Security, France cited large-scale cyberattacks on national infrastructures as one of the major threats that France will face over the next 15 years. As a result, France created the French Network and Information Security Agency (ANSSI) in 2009 to lead its newly developed national strategy on information systems defense and security. France identifies four key strategic objectives in its national strategy document, including: become a world power in the area of cyber defense; safeguard France's ability to make critical policy decisions through the protection of sensitive information related to its sovereignty; strengthen the cybersecurity of critical national infrastructures; and ensure security in cyberspace. The document also describes seven key actions France will undertake to help achieve its strategic objectives, several of which include: effectively anticipate and analyze the environment to make appropriate decisions; detect and block attacks as well as alert and support potential victims; and enhance and perpetuate scientific, technical, industrial and human capabilities in order to maintain French independence in the realm of information security (French Network and Information Security Agency 2011, pp. 5-8).

6.5.5 Information and Computer Security Strategies in India

India's national cybersecurity strategy doctrine explains that its vision is to build a secure and resilient cyberspace for citizens, businesses, and government. India's cybersecurity mission is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to

cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation. The doctrine highlights a number of strategies for accomplishing this mission including, but not limited to creating a secure cyber ecosystem, creating an assurance framework, encouraging open standards, strengthening the regulatory framework, and promoting research and development in the area of cybersecurity (India Ministry 2013).

6.5.6 Information and Computer Security Strategies in Japan

Japan's most recent cybersecurity strategy doctrine is particularly advanced because it acknowledges that the government must be capable of managing any information security incident, should it occur, to ensure the nation's safety and security. So instead of focusing on characterizing and preventing threats exclusively, Japan has focused substantial efforts on ensuring that its information technology infrastructure has a robust crisis management capability led by stakeholders in both the public and private sectors. Japan describes several specific policy directives as mechanisms for establishing more robust response and management capability: reinforcement of policies taking account of possible outbreaks of cyberattacks and establishment of a counteractive organization; establishing policies adapted to changes in the information security environment; and establishing active rather than passive information security measures (Japanese Information Security Policy Council 2010, pp. 2 and 7).

6.5.7 Information and Computer Security Strategies in the Russian Federation

Russia's cybersecurity doctrine explains that information security influences and must be addressed from various tiers of society: at a national level, societal level, and individual level. The doctrine describes Russia's national interests, potential threats and origins of those threats, the state of Russia's current information security infrastructure, and methods for ensuring information security in Russia. Russia's strategy doctrine serves as the basis for shaping government policy on information security in the Russian Federation; preparing suggestions to improve the legal, procedural, scientific-technical and organizational framework for ensuring information security, and devising targeted national information security programs (Russian Federation 2008).

6.5.8 Information and Computer Security Strategies in the United States

The United States national strategy outlines its key objective to work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, the United States will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace. Furthermore, the United States will realize this future and help promulgate positive norms by combining diplomacy, defense, and development to enhance prosperity, security, and openness so all can benefit from networked technology (The White House 2011, pp. 8-11).

6.6 European Union Agency for Network and Information Security

Information technology and operative networks play an increasingly important role in facilitating the smooth functioning of the European Union (EU) market and also affect the daily lives of the citizens and

businesses. As a result, the European Parliament and Council established European Union Agency for Network and Information Security (ENISA) in 2004 (Regulation [EC] No 460/2004) to help the European Commission, its Member States, and the European business community address, respond to, and prevent network and information security problems. ENISA is designed to be an independent Center of Expertise that delivers high-quality and transparent technical advice in response to needs of EU stakeholders and stimulates cooperation between the public and private sector to meet evolving challenges in the area of information security. ENISA also assists the European Commission in the technical preparatory work for updating and developing community legislation in the field of network and information security (ENISA 2014a).

ENISA's core mission is to ensure strong and effective network and information security within the EU and to develop a culture of network and information security for the benefit of citizens, consumers, and business and public sector organizations in the EU (ENISA 2014a). ENISA's primary functions and activities include the following (ENISA 2014b).

- Advise and assist the European Commission and Member States on information security topics and how to collaborate with industry stakeholders to address security-related problems with hardware and software products.
- Collect and analyze data on security incidents in Europe and emerging risks.
- Promote risk assessment and risk management methods to enhance EU capability to deal with information security threats.
- Raise awareness and promote cooperation between various stakeholders in the information security field, notably by helping to facilitate public/private partnerships.
- ENISA leads CERTs that act as primary responders when information security incidents occur and also provide security services for their stakeholders such as alerts and warnings, advisories, and security training (ENISA 2014c).
- ENISA's Critical Information Infrastructure Protection (CIIP) and Resilience Unit is responsible for assisting competent national EU agencies, the private sector, and EU Commission in developing preparedness, response and recovery strategies, policies, and measures to address emerging critical information infrastructure threats (ENISA 2014e).
- ENISA's Identity and Trust team is responsible for helping European Commission stakeholders implement and revise, as needed, various EU policies and directives related to information security ENISA 2014d).

In February 2014, ENISA, the EU, and the European Free Trade Association finalized a series of standard operational procedures (SOPs) on how to manage multinational cyber crises. Through a combination of contact points, guidelines, workflows, templates, tools, and best practices, the EU-SOPs provide guidance on how to manage major cyber incidents that could escalate to a crisis. Most notably, the EU-SOPs emphasize that it is critical to establish direct links between decision makers and policy makers in order to successfully manage cyber crises (ENISA 2014f).

7.0 REFERENCES

ASD – Australian Signals Directorate. 2012. "Application Whitelisting Explained." Accessed September 11, 2014 at http://www.asd.gov.au/publications/csocprotect/application_whitelisting.htm.

ASD – Australian Signals Directorate. 2013. "'Top 4' Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirements Explained." Accessed September 11, 2014 at http://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf.

ASD – Australian Signals Directorate. 2014. "Top 35 Strategies to Mitigate Targeted Cyber Intrusions." Accessed September 11, 2014 at http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf.

Beechey J. 2011. *Application Whitelisting: Panacea or Propaganda?* Available at http://www.sans.org/reading-room/whitepapers/application/application-whitelisting-panacea-propaganda-33599 .

CERT. 2010. "Insider Threat Deep Dive: IT Sabotage." Published September 22, 2010. Accessed September 7, 2014 at http://www.cert.org/blogs/insider-threat/post.cfm?EntryID=57.

Commonwealth of Australia. 2009. "Cybersecurity Strategy." Accessed September 11, 2014 at http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

Council on CyberSecurity. 2014. "The Critical Security Controls for Effective Cyber Defense Version 5.1" Accessed November 13, 2014 at http://www.counciloncybersecurity.org/critical-controls/.

Czech Republic. 2014. "Cyber Security Strategy of the Czech Republic for the 2011-2015 Period." Accessed September 11, 2014 at http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF.

ENISA - European Union Agency for Network and Information Security. 2014a. "About ENISA." Accessed September 11, 2014 at https://www.enisa.europa.eu/about-enisa.

ENISA - European Union Agency for Network and Information Security. 2014b. "ENISA Activities. Accessed September 11, 2014 at https://www.enisa.europa.eu/about-enisa/activities.

ENISA - European Union Agency for Network and Information Security (ENISA). 2014c. "CERT." Accessed September 11, 2014 at https://www.enisa.europa.eu/activities/cert.

ENISA - European Union Agency for Network and Information Security (ENISA). 2014d. "Identity, Privacy and Trust." Accessed September 11, 2014 at https://www.enisa.europa.eu/activities/identity-and-trust/identity-privacy-and-trust.

ENISA - European Union Agency for Network and Information Security. 2014e. "Resilience of Networks and Services and Critical Information Infrastructure Protection." Accessed September 11, 2014 at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/resilience.

ENISA - European Union Agency for Network and Information Security. 2014f. "Standard Operational Procedures to manage multinational cyber crises finalized by EU, EFTA Member States and ENISA." Accessed September 11, 2014 at https://www.enisa.europa.eu/media/press-releases/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa.

European Parliament. 2004. "Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency." Accessed September 11, 2014 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

Federal Office for Information Security. 2014a. "BSI-Standards." Accessed April 3, 2014, at https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html.

Federal Office for Information Security. 2014b. The BSI. Accessed 3 Apr. 2014 at https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html.

French Network and Information Security Agency. 2011. "Information systems defence and security: France's strategy." Accessed on September 11, 2014 at http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.

IBM Global Technology Services. 2014. *IBM Security Services 2014 Cyber Security Intelligence Index*. IBM Corporation, Somers, New York. Available at http://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

IEEE Standard 1074-1995. 1997. "IEEE Standard for Developing Software Life Cycle Processes." Accessed October 9, 2014 at http://arantxa.ii.uam.es/~sacuna/is1/normas/IEEE_Std_1074_1997.pdf.

India Ministry - India Ministry of Communication and Information Technology, Department of Electronics and Information Technology. 2013. "Notification on National Cyber Security Policy 2013 (NCSP-2013)." Available at http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf.

Intel Security. 2014. *Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II.* Intel Security, Santa Clara, California. Available at http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

ISA99 - ISA99 Committee. 2014. "ISA99: Developing the Vital ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems Security." Accessed September 11, 2014 at http://isa99.isa.org/ISA99%20Wiki/Home.aspx. Last modified on July 27, 2014.

ISO – International Organization for Standardization. 2009. "ISO 31000 - Risk Management." Accessed October 8, 2014 at http://www.iso.org/iso/home/standards/iso31000.htm.

ISO – International Organization for Standardization. 2014a. "ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary." Accessed October 16, 2014 at http://standards.iso.org/ittf/licence.html.

ISO – International Organization for Standardization. 2014b. "ISO 27001 Controls and Objectives Annex A." Accessed October 8, 2014 at http://gender.gov.mu/English/Documents/activities/gender%20infsys/AnnexIX1302.pdf.

ISO/IEC – International Standards Organization/International Electrotechnical Commission. 2013. *Information Technology—Security Techniques—Code of Practice for Information Security Controls*. ISO/IEC 27002:2013. Available at http://www.iso.org/iso/catalogue_detail?csnumber=54533.

IT Governance. 2014. "The ISO/IEC 27000 Family of Information Security Standards," IT Governance, Ltd. Accessed March 31, 2014 at https://www.itgovernance.co.uk/iso27000-family.aspx.

Jackson, CM. 2013. "Estonian Cyber Policy after the 2007 Attacks: Drivers of Change and Factors for Success." New Voices in Public Policy, Volume VII, Spring 2014, George Mason University, School of Public Policy. Available at http://journals.gmu.edu/index.php/newvoices/article/download/69/95.

Japanese Information Security Policy Council. 2010. "Information Security Strategy for Protecting the Nation." Accessed September 11, 2014 at http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

Johnson CW. 2014. "CyberSafety: On the Interactions between CyberSecurity and the Software Engineering of Safety-Critical Systems." Accessed September 11, 2014 at http://www.dcs.gla.ac.uk/~johnson/papers/IET_2011/CyberSafety.pdf.

NIST - National Institute of Standards and Technology. 1995. *An Introduction to Computer Security: The NIST Handbook*. NIST Special Publication 800-12. National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed October 9, 2014 at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

NIST - National Institute of Standards and Technology. 1996. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. NIST Special Publication 800-14. National Institute of Standards and Technology, Gaithersburg, Maryland. Available at http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.

NIST - National Institute of Standards and Technology. 1998. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. NIST Special Publication 800-16. National Institute of Standards and Technology, Gaithersburg, Maryland. Available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

NIST - National Institute of Standards and Technology. 2003. *Building an Information Technology Security Awareness and Training Program*. NIST Special Publication 800-50. National Institute of Standards and Technology, Gaithersburg, Maryland. Available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

NIST - National Institute of Standards and Technology. 2006. *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86. National Institute of Standards and Technology, Gaithersburg, Maryland. Available at http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

NIST - National Institute of Standards and Technology. 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. Special Publication 800-94. Available at http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

NIST - National Institute of Standards and Technology. 2011. *Managing Information Security Risk, Organization, Mission and Information System View*. NIST Special Publication 800-39. National Institute of Standards and Technology, Gaithersburg, Maryland. Available at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

NIST - National Institute of Standards and Technology. 2012a. *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30, revision 1. National Institute of Standards and Technology, Gaithersburg, Maryland. Accessed October 9, 2014 at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

NIST - National Institute of Standards and Technology. 2012b. *Computer Security Incident Handling Guide*. NIST Special Publication 800-61, revision 2. National Institute of Standards and Technology, Gaithersburg, Maryland. Available at http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

NIST - National Institute of Standards and Technology. 2013a. *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82, revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf.

NIST - National Institute of Standards and Technology. 2013b. *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST Special Publication 800-53, revision 4. Available at http://dx.doi.org/10.6028/NIST.SP.800-53r4.

NIST - National Institute of Standards and Technology. 2014a. "NIST General Information." Accessed September 11, 2014 at http://www.nist.gov/public_affairs/general_information.cfm. Last updated January 31. 2014.

NIST - National Institute of Standards and Technology. 2014b. "National Vulnerability Database, Statistics Results Page." Accessed October 15, 2014 at http://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&pub_date_start_month=0&pub_date_start_year=2004&pub_date_end_month=11&pub_date_end_year=2013.

NIST - National Institute of Standards and Technology. 2014c. "The Security Content Automation Protocol (SCAP)." Accessed November 14, 2014 at http://scap.nist.gov/. Last updated January 24, 2014.

NIST - National Institute of Standards and Technology. 2014d. "Special Publications (800 Series)." Accessed on November 17, 2014 at http://csrc.nist.gov/publications/PubsSPs.html. Last updated October 9, 2014.

Norton. 2014. "2013 Norton Report." Accessed October 8, 2014 at http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx.

NovaTech. 2014. "Addressing ISA/IEC-62443 Cyber Security," February 19. 2014. Accessed September 11, 2014 at https://www.novatechweb.com/news/addressing-isaiec-62443-cyber-security.

OWASP. 2014. OWASP Risk Rating Methodology. Accessed November 11, 2014 at https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. Last updated September 19, 2014.

Russian Federation - The Ministry of Foreign Affairs of the Russian Federation. 2008. "Information Security Doctrine of the Russian Federation." Accessed September 11, 2014 at http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument

Schneier B. 1999. "Modeling security threats." *Dr. Dobb's Journal*. Accessed November 13, 2014 at https://www.schneier.com/paper-attacktrees-ddj-ft.html.

The SANS Institute and The Anfield Group. 2014. "NERC CIP Standard Mapping to the Critical Security Controls - Draft." Accessed September 11, 2014 at https://www.sans.org/media/critical-security-controls/nerc-cip-mapping-sans20-csc.pdf.

The White House. 2011. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." Accessed September 11, 2014 at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

The White House. 2012. "National Strategy for Information Sharing and Safeguarding.". Accessed November 11, 2014 at http://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015a. "How To Implement Security Controls for an Information Security Program at CBRN Facilities". United Nations Interregional Criminal Justice Research Institute. Turin, Italy. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-ACT-10019.pdf.

UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015b. "Information Security Management System Planning for CBRN Facilities." United Nations Interregional Criminal Justice Research Institute. Turin, Italy. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24874.pdf.

U.S. Department of Justice. 2004. "Forensic Examination of Digital Evidence: A Guide for Law Enforcement". Accessed October 9, 2014 at https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

U.S. Department of Justice. 2008. "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition." Accessed October 9, 2014 at https://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

8.0 GLOSSARY

Availability (prevent unauthorized access restrictions). This refers to the ability or assurance that authorized individuals, information technology, or controls systems are able to access and interact with required information in an uninterrupted and timely manner.

Cracker is an individual who demonstrates malicious intent by breaking into or otherwise violating the system integrity of computers or networks without authorization. Crackers typically steal or destroy data, deny access to legitimate users, and cause problems for their targets.

Cyberattack includes a wide assortment of computer-based events that are capable of modifying, destroying, or compromising the integrity and confidentiality of data; results in the denial of access to systems, networks, services, or data; or otherwise negatively affects the proper operation or function systems, networks, and associated equipment. Cyberattacks may involve the use of computer viruses, worms, malware, false data, denial of service, or other types of exploits and may be directed or nondirected in nature. Cyberattacks also may include physical attacks involving the theft or destruction of hardware or seek to modify environmental conditions in order to affect the functionality of a computer-based system.

Confidentiality (prevent unauthorized access). This refers to the ability or assurance to limit access to information to authorized individuals or secret systems or otherwise prevent its unauthorized disclosure.

Hacker is a person who, without authorization, uses programming skills or tools to gain access to a computer system or network.

Hacktivists are motivated by perceived acts of social injustice by government authorities that affect human rights, free speech, religious beliefs, the environment, among other topics. Hacktivists engage in cyberattacks as a form of technical protest, activism, or civil disobedience in order to force changes in social policy or governmental behavior.

Integrity (prevent unauthorized modification). This refers to the assurance that information has not been modified in an unauthorized manner that would affect its accuracy or reliability. This includes information used by personnel, information technology, or controls systems that operate facility processes.

Management controls concentrate on the management of information security. Controls within this category include activities involving certification, accreditation, security assessments, planning, risk assessment, and system or services acquisition.

Operational controls are safeguards or protective measures that are to be performed by humans rather than by automated means. Controls within this category include activities involving training, configuration management, contingency planning, incident response, maintenance, media protection, physical and environmental protection, system and information integrity, and personnel security.

Resiliency involves the ability to resist adverse impacts, absorb impacts while still maintaining functionality, or quickly recover from an attack. Resiliency, like vulnerabilities, includes both human and technological components.

Risk, specifically **information security risk,** is a product of the likelihood that something adverse will happen to information and the resulting consequences of that adverse event on those who need to use that information.

Technical controls are considered to be safeguards or protective measures that are executed through mechanisms contained within the hardware, firmware, operating system or application software. Controls within this category would include access controls, audit and accountability, identification and authentication, and system and communications protection. This classification of controls would include devices typically related to security such as routers, firewalls, intrusion detection and prevention systems, smart-tokens, and logging systems, to name a few. With technical controls, actions are automatically taken in response to a triggering event.

Threat represents the intent, capability, and opportunity of an adversary to attack or inflict harm.

Threat agents carry out threats against vulnerable targets using tools, tactics, and procedures (TTP) to accomplish their objectives in response to some motivation (i.e., political ideology, religious belief, money, or challenge).

Vulnerability is defined to be a weakness in the physical or electronic configuration of an asset that could allow an action that compromises the security of the assets.

Contact:
UNICRI
Viale Maestri del Lavoro, 10,
10127, Turin, Italy
Tel: (+39) 011 6537 111
Fax: (+39) 011 63133 68
information@unicri.it
www.unicri.it

Clifford Glantz
Pacific Northwest National Laboratory
P.O. Box 999, MSIN K9-30, Richland, WA 99352
Tel: 001-509-375-2166
cliff.glantz@pnnl.gov
www.pnnl.gov