

# **Critical Infrastructure Cybersecurity**

# **Critical Infrastructure Cybersecurity**

# **Critical Infrastructure Cybersecurity**


An open-source course sponsored, published, and made available to instructors for their free use by CyberWatch West

CyberWatch West

Whatcom Community College

Bellingham, WA

# Critical Infrastructure Cybersecurity

 Icon for the Creative Commons Attribution 4.0 International License

Critical Infrastructure Cybersecurity by Whatcom Community College and CyberWatch West is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/), except where otherwise noted.

Except where otherwise noted, these materials are licensed under a Creative Commons Attribution 4.0 International License. ©2017 CyberWatch West, Whatcom Community College.

CyberWatch West is funded by a National Science Foundation Advanced Technological Education Grant and is located at Whatcom Community College, 237 West Kellogg Road, Bellingham, WA.

# Contents

1. [Course Description](#)
2. [Prerequisites](#)
3. [Technology Requirements](#)
4. [Objectives & Outcomes](#)
5. [Note to Instructors](#)
6. [Module 1: Introduction to Critical Infrastructure](#)
7. [Module 1 Description & Objectives](#)
8. [Module 1 Presentation & Required Reading](#)
9. [Module 1 Hands-on Activity](#)
10. [Module 1 Team Activity](#)
11. [Module 1 Assessment](#)
12. [Module 2: Introduction to Control Systems & SCADA](#)
13. [Module 2 Description & Objectives](#)
14. [Module 2 Presentation & Required Reading](#)
15. [Module 2 Hands-on Activity](#)
16. [Module 2 Team Activity](#)
17. [Module 2 Assessment](#)
18. [Module 3: Technologies](#)
19. [Module 3 Description & Objectives](#)
20. [Module 3 Presentation & Required Reading](#)
21. [Module 3 Hands-on Activity](#)
22. [Module 3 Team Activity](#)
23. [Module 3 Assessment](#)
24. [Module 4: Risk Management](#)
25. [Module 4 Description & Objectives](#)
26. [Module 4 Presentation & Required Reading](#)
27. [Module 4 Hands-on Activity](#)
28. [Module 4 Team Activity](#)
29. [Module 4 Assessment](#)
30. [Module 5: Threats](#)
31. [Module 5 Description & Objectives](#)
32. [Module 5 Presentation & Required Reading](#)
33. [Module 5 Hands-on Activity](#)

34. [Module 5 Team Activity](#)
35. [Module 5 Assessment](#)
36. [Module 6: Vulnerabilities](#)
37. [Module 6 Description & Objectives](#)
38. [Module 6 Presentation & Required Reading](#)
39. [Module 6 Hands-on Activity](#)
40. [Module 6 Team Activity](#)
41. [Module 6 Assessment](#)
42. [Module 7: Risk Assessments](#)
43. [Module 7 Description & Objectives](#)
44. [Module 7 Presentation & Required Reading](#)
45. [Module 7 Hands-on Activity](#)
46. [Module 7 Team Activity](#)
47. [Module 7 Assessment](#)
48. [Module 8: Remediation](#)
49. [Module 8 Description & Objectives](#)
50. [Module 8 Presentation & Required Reading](#)
51. [Module 8 Hands-on Activity](#)
52. [Module 8 Team Activity](#)
53. [Module 8 Assessment](#)
54. [Module 9: Incident Response](#)
55. [Module 9 Description & Objectives](#)
56. [Module 9 Presentation & Required Reading](#)
57. [Module 9 Hands-on Activity](#)
58. [Module 9 Team Activity](#)
59. [Module 9 Assessment](#)
60. [Module 10: Policy & Governance](#)
61. [Module 10 Description & Objectives](#)
62. [Module 10 Presentation & Required Reading](#)
63. [Module 10 Hands-on Activity](#)
64. [Module 10 Team Activity](#)
65. [Module 10 Assessment](#)
66. [Module 11: Trends](#)
67. [Module 11 Description & Objectives](#)
68. [Module 11 Presentation & Required Reading](#)
69. [Module 11 Hands-on Activity](#)
70. [Module 11 Team Activity](#)

71. [Module 11 Assessment](#)
72. [Module 12: Sector Reports Out](#)
73. [Sector Reports Out](#)
74. [Supplemental Materials & Resources](#)
75. [Textbook Mapping](#)
76. [Sample Syllabus](#)

# Course Description

1

Students will address basic security concepts as they apply to critical infrastructure systems. Concepts addressed in the course will include Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), national standards for the protection of critical infrastructure, and risk management concepts and tools for critical infrastructure systems. Students will perform a risk assessment of a specific critical infrastructure sector using an appropriate risk assessment framework and tools, identifying threats and vulnerabilities specific to the sector, and making appropriate recommendations for mitigating risk.



# Prerequisites

2

Students should have completed an introductory security course, such as CompTIA's Security+, or otherwise have knowledge of basic network and computer security concepts and technologies.

# Technology Requirements

3

Students must be able to access and subscribe to the [FEMA education portal](#) and the [ICS-CERT education portal](#).

# Objectives & Outcomes

4

# Course Objectives

Topics addressed in the course include:

- Critical infrastructure (CI) and critical infrastructure security and resilience (CISR), including the 16 critical infrastructure sectors, as defined by the Department of Homeland Security (DHS) and identified in Presidential Policy Directive 21 (PPD-21: Critical Infrastructure Security and Resilience).
- Industrial Control Systems (ICS) such as SCADA, PCS, and DCS.
- Risk Management Frameworks applicable to CI systems.
- Cybersecurity services, such as confidentiality, integrity, availability, and authentication, as they apply to CI systems.
- Cybersecurity threats, risks, vulnerabilities, and attacks as they apply to CI systems.
- Vulnerability assessments and tools applicable to CI systems.
- CI systems risk management strategies.
- Trends in cybersecurity impacting CI sectors.

# Student Outcomes

At the conclusion of the course, students will be able to:

- Define CI sectors and identify legislation and standards addressing CI protection.
- Define common terms and concepts associated with CI, including ICS, SCADA, PCS, and DCS.
- Identify the components and process of implementing a CISR risk management program.
- Describe cybersecurity services such as confidentiality, integrity, availability, and authentication as they apply to CI systems.
- Select appropriate vulnerability assessment frameworks and tools as part of a risk assessment of a CI system.
- Identify and describe cybersecurity threats, risks, vulnerabilities, and attacks as they apply to CI systems.
- Identify an appropriate risk management strategy for CISR.

# Note to Instructors

5

This twelve-module course includes suggested activities and assignments for each module. Particular assignments can be consolidated or eliminated, depending on the needs of specific classes.

One recommended approach is to have student teams work on case studies for fictional organizations throughout the course; their work culminates in a final project presented to the class. Instructors following this method should consider assigning student teams the creation of several presentation slides (using Microsoft PowerPoint or other presentation applications), for modules in which more than one optional assignment is described. Student teams can combine all their slides into a single presentation as their team activity for Module 11, and share their team's presentation with the class for Module 12.

Modules 1–11 include suggested assessment questions. The answers to the questions are not provided within the modules, in order to prevent students from finding and downloading them. To receive the answers, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.

# **Module 1: Introduction to Critical Infrastructure**

|

# **Module 1 Description & Objectives**

1



# Description

This module covers the Critical Infrastructure Security and Resilience foundational courses and certifications from the Federal Emergency Management Administration (FEMA). It is based on a three-part assignment that uses the online FEMA Emergency Management Institute courses and exam certifications that cover the following three topics:

- IS-860.C: The National Infrastructure Protection Plan, An Introduction
- IS-913.A: Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration
- IS-921.A: Implementing Critical Infrastructure Security and Resilience

The focus is on five key subject sectors that the National Infrastructure Protection Plan identifies as “Lifeline” sectors: Energy, Water and Wastewater Systems, Communications, Transportation Systems, and Emergency Services. This module gives students a better understanding of what those assets are, what components are considered “critical,” and how to identify them for entry into the IP Gateway that serves as the single interface through which Department of Homeland Security (DHS) partners can access the department’s integrated infrastructure protection tools and information.

## Objectives

- Define critical infrastructure, protection, and resilience in the context of the National Infrastructure Protection Plan (NIPP).
- Describe critical infrastructure in communities and the impact Lifeline sector assets have on a community’s resiliency.

- Describe the processes that support critical infrastructure security and resilience.
- Identify strategies and methods for achieving results through critical infrastructure partnerships.
- Describe the roles and responsibilities of entities such as the DHS, sector-specific agencies, and state, local, tribal, and territorial governments.
- Discuss common standards bodies, such as the North American Electricity Reliability Council (NAERC) and the National Institute of Standards and Technology (NIST).
- Understand which certifications are required to protect critical infrastructure.

# **Module 1 Presentation & Required Reading**

2

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=26>

[Download \[1.79 MB\]](#)

# Required Reading

Miller, Stephen, and Clark, Richard H. [\*Framework for SCADA Cybersecurity. Smashwords Edition\*](#), eBook ISBN 978-1310-30996-0. Chapter 2 “Cybersecurity Framework Introduction,” Section 1 “Framework Introduction,” pages 43-45.

# Module 1 Hands-on Activity



## Overview

This three-part assignment uses the online FEMA Emergency Management Institute courses and exam certifications that cover the following three topics:

1. IS-860.C: [The National Infrastructure Protection Plan, An Introduction](#)
2. IS-913.A: [Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration](#)
3. IS-921.A: [Implementing Critical Infrastructure Security and Resilience](#)

The focus is on five key subject sectors that the National Infrastructure Protection Plan identifies as “Lifeline” sectors: Energy, Water and Wastewater Systems, Communications, Transportation Systems, and Emergency Services. This module gives students a better understanding of what those assets are, what components are considered “critical,” and how to identify them for entry into the IP Gateway that serves as the single interface through which Department of Homeland Security (DHS) partners can access its integrated infrastructure protection tools and information.

### Hands-on Activity Objectives

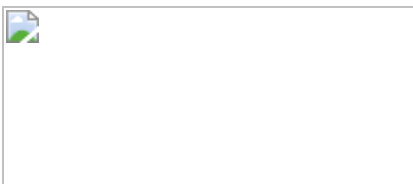
- Understand the roles and responsibilities of entities such as the DHS, sector-specific agencies, and state, local, tribal, and territorial governments.
- Describe the processes that support critical infrastructure security and resilience.

- Define critical infrastructure, protection, and resilience in the context of the National Infrastructure Protection Plan (NIPP).
- Identify strategies and methods for achieving results through critical infrastructure partnerships.
- Identify various methods for assessing and validating information.
- Describe critical infrastructure in communities and the impact Lifeline sector assets have on a community's resiliency.
- Discuss common standards bodies, such as the North American Electricity Reliability Council (NAERC) and National Institute of Standards and Technologies (NIST).

Independent Study Exams require a FEMA Student Identification (SID) Number. Students who do not have a SID can register for one at <https://cdp.dhs.gov/femasid>.

Questions regarding the FEMA Independent Study Program or other Emergency Management Institute (EMI) related requests, such as requests for certificates, transcripts, or online test scores/results, should be referred to the FEMA Independent Study program office at 301-447-1200 or emailed to [Independent.Study@fema.dhs.gov](mailto:Independent.Study@fema.dhs.gov). Please do not contact the FEMA SID Help Desk, as they are unable to provide assistance with such requests.

---





# **IS-860.C: The National Infrastructure Protection Plan, An Introduction**

<https://training.fema.gov/is/courseoverview.aspx?code=IS-860.c>

# Course Overview

Ensuring the security and resilience of the critical infrastructure of the United States is essential to the nation's security, public health and safety, economic vitality, and way of life.

The purpose of this course is to present an overview of the National Infrastructure Protection Plan (NIPP). The NIPP provides the unifying structure for the integration of existing and future critical infrastructure security and resilience efforts into a single national program.

## Learning Objectives

- Explain the importance of ensuring the security and resilience of critical infrastructure of the United States.
- Describe how the NIPP provides the unifying structure for the integration of critical infrastructure protection efforts into a single national program.
- Define critical infrastructure, protection, and resilience in the context of the NIPP.

# **Primary Audience**

The course is intended for DHS and other federal staff responsible for implementing the NIPP, and tribal, state, local, and private sector emergency management professionals. The course is also designed to teach potential security partners about the benefits of participating in the NIPP.

# Prerequisites

None

# Course Length

2 hours



---

# **IS-913.A: Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration**

<http://training.fema.gov/is/courseoverview.aspx?code=IS-913.a>

# Course Overview

The purpose of this course is to introduce the skills and tools to effectively achieve results for critical infrastructure security and resilience through partnership and collaboration.

The course provides an overview of the elements of and processes to develop and sustain successful critical infrastructure partnerships.

## Learning Objectives

- Explain the value of partnerships to infrastructure security and resilience.
- Identify strategies to build successful critical infrastructure partnerships.
- Describe methods to work effectively in a critical infrastructure partnership.
- Identify processes and techniques used to sustain critical infrastructure partnerships.
- Identify strategies and methods for achieving results through critical infrastructure partnerships.

# **Primary Audience**

The course is designed for critical infrastructure owners and operators from both the government and private sector and those with critical infrastructure duties and responsibilities at the state, local, tribal, and territorial levels.



# Prerequisites

None. The following is recommended prior to starting the course:

- IS-921.A, Implementing Critical Infrastructure Security and Resilience

# Course Length

2 hours



---

# **IS-921.A: Implementing Critical Infrastructure Security and Resilience**

<http://training.fema.gov/is/courseoverview.aspx?code=IS-921.a>

# Course Overview

This course introduces those with critical infrastructure duties and responsibilities at the state, local, tribal, and territorial levels to the information they need and the resources available to them in the execution of the mission to secure and improve resilience in the nation's critical infrastructure.

## Learning Objectives

- Summarize critical infrastructure responsibilities.
- Identify the range of critical infrastructure government and private-sector partners at the state, local, tribal, territorial, regional, and federal levels.
- Describe processes for effectively sharing information with critical infrastructure partners.
- Identify various methods for assessing and validating information.

# **Primary Audience**

This course is designed for all individuals with critical infrastructure protection responsibilities.

# Prerequisites

None. The following are recommended prior to starting the course:

- Review of the National Infrastructure Protection Plan (NIPP) and Critical Infrastructure Support Annex to the National Response Framework (NRF) documents.

OR

- Completion of the following Independent Study courses:
  - IS-860.B, National Infrastructure Protection Plan (NIPP);  
and
  - IS-821.A, Critical Infrastructure Support Annex.

# Course Length

3 hours

# **Assignment Deliverables**

1. Completion of all three FEMA Emergency Management Institute courses and exam certifications.



# Grading Criteria Rubric

- Students should submit copies of all three exam completion certificates.

Grade points: 300

# Module 1 Team Activity

4

 **"Team" by  
Newtown  
grafitti via  
Flickr CC**

## **Overview**

Students pair into teams, which identify one of the 16 critical infrastructure sectors to focus on throughout the course. Each week's module will be examined through the lens of the chosen sector. Student teams are expected to investigate their chosen sector and create a fictitious organization that will be used as a case study in future assignments.

### **Team Activity Objectives**

- Define critical infrastructure, protection, and resilience in the context of the NIPP.
- Identify strategies and methods for achieving results through critical infrastructure partnerships.
- Identify various methods for assessing and validating information.
- Describe critical infrastructure in communities and the impact Lifeline sector assets have on a community's resiliency.
- Discuss common standards bodies, such as the North American Electricity Reliability Council (NAERC) and National Institute of Standards and Technologies (NIST).

Please select a critical infrastructure sector for your team:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Now create a fictitious organization that would work in that sector. Determine the organization's name, number of employees, and the type of work it does. For example, to investigate the Nuclear Reactors, Materials, and Waste sector, you could describe a nuclear plant with 350 employees, where uranium is refined for use in nuclear weapons.

Research the following about organizations like the one you have described:

- Is this sector a "Lifeline" sector?
- What standards does your organization fall under?
- What role would your sector-specific agency play in your organization?
- Identify at least three potential cybersecurity risks to your organization.

# Assignment Options

**Option 1:** Write a two-page abstract on your sector and your fictitious organization, answering the four questions above.

**Option 2:** Prepare 2–3 presentation slides about your sector and your fictitious organization, answering the four questions above.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100

# Module 1 Assessment

5

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. Nuclear power plants that generate electricity fall under the Energy Sector.

\_\_\_\_\_ 2. “Lifeline” critical infrastructure sectors are those sectors that are essential for the operation of most other critical infrastructure.

\_\_\_\_\_ 3. A coordinating sector-specific agency for the Food and Agriculture Sector is the Department of Health and Human Services.

\_\_\_\_\_ 4. The organization that defines the standards for reliable bulk power systems is NIST.



# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 5. Which of the following is **not** a Lifeline sector?

- a. Energy
- b. Telecommunications
- c. Healthcare and Public Health
- d. Transportation Systems

\_\_\_\_\_ 6. Which of the following is **not** a segment in the Energy sector?

- a. Gas
- b. Electricity
- c. Oil
- d. Solar

\_\_\_\_\_ 7. Which of the following designates DHS as the responsible agency to provide strategic guidance to the critical sectors?

- a. NIST
- b. NERC
- c. PPD-21
- d. SLTT

\_\_\_\_\_ 8. Which of the following is a role of SLTTGCC?

- a. Coordinate with DHS
- b. Serve as a federal interface
- c. Provide organizational structure, coordinating across jurisdictions
- d. Carry out incident management responsibilities

# Completion

*Complete the sentence.*

9. Infrastructure resilience is

---

## Short Answer

10. Name the five Lifeline sectors and explain why these sectors are essential to the nation's economy and well-being.

11. Identify two other sectors on which the Food and Agriculture Sector depends and explain the relationship.

12. Explain how attacks on the Water and Wastewater Systems sector can negatively impact health and human safety.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# **Module 2: Introduction to Control Systems & SCADA**

||

# **Module 2 Description & Objectives**

6

# Description

This module introduces Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Process Control Systems (PCS), with overviews of what they are and how they are used.

## Objectives

- Describe the components and applications of industrial control systems.
- Describe the purpose and use of SCADA, DCS, and PCS systems.
- Describe the configuration and use of field devices used to measure critical infrastructure processes, such as flow rate, pressure, temperature, level, density, etc.
- Describe the use and application of Programmable Logic Controllers (PLCs) in automation.

# **Module 2 Presentation & Required Reading**

7



# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=41>

[Download \[1.90 MB\]](#)

# Required Reading

None

# Module 2 Hands-on Activity

8



## Overview

Students download a 15-day free trial of PLC Ladder (located at [PLCtrainer.net](http://PLCtrainer.net) or [LogicsPro](http://LogicsPro)). They install the software and explore its options to understand how PLC works; packet capture – protocol and transit across the network; and how to program the PLC.

### Hands-on Activity Objectives

- Describe the purpose and use of SCADA, DCS, and PCS systems.
- Describe the configuration and use of field devices used to measure critical infrastructure processes, such as flow rate, pressure, temperature, level, density, etc.
- Provide examples of HMI screens and displays used within SCADA systems.
- Describe the use and application of PLCs in automation.

# Lab Assignment

## Use PLC Simulator to explore relay logic

1. Install the LogixPro 500 PLC simulator on a Windows VM. It can be used with a 15-day free trial (available from [The Learning Pit](#)).
  1. [Virtual Box Download](#)
  2. [Virtual Box Documentation User Manual](#)
2. Launch the LogixPro simulator.
3. Click on the “Help” drop-down menu and select “Student Exercises.” The following web page will open.
  
4. Under the “Student RSLogix Programming Exercises” section, select the “Relay Logic .... Introductory Exercise” option. The following web page will open.
  
5. Complete the “LogixPro Relay Logic Introductory Lab” exercise following these instructions. You can use the printed handout instead if preferred.
6. Under the “Student RSLogix Programming Exercises” section, select the “Door Simulation .... Applying Relay Logic” option. The following web page will open.
  
7. Complete the “LogixPro Door Simulation Lab” exercise following these instructions. You can use the printed handout instead if preferred.

8. Under the “Student RSLogix Programming Exercises” section, select the “Silo Simulator .... Applying Relay Logic to a Process” option. The following web page will open.

9. Complete the “LogixPro Silo Lab” exercise following these instructions. You can use the printed handout instead if preferred.

Grade Points: 100

*This lab was developed by CSEC, the Cyber Security Education Consortium, an Advanced Technological Education (ATE) program funded by the National Science Foundation.*

# Module 2 Team Activity

9



## Overview

Student teams continue to build a description of the operating environment for their sector-based organizations. What systems will be used within the organization?

### Team Activity Objectives

- Describe the purpose and use of SCADA, DCS, and PCS systems.
- Describe the configuration and use of field devices used to measure critical infrastructure processes, such as flow rate, pressure, temperature, level, density, etc.
- Provide examples of HMI screens and displays used within SCADA systems.
- Describe the use and application of PLCs in automation.
- Describe the components and applications of industrial control systems.

Write a description of the operating environment for your sector-based organization. Determine what industrial control/SCADA and business IT systems will be used within the organization.



# Assignment

Write a 2-page abstract summarizing your findings on your sector and the industrial control/SCADA and business IT systems that will be used within your fictitious organization.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade points: 100

# Module 2 Assessment

10

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. Radio telemetry is not used much to communicate field data as it is expensive and limited in range to only several hundred feet from the device.

\_\_\_\_\_ 2. Remote Telemetry Units (RTUs) and Programmable Logic Controllers (PLCs) serve roughly the same purpose, monitoring process feedback and sending the data to a centralized computer.

\_\_\_\_\_ 3. A logic programming language that is similar to an AC wiring diagram is called a Function Block Diagram.

\_\_\_\_\_ 4. SCADA systems can be networked in either a LAN or a WAN.

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 5. Which of the following is **not** a part of industrial control systems?

- a. Supervisory Control and Data Acquisition
- b. Distributed Control Systems
- c. Production Control Systems
- d. Programmable Logic Controllers

\_\_\_\_\_ 6. Which of the following is **not** one of the main methods by which measurement data is communicated to a system?

- a. Computer protocols, such as serial communications
- b. Analog devices
- c. Binary alarms
- d. Digital devices

\_\_\_\_\_ 7. Which of the following is **not** a function of SCADA data?

- a. Providing
- c.

information from which reports and trending data can be generated

Providing meaningful displays for operators

b.

Monitoring

and

annunciating the above

alarm

conditions

d. All of

# Completion

*Complete each sentence.*

8. A system that provides for remote monitoring and control of industrial devices and equipment (bringing plant/process data into a computer systems) is known as \_\_\_\_\_.

9. \_\_\_\_\_ can be either digital or analog devices that provide an audible warning of a condition.

## Short Answer

10. Discuss some of the useful information that SCADA reports can provide.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*



# Module 3: Technologies

III

# **Module 3 Description & Objectives**

11

# Description

A number of different networking and SCADA protocols, hardware, and security devices are available to protect a network and the devices on that network. This module addresses the various mechanisms for employing hardware, protocols, and technologies with basic protections in infrastructure and network design. It also identifies methods for enhancing the security of an enterprise network through the positioning of certain pieces of hardware, protocol, and network equipment.

## Objectives

- List several types of networking hardware and explain the purpose of each.
- List and describe the functions of common communications protocols and network standards used within CI.
- Identify new types of network applications and how they can be secured.
- Identify and understand the differences between IPv4 and IPv6.
- Discuss the unique challenges/characteristics of devices associated with industrial control systems.
- Explain how existing network administration principles can be applied to secure CIKR.

# **Module 3 Presentation & Required Reading**

12

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=57>

[Download \[1.42 MB\]](#)

# Required Reading

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Department of Homeland Security. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*. September 2016. Available online at <https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP>.

# Module 3 Hands-on Activity



## Overview

Explore the interactive graphic [Secure Architecture Design](#). This secure design is the result of an evolutionary process of technology advancement and increasing cyber vulnerability presented in the Recommended Practice document *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.

### Hands-on Activity Objectives

- List several types of networking hardware and explain the purpose of each.
- List and describe the functions of common communications protocols and network standards used within CI.
- Explain how existing network administration principles can be applied to secure CIKR.
- Identify new types of network applications and how they can be secured.



# Assignment

Use the [ICS-Cert](#) learning portal to examine an enterprise diagram for an overview of a network. If you are not registered yet, please register.

Hover over the various areas of the Secure Architecture Design graphic, located at <https://ics-cert.us-cert.gov/Secure-Architecture-Design>. Click inside the box for additional information associated with the system elements.

After downloading and reading *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies* (see [Required Reading](#)), navigate through the embedded description in the Secure Architectural Design diagram.

Write a short paper describing the following recommended practices for improving industrial control systems cybersecurity with Defense-In-Depth Strategies for your team's fictitious sector-based company:

- Security Challenges within Industrial Control Systems
- Isolating and Protecting Assets: Defense-in-Depth Strategies
- Recommendations and Countermeasures

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade points: 100

# Module 3 Team Activity

14



## Overview

Student teams continue to build a description of the operating environment for their sector-based organizations. They identify the networking protocols and technologies that will be used within the organization.

### Team Activity Objectives

- List several types of networking hardware and explain the purpose of each.
- List and describe the functions of common communications protocols and network standards used within CI.
- Explain how existing network administration principles can be applied to secure CIKR.
- Identify new types of network applications and how they can be secured.
- Discuss the unique challenges/characteristics of devices associated with industrial control systems.

## Assignment

Using Visio or another diagramming application, develop and draw a network diagram of your enterprise system. See the example below.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Diagram

Grade Points: 100

# Module 3 Assessment

15

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. Unlike IT systems, ICS places more importance on availability than on confidentiality.

\_\_\_\_\_ 2. Stateless firewalls examine each packet and make a determination about whether or not the packet is allowed based on context.

\_\_\_\_\_ 3. IPv6 is an improvement over IPv4 because of its ability to support encryption, authentication, and longer address space.



# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 4. Which of the following is **not** an element of Operational Technology?

- a. Event-driven architecture
- b. Processes transactions and provides information
- c. Consists of electromechanical, sensors, actuators, coded displays, handheld devices
- d. Controls machines rather than providing support to people

\_\_\_\_\_ 5. Which of the following is **not** a major component of an ICS network?

- a. Fieldbus Network
- b. Remote Access Points
- c. Communications routers
- d. File server

\_\_\_\_\_ 6. Which of the following is **not** an open communication protocol?

- a. Modbus
- b. Fieldbus
- c. DNP3
- d. HART

# Completion

*Complete the sentence.*

7. A \_\_\_\_\_ network is an industrial network system connecting instruments, sensors, and other devices to a PLC or controller.

8. \_\_\_\_\_ was created in 1979 as a communications protocol for use with PLCs and is now a defacto standard.

# Matching

*Match the major component of an ICS to its function.*

- |   |   |
|---|---|
| A. Control Server                             | E. Intelligent Electronic Devices (Sensors/Actuators) |
| B. SCADA Server or Master Terminal Unit (MTU) | F. Human-Machine Interface (HMI)                      |
| C. Remote Terminal Unit (RTU)                 | G. Data Historian                                     |
| D. Programmable Logic Controller (PLC)        | H. Input/Output (IO) Server                           |

- \_\_\_\_\_ 9. Controllers used at the field level
- \_\_\_\_\_ 10. Hosts DCS or PLC software
- \_\_\_\_\_ 11. Software and hardware used by a person to monitor the state of the process and manage the settings
- \_\_\_\_\_ 12. Devices that convert physical properties to an electronic signal and then perform a physical action
- \_\_\_\_\_ 13. Device that collects, buffers, and provides access to information on subcomponents
- \_\_\_\_\_ 14. Master in a SCADA system

\_\_\_\_\_ 15. Centralized database that logs information received from ICS devices

\_\_\_\_\_ 16. Special purpose data acquisition and control unit device

## Short Answer

17. Address some of the potential challenges with ICS devices.

18. Identify some “best practices” in securing critical infrastructure and key resources (CIKR).

19. Discuss some “best practices” in ICS firewall design.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 4: Risk Management

IV

# **Module 4 Description & Objectives**

16



# Description

This module covers cybersecurity critical infrastructure and risk management. It introduces the NIST Cybersecurity Framework, the structure of the framework, and how it is used. It also describes the processes of risk management in the framework—framework basics, structure, and a business process management approach to implementing and applying the framework.

## Objectives

- Describe basic security service principles (confidentiality, integrity, availability, and authentication) and their relative importance to CI systems.
- Explain basic risk management principles.
- Identify various risk management frameworks and standards, such as the NIST Cybersecurity Framework and the North American Electricity Reliability Council (NERC).
- Describe how to use the framework core process.
- Describe how to use the Framework Implementation Tiers to identify cybersecurity risk and the processes necessary to effectively manage that risk.
- Describe the Cybersecurity Framework Assessment Process Model.
- Demonstrate an understanding of how the framework process holistically manages risk.

# **Module 4 Presentation & Required Reading**

17

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=70>

[Download \[950.35 KB\]](#)

# Required Reading

None


# Module 4 Hands-on Activity

18

There is no hands-on activity for this module.

# Module 4 Team Activity

19

 "Team" by  
Newtown  
grafitti via  
Flickr. CC BY

# Overview

Student teams continue to build a description of the operating environment for their sector-based organization. They select an appropriate risk management framework for the sector-based organization. In the absence of one required by the industry, teams should begin to apply the NIST Cybersecurity Framework to the selected organization. Each team's work should be reviewed by the instructor.

## Team Activity Objectives

- Identify various risk management frameworks and standards, such as the NIST Cybersecurity Critical Infrastructure Framework (“NIST Cybersecurity Framework”) and North American Electricity Reliability Council (NERC).
- Describe how to use the framework core process.

# Assignment

Below are some of the risk management frameworks available. Please select one of them to ensure your team can complete the Team Assignment in Module 7.

- [NIST Framework for Improving Critical Infrastructure Cybersecurity \(“NIST Cybersecurity Framework”\)](#)
- [NIST Special Publication 800-53 Rev 3 and NIST Special Publication 800-53 Rev 3 App I](#)
- [NIST Special Publication 800-53 Rev 4 and NIST Special Publication 800-53 Rev 4 App I](#)
- [Consensus Audit Guidelines \(CAG\)](#)
- [Cyber Resilience Review \(CRR\): Questions Set with Guidance](#)
- [CFATS Risk-Based Performance Standards \(RBPS\): Chemical Facilities Anti-Terrorism Standard, “RBPS 8 – Cyber,” pp. 71-81](#)
- [Committee on National Security Systems \(CNSS\) Instruction No. 1253, Baseline Security Categorization Method](#)
- [Committee on National Security Systems Instruction \(CNSSI\) No. 1253, Security Control Overlays for Industrial Control System \(ICS\), Volume 1](#)
- [DHS Catalog of Control Systems Security: Recommendations for Standards Developers, Revisions 6 and 7](#)
- [TSA Pipeline Security and Incident Recovery Protocol Plan](#)
- [Information Assurance Implementation, \*Department of Defense\*, DODI 8500.2, February 6, 2003.](#)
- [ISO/IEC 15408 revision 3.1: Common Criteria for Information Technology Security Evaluation, Revision 3.1](#)
- [NERC Reliability Standards CIP-002-009 Revisions 3 and 4](#)
- [NIST Special Publication 800-82 Guide to Industrial Control Systems Security, June 2011](#)
- [NIST Special Publication 800-82 Rev 1](#)
- [NIST Special Publication 800-82 Rev 2 \(Draft\)](#)
- [NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Rev 2](#)



- [NRC Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, January 2010](#)
- [Nuclear Energy Institute \(NEI\) 08-09 Cyber Security Plan for Nuclear Power Reactors](#)
- [TSA Pipeline Security Guidelines, April 2011](#)

# Assignment Options

**Option 1:** Write a 2-page abstract summarizing why your team chose your selected risk management framework for your sector-based organization.

**Option 2:** Prepare 2–3 presentation slides on your justification for selecting this risk management framework.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Total Points: 100

# Module 4 Assessment

20

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. NIST developed the Cybersecurity Framework as a mandatory set of standards to manage risks to critical infrastructure.

\_\_\_\_\_ 2. Risk tolerance is the acceptable level of risk a company is willing to take.

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 3. Which of the following is **not** considered a basic security service?

- a. Confidentiality
- b. Authentication
- c. Integrity
- d. Network Security

\_\_\_\_\_ 4. All of the following are standards defined in the NERC CIP standards, except:

- a. Personnel and Training
- b. Sabotage Reporting
- c. Authentication and Access Controls
- d. Recovery Plans for Critical Cyber Assets

\_\_\_\_\_ 5. Continuous Monitoring activities occur under which Framework Core activity?

- a. Identify
- b. Detect
- c. Respond
- d. Protect

\_\_\_\_\_ 6. An impact analysis is a part of which step in the risk management process?

- a. Risk control
- b. Risk assessment
- c. Risk identification
- d. Risk mitigation

\_\_\_\_\_ 7. Which risk handling method reduces the likelihood of the risk occurring to as low as zero?

- a. Mitigation
- b. Avoidance
- c. Transference
- d. Acceptance

# Multiple Response

*Select all the choices that apply.*

\_\_\_\_\_ 8. Which of the following are a part of the Framework Processes?

- a. Framework Implementation Profile
- b. Framework Drivers
- c. Framework Tiers
- d. Framework Core Functions



# Completion

*Complete each sentence.*

9. The Framework \_\_\_\_\_ provide background on how an organization views cybersecurity risk and the processes that are in place to manage that risk.

10. \_\_\_\_\_ is defined as the process of identifying vulnerabilities and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of the information system.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 5: Threats

v

# **Module 5 Description & Objectives**

21

# Description

In cybersecurity, a *threat* is the potential for a negative security event to occur. This module examines common attacks against critical infrastructure including hijacking, denial-of-service attacks, malicious software, SMTP spam engines, Man-in-the-Middle (MITM) attacks, and social engineering. It explores how attacks are being conducted through users, and the different kinds of attacks that target server-side and client-side applications. The module also explores some of the common attacks that are launched against networks, CI and SCADA/Control Systems, and other CI devices today. There is a discussion of how malware is designed and configured, how it works, and the current and future impact of malware on SCADA systems. An overview of how malware like Stuxnet impacts SCADA systems serves as an example.

## Objectives

- Define threats and threat agents, and explain how risk assessment relates to understanding threats.
- Identify how different threats—including hijacking, denial-of-service attacks, malicious software, SMTP spam engines, Man-in-the-Middle (MITM) attacks, and social engineering—would apply to critical infrastructure.
- Identify different types of malware and their intended payloads.
- Describe social engineering psychological attacks.
- List and explain the different types of server-side web application and client-side attacks relevant to critical infrastructure.
- Describe overflow attacks and provide examples of the impact on CI systems.
- Provide examples of malware attacks, such as Flame, Stuxnet, BlackEnergy, Havex, and Duqu, and discuss their functionality

and impact on critical infrastructure systems.

# **Module 5 Presentation & Required Reading**

22

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=82>

[Download \[868.51 KB\]](#)

# Required Reading

U.S. Government Accountability Office (GOA). [\*Critical Infrastructure Protection: Cybersecurity Guidance Is Available But More Can Be Done to Promote Its Use\*](#). GAO-12-92. Published: December 9, 2011. Publicly released: January 9, 2012.



# Module 5 Hands-on Activity

23

There is no hands-on activity for this module.

# Module 5 Team Activity

24



## Overview

Student teams continue to build descriptions of the operating environment for their sector-based organizations. They review the different threat possibilities using the Government Accountability Office (GAO) table, “Sources of Emerging Cybersecurity Threats.” Teams identify the different threats that would be likely to impact their sector-based organizations, providing a rationalization for their selections.

### Team Activity Objectives

- Define threats and threat agents, and explain how risk assessment relates to understanding threats.
- Identify how different threats—including hijacking, denial-of-service attacks, malicious software, SMTP spam engines, Man-in-the-Middle (MITM) attacks, and social engineering—would apply to critical infrastructure.
- Identify different types of malware and their intended payloads.
- Describe overflow attacks and provide examples of the impact on CI systems.
- Provide examples of malware attacks, such as Flame, Stuxnet, BlackEnergy, Havex, and Duqu, and discuss their functionality and impact on critical infrastructure systems.

## Assignment

Review the [Required Reading](#) text, GAO-12-92, *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use*.

Also read the table below, which is a reproduction of Table 1 from the U.S. Government Accountability Office (GOA) report *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, May 2005.

Table 1, Sources of Emerging Cybersecurity Threats. U.S. Government Accountability Office (GOA) r  
*Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling  
Cybersecurity Responsibilities*, May 2005. Available for download from <http://www.gao.gov/products/05-434>.

Look at other resources, like the page “Cyber Threat Source Descriptions” on the ICS-CERT website (<https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions>). Research the operation of at least one of the following malware attacks: Flame, Stuxnet, BlackEnergy, Havex, and Duqu.

How does your review affect the confidentiality, integrity, and availability scores? In addition, are there any organizational concerns that might stem from security incidents that go beyond the impact analysis?

Based on your team’s investigation of your chosen sector and created fictitious organization, select standards from the CSET list “Risk Assessment Standards” (available for download or online viewing below).



Loading...



Taking too long?

↻ Reload document

|

[↶ Open in new tab](#)

One or more interactive elements has been excluded from this version of the text. You can view them online here: <https://textbooks.whatcom.edu/cwwcic/?p=88>

[Download \[296.42 KB\]](#)

# Assignment Options

**Option 1:** Submit a detailed written explanation of how you selected appropriate risk assessment standards for your fictitious organization.

**Option 2:** Prepare 2–3 presentation slides explaining your justification for selecting those particular risk assessment standards.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points 100



# Module 5 Assessment

25

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. An attacker has successfully committed a denial-of-service attack against a website, bringing it down for three hours until network engineers could resolve the problem. This is classified as a threat.

\_\_\_\_\_ 2. Vulnerabilities are weaknesses that allow a threat to occur.

\_\_\_\_\_ 3. Attacks require malicious intent, so they are always caused by people who intend to violate security.

\_\_\_\_\_ 4. Lightning is an example of a threat agent.

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 5. Which of the following is **not** an example of a threat category?

- a. Attacks
- b. Buggy software
- c. Natural event
- d. Human error

\_\_\_\_\_ 6. Which of the following is **not** a threat to critical infrastructure?

- a. Availability of very sophisticated tools that don't require much skill to use
- b. The high-profile nature of critical infrastructure systems
- c. The rapid development of technology of industrial control systems
- d. The interconnected nature of industrial control systems

\_\_\_\_\_ 7. An attacker that breaks into computers for profit or bragging rights is a/an . . .

- a. Cracker
- b. Insider
- c. Terrorist
- d. Hostile country

# Completion

*Complete the sentence.*

8. The types of attacks and attackers specific to a company is known as the threat \_\_\_\_\_.

9. A social engineering attack in which victims are tricked into clicking an emailed link that infects their system with malware or sends their user IDs and passwords to the attacker is known as \_\_\_\_\_.

10. A security control that creates a list of authorized applications, preventing unauthorized applications from downloading and installing, is called a/an \_\_\_\_\_.

# Matching

*Match each threat to its definition.*

- |  |                     |
|--|---------------------|
| A. Denial-of-service (DoS) attack              | F. SQL injection    |
| B. Hijacking                                   | G. Trojan horse     |
| C. Ransomware                                  | H. Virus            |
| D. Distributed denial-of-service (DDoS) attack | I. SMTP spam engine |
| E. Buffer overflow                             | J. Worm             |

\_\_\_\_\_ 11. An attack in which multiple attackers attempt to flood a device

\_\_\_\_\_ 12. Malware that replicates autonomously

\_\_\_\_\_ 13. A web application attack against a connected database

\_\_\_\_\_ 14. Malicious code attached to a file that, when executed, delivers its payload

\_\_\_\_\_ 15. Malware that encrypts the victims files on their computer until money is sent to the attacker

\_\_\_\_\_ 16. An attack that leverages email protocols to send out messages from the infected device

\_\_\_\_\_ 17. An attack that seizes control of communications, sending the communications to the attacker's system

\_\_\_\_\_ 18. An attack in which a single attacker overwhelms a system with a flood of traffic in order to make it unavailable

\_\_\_\_\_ 19. An attack that writes data to unexpected areas of memory, causing the device to crash

\_\_\_\_\_ 20. Malware embedded in what appears to be a useful file

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 6: Vulnerabilities

VI



# **Module 6 Description & Objectives**

26

# Description

Vulnerabilities are weaknesses that enable threats to be actualized. This module discusses cybersecurity vulnerabilities in general and those that are of a higher concern for critical infrastructure systems. It also identifies processes and tools for discovering vulnerabilities.

## Objectives

- Identify the common vulnerabilities associated with Control Systems (CS).
- Identify SCADA cyber vulnerabilities.
- Describe how an attacker may gain control of the SCADA system.
- Define vulnerability assessment and explain why it is important.
- Identify vulnerability assessment techniques and tools, such as CSET, Nessus, and other assessment tools.
- Explain the differences between vulnerability scanning and penetration testing.

# **Module 6 Presentation & Required Reading**

27

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=96>

[Download \[1.79 MB\]](#)

# Required Reading

Parfomak, Paul W. [\*Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options\*](#). CRS Report for Congress, RL33206. Updated September 12, 2008. Available from the Homeland Security Digital Library.

# Module 6 Hands-on Activity

28

There is no hands-on activity for this module.

# Module 6 Team Activity



## Overview

Student teams continue to build a description of the operating environment for their sector-based organization, describing how they would use vulnerability scanning and/or penetration testing to evaluate threat potentials.

### Team Activity Objectives

- Identify vulnerability assessment techniques and tools, such as CSET, Nessus, and other assessment tools.
- Explain the differences between vulnerability scanning and penetration testing.

Having identified threats that would be likely to impact your sector-based organization in the [Module 5 Team Activity](#), consider how you would use vulnerability scanning and/or penetration testing to evaluate additional threat potentials. What tools would you use, and how could they impact the availability of a real-time control and/or SCADA system?

Look for passive penetration tools and tests that will not take the control and/or SCADA systems down.



# Assignment Options

**Option 1:** Write a 2-page abstract summarizing your team's rationale for using vulnerability scanning and/or penetration testing. What tools would your team use, and how could these decisions impact the availability of a real-time control and/or SCADA system?

**Option 2:** Prepare 2–3 presentation slides summarizing your team's rationale for using vulnerability scanning and/or penetration testing. What tools would your team use, and how could these decisions impact the availability of a real-time control and/or SCADA system?

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100

# Module 6 Assessment

30

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. Security testing on SCADA systems, if not performed correctly, can disrupt operations.

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_ 2. Which of the following is **not** a main category of SCADA systems?

- a. Legacy/Proprietary
- b. Modern/Common
- c. Legacy/Common
- d. Modern/Proprietary

\_\_\_\_ 3. Which of the following tests attempts to actually exploit weaknesses in the system?

- a. Vulnerability assessment
- b. Penetration test
- c. Risk assessment
- d. Regression testing

\_\_\_\_ 4. Which of the following is **not** a vulnerability associated with a control system?

- a. Discovery of unique numbers (point reference
- b. Legacy systems that have not been updated

numbers) in  
use

b. Wireless  
access points  
that do not  
provide  
authentication  
to the  
network

d. All are  
vulnerabilities

# Matching

*Match the following assessment tools with their descriptions.*

- A. CSET    D. Wireshark  
B. Nessus   E. Snort  
C. Packet sniffer   F. Nmap/netstat

- \_\_\_\_\_ 5. Popular vulnerability scanner  
\_\_\_\_\_ 6. An intrusion detection system  
\_\_\_\_\_ 7. Used to identify open TCP/UDP ports  
\_\_\_\_\_ 8. DHS tool used to assess an ICS's security posture  
\_\_\_\_\_ 9. Packet sniffing tool  
\_\_\_\_\_ 10. Generic term for a tool used to examine network communications

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 7: Risk Assessments

VII



# **Module 7 Description & Objectives**

31

# Description

This module introduces risk assessment processes and the types of assessments available. Students download the Department of Homeland Security (DHS) CSET tool that was introduced in Module 6. They install it and use it to perform a Cybersecurity Framework Critical Infrastructure Risk Assessment.

## Objectives

- Identify the different risk assessment frameworks.
- Discuss Supply Chain Risk Management (SCRM) principles.
- Explain how regulatory requirements are used in determining additional items to review in a risk assessment.
- Demonstrate an understanding of the CSET tool risk assessment functions.
- Apply the CSET tool to an IT general risk assessment.
- Develop a report using CSET.
- Apply the standard available in the CSET tool to an IT general risk assessment.

# **Module 7 Presentation & Required Reading**

32

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=108>

[Download \[920.96 KB\]](#)

# Required Reading

None

# Module 7 Hands-on Activity



# **Overview**

Students download the Department of Homeland Security (DHS) CSET tool, install it, and use it to perform a Cybersecurity Framework Critical Infrastructure Risk Assessment.

## **Hands-on Activity Objectives**

- Download, install, and run the CSET tool.
- Demonstrate an understanding of the CSET tool risk assessment functions.
- Apply the CSET tool to an IT general risk assessment
- Develop a report using CSET.
- Apply the standard available in the CSET tool to an IT general risk assessment.

# Preparation

Watch some of the video tutorials available to help you better understand how to use the CSET tool. The videos are designed to play within YouTube, so you must have an active Internet connection to view them. You can access these videos by navigating to the CSET YouTube channel, <https://www.youtube.com/c/CSETCyberSecurityEvaluationTool> (link is external). To use close captioning in YouTube, click on the “cc” icon on the video window.



# Downloading CSET onto a PC

## System Requirements

In order to execute CSET, the following minimum system hardware and software is required:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- CD-ROM drive if creating a physical CD
- 5 GB free disk space
- 3 GB of RAM
- Microsoft Windows 7\* or higher
- A Microsoft Office compatible (.docx) document reader is required to view reports in .docx format
- A Portable Document Format (PDF) reader such as Adobe Reader is required to view supporting documentation. The latest free version of Adobe Reader may be downloaded from <http://get.adobe.com/reader/> (link is external).
- Microsoft .NET Framework 4.6 Runtime (included in CSET installation)
- SQL Server 2012 Express LocalDB (included in CSET installation)

**NOTE:** For all platforms, we recommend that you upgrade to the latest Windows Service Pack and install critical updates available from the Windows Update website to ensure the best compatibility and security.

## Downloading CSET

Download CSET using the following link: <http://ics-cert.us-cert.gov/Downloading-and-Installing-CSET>.

After clicking the link, you will be asked to identify yourself and will then be given the opportunity to download the file CSET\_x.x.iso (where x.x represents the download version).

The CSET download is in a file format known as “ISO.” This file is an “image” of the equivalent installation files included on the CSET CD. Because of this format, it is necessary to process the download using one of the following methods:

1. **Decompressing the File** — Open the file using any one of the newer compression utility software programs.
2. **Mounting the File** — This method loads the ISO file using utility software to make the file appear like a virtual drive with the original CD loaded.
3. **Burning the file to CD** — This method uses CD-burn software and the ISO file to burn the files onto your own CD to create a physical disk identical to the CSET original.

These methods require separate software utilities. A variety of both free and purchased utility programs available through the Internet will work with the ISO file format. As DHS does not recommend any specific application or vendor, it will be necessary for you to find a product that provides the necessary functionality. Step-by-step instructions for each method are provided below.

## **Decompressing the File**

1. Click the “Download CSET” link above and complete the requested information to download the ISO file.
2. Save the file to your hard drive of choice (i.e., your computer hard drive or USB drive), maintaining the file name and extension (.iso).
3. Open the ISO file with a compression utility program and save the files to your hard drive of choice, maintaining the original names and file extensions.
4. Complete the “Installing the CSET Program” instructions below.

## **Mounting the File**

1. Click the “Download CSET” link above and complete the requested information to download the ISO file.
2. Save the file to your hard drive of choice (i.e., your computer hard drive or USB drive), maintaining the file name and extension (.iso).
3. Run your ISO-specific utility program that is capable of mounting the file. Complete the instructions within the utility software to create a virtual drive using the ISO file. If you do not have an ISO utility application, you will need to find and install one before continuing with these instructions.
4. Complete the “Installing the CSET Program” instructions below.

## **Burning the file to CD**

1. Click the “Download CSET” link at the bottom of this page and complete the requested information to download the ISO file.
2. Save the file to the hard drive on your computer, maintaining the filename and extension (.iso).
3. Insert a blank, writable CD into the computer’s CD drive.
4. Run your CD-burn utility program. Complete the instructions on your utility program to burn the ISO image to your DVD. (If you do not have an application that can do this, you will need to find and install one before continuing with these instructions.)
5. Complete the “Installing CSET Program” instructions below.

## **Installing the CSET Program**

1. Find the CSET\_Setup.exe file in the folder, virtual drive, or CD containing the CSET files.
2. Double-click the CSET\_Setup.exe file to execute. This will initiate the installer program.

3. Complete the instructions in the installation wizard to install the CSET program.
4. Read the material within the ReadMe document for a summary explanation of how to use the tool. Help is also available through the User Guide, screen guidance text, and video tutorials.

# Using CSET on a Mac

If you are using a Mac, you will need to download Oracle's VM VirtualBox and set up a virtual PC. Then you can download and install CSET on the virtual PC per the above instructions. Here is the download link for VM VirtualBox:

<http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>.

## About Oracle VM VirtualBox

VirtualBox is powerful *Cross-platform Virtualization Software* for x86-based systems. "Cross-platform" means that it installs on Windows, Linux, Mac OS X, and Solaris x86 computers. "Virtualization Software" means that you can create and run multiple virtual machines, running different operating systems, on the same computer at the same time. For example, you can run Windows and Linux on your Mac, run Linux and Solaris on your Windows PC, or run Windows on your Linux systems.

Oracle VM VirtualBox is [available](#) as Open Source or pre-built Binaries for Windows, Linux, Mac OS X, and Solaris.

# Requesting a copy of CSET

If you are unable to download or install CSET from the link, you may request that a copy be shipped to you. To request a copy, please send an email to [cset@hq.dhs.gov](mailto:cset@hq.dhs.gov) (link sends e-mail). Please insert "CSET" in the subject line and include the following in your email request:

- Your name
- Organization name
- Complete street address (no P.O. boxes)
- Telephone number
- The error or installation issue you encountered when attempting the download

# Assignment

Once you have installed CSET, perform a “Screen Print” of your desktop to show that the icon for CSET has been installed. Open a Microsoft Word document and paste the screen print into the document. Save the document and submit it to the instructor.

# Grading Criteria Rubric

1. Proof that the CSET Tool has been downloaded and installed.

Grade points: 100



# Module 7 Team Activity

34



## Overview

Student teams use the CSET tool to produce a risk assessment report for their sector-based organization.

### Team Activity Objectives

- Identify the different risk assessment frameworks.
- Demonstrate an understanding of the CSET tool risk assessment functions.
- Apply the CSET tool to an IT general risk assessment.
- Develop a report using CSET.
- Apply the standard available in the CSET tool to an IT general risk assessment.

# Assignment

Run a CSET Risk Assessment on your team's fictitious organization. Use the standard(s) that apply to your team's sector-based organization, based on your work in the [Module 5 Team Activity](#).

Use the vulnerability assessment plans you developed in the [Module 6 Team Activity](#) to help in your assessment. Import the network diagram your team developed for the [Module 3 Team Activity](#).

Run the CSET tool and follow the steps to perform a risk assessment on your organization infrastructure. Save the Executive Summary of your assessment as proof that you completed this Team Activity.

Student teams submit their CSET Executive Summary PDF Report file to their instructor.

# Grading Criteria Rubric

- Submission of CSET Executive Summary PDF Report file

Grade Points: 100

# Module 7 Assessment

35

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. A risk assessment that uses descriptive terminology, such as “high,” “medium,” and “low,” is called a quantitative risk assessment.

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_ 2. In which phase of the Critical Infrastructure Risk Management Framework is the goal to identify, detect, disrupt, and prepare for hazards and threats; reduce vulnerabilities; and mitigate consequences.

- a. Assess and analyze risk
- b. Establish program goals
- c. Implement risk management activities
- d. Identify assets

\_\_\_\_ 3. \_\_\_\_\_ is a computerized, open-source risk assessment tool that consists of UML-based packages.

- a. OCTAVE
- b. CORAS
- c. CSET
- d. SNORT

\_\_\_\_ 4. \_\_\_\_\_ was developed by Carnegie Mellon as a suite of tools, techniques, and methods for risk-based information security assessment and planning; it utilizes event/fault trees.

- a. OCTAVE
- b. CORAS
- c. CSET
- d. SNORT



# Completion

*Complete the sentence.*

5.

---

\_\_\_\_\_ refers to the logistics associated with obtaining needed components.

## Short Answer

6. Discuss the impact that an industry's regulatory environment might have on risk assessment. Provide an example of a regulation in a sector that would have to be security tested.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 8: Remediation

VIII

# **Module 8 Description & Objectives**

36

# Description

This module covers how to control risk to the network through appropriate remediation techniques. It introduces the concept of the Security Design Life Cycle (SDLC) and the importance of building security in at initiation, rather than “bolting” it on afterwards. In ICS and other SCADA systems, this may not be possible. Foundation guidelines and policies for controlling risk and personnel behavior will be addressed. An enumeration of network protection systems will be provided, including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

The module discusses the importance of digital signatures to providing device authentication, and how vulnerabilities specific to ICS systems relate to remediation techniques. Additionally, it covers common vulnerabilities found in ICS systems and techniques to identify vulnerabilities, as well as remediation techniques.

## Objectives

- Describe how risk management techniques control risk.
- Explain the concept of the Security Design Life Cycle (SDLC).
- List the types of security policies and how these relate to remediation.
- Describe how awareness and training can provide increased security.
- Identify remediation techniques in an ICS network, including routers, firewall technology, and tools for configuring firewalls and routers.
- Describe intrusion detection and prevention systems and web-filtering technologies.
- Explain the importance of digitally signed code for pushes of firmware and other updates to automated devices.

- Demonstrate the ability to evaluate and assess vulnerabilities in ICS networks.
- Explain and make recommendations for remediation strategies in an ICS network.
- Describe the hazards (do and don'ts) of the corporate network process vs. ICS network process.

# **Module 8 Presentation & Required Reading**

37

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=120>

[Download \[1.13 MB\]](#)



# Required Reading

None

# Module 8 Hands-on Activity

38



# Overview

Students download and install a digital certificate.

## Hands-on Activity Objectives

- Demonstrate the ability to research, locate and install a digital certificate.
- Explain the importance of digitally signed code for pushes of firmware and other updates to automated devices.

# Assignment

Research what digital certificates are available for your PC operating system.

Follow procedures for downloading and installing a selected digital certificate. Take screenshots of the steps you follow.

Write a short paper describing your research findings on how to download and install a digital certificate. As attachments to your paper, provide screenshots of the steps you followed to install the digital certificate.

# Grading Criteria Rubric

- Content
- Evidence of download and installation via screenshots
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100

# Module 8 Team Activity

39



## Overview

Based on the risks that teams identified for their sector-based organization's infrastructure in Module 7, student teams identify appropriate security controls to mitigate these risks.

### Team Activity Objectives

- Describe how risk management techniques control risk.
- List the types of security policies and how these relate to remediation.
- Describe how awareness and training can provide increased security.
- Identify remediation techniques in an ICS network including routers, firewall technology, and tools for configuring firewalls and routers.
- Describe intrusion detection and prevention systems and web-filtering technologies.
- Demonstrate the ability to evaluate and assess vulnerabilities in ICS networks.
- Explain and make recommendations for remediation strategies in an ICS network.
- Describe the hazards (do and don'ts) of the corporate network process vs. ICS network process.

Using the CSET tool reports and identification of gaps in security from [Module 7](#), develop a list of controls to be implemented to close the gaps and mitigate these risks.



# Assignment Options

**Option 1:** Write a 2-page abstract summarizing the security controls your team would use to mitigate specific risks, based on the CSET gaps report.

**Option 2:** Prepare 2–3 presentation slides describing the security controls your team would use to mitigate specific risks, based on the CSET gaps report.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100

# Module 8 Assessment

40

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. A device that looks for unusual behavior, such as odd protocols arriving at a server, is known as a signature-based IDS/IPS.

\_\_\_\_\_ 2. Web-filtering based on creating a list of unauthorized sites that may not be accessed is called whitelisting.

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 3. Purchasing cybersecurity insurance to cover losses in the event of a security breach is an example of risk \_\_\_\_\_.

- a. Avoidance
- b. Mitigation
- c. Transference
- d. Acceptance

\_\_\_\_\_ 4. Deciding to delay the implementation of a new system until all security vulnerabilities can be resolved is an example of risk \_\_\_\_\_.

- a. Avoidance
- b. Mitigation
- c. Transference
- d. Acceptance

\_\_\_\_\_ 5. Devices such as Intrusion Detection Systems (IDSs) are considered risk \_\_\_\_\_ strategies as they reduce the impact of the event through early detection.

- a. Avoidance
- b. Mitigation
- c. Transference
- d. Acceptance

\_\_\_\_\_ 6. George has determined that the impact to the business from an internal server hard disk crash would be \$2,000, including three hours of time to rebuild the data from backups. Historically, server drives fail about once every three years. As an option, he could cluster the server (install a second server to act in tandem with the first server) at a cost of \$5,000 for hardware and installation. Assume he has a three-year equipment life cycle so he would have to replace this equipment in three years. Which of the following makes the most sense as a risk strategy?

- |  |   |
|--|---|
| a. Install the second server, as any downtime is bad.                  | c. Avoid using the server until hard drives become more reliable. |
| b. Accept the risk, as it is less expensive than the proposed control. | d. Find a new job. He wasn't hired to be an accountant.           |

\_\_\_\_\_ 7. In the \_\_\_\_\_ phase of the SDLC, the system is performing work, with occasional updates to hardware and software.

- |                            |                              |
|----------------------------|------------------------------|
| a. Initiation              | c. Operations/maintenance    |
| b. Development/acquisition | d. Implementation/assessment |

\_\_\_\_\_ 8. Wiping hard drives and destroying software used with a system occurs at which stage of the SDLC?

- a. Initiation
- b. Disposal
- c. Operations/maintenance
- d. Implementation/assessment

\_\_\_\_\_ 9. Establishing guidelines for including security into contracting language occurs at which stage of the SDLC?

- a. Initiation
- b. Development/acquisition
- c. Operations/maintenance
- d. Implementation/assessment

\_\_\_\_\_ 10. The Gramm-Leach-Bliley Act (GLBA) that established security and privacy safeguards on depositor accounts at financial institutions is an example of what type of security policy?

- a. Regulatory
- b. Advisory
- c. Informative
- d. Issue-specific

\_\_\_\_\_ 11. A device that receives packets that need to be sent out to other networks is known as a/an \_\_\_\_\_.

- a. Firewall
- b. IDS/IPS
- c. Router
- d. Switch

# Completion

*Complete each sentence.*

12. \_\_\_\_\_ risk is the amount of risk that remains after security controls have been applied.



# Matching

*Match the remediation technique/control to an appropriate category.*

- |  |                                     |
|--|-------------------------------------|
| A. Incident Response                   | F. System and Information Integrity |
| B. Personnel Security                  | G. Audit and Accountability         |
|  | H. Monitoring and Reviewing         |
| C. Physical and Environment Security   | Control System Security Policy      |
| D. System and Communication Protection | I. Access Control                   |
| E. Media Protection                    | J. Organizational Security          |

\_\_\_\_\_ 13. Developing a policy for removing access when an employee is terminated

\_\_\_\_\_ 14. Encrypting all sensitive data in transit

\_\_\_\_\_ 15. Implementing an IDS/IPS

\_\_\_\_\_ 16. Installing an uninterruptible power supply (UPS)

\_\_\_\_\_ 17. Enabling logging of all after-hours access

\_\_\_\_\_ 18. Issuing smart cards to users to enable multi-factor authentication

\_\_\_\_\_ 19. Developing a disaster recovery plan (DRP)

\_\_\_\_\_ 20. Establishing a security officer who has oversight of the system

\_\_\_\_\_ 21. Encrypting all backup data

\_\_\_\_\_ 22. Compliance audit

## Short Answer

23. Discuss the difference between role-based security training and security awareness training. What recommendations would you make for how frequently these should occur?

24. You've been asked to implement a firewall. Discuss best practices for configuring a firewall.

25. Discuss the difference between a business network and an ICS network.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 9: Incident Response

IX

# **Module 9 Description & Objectives**

41

# Description

Students learn about Incident Response (IR) strategies, including prevention and containment. They also learn how to create an Incident Response Plan.

## Objectives

- List some common types of incidents that may occur in SCADA/ICS systems.
- Identify the phases of an Incident Response (IR), as described in the NIST SP 800-61.
- Define incident containment and describe how it is applied to an incident.
- Discuss the IR reaction strategies unique to each category of incident.
- Explain the components of an Incident Response Plan.
- Identify the 14 response core capabilities covered in the National Response Framework.

# **Module 9 Presentation & Required Reading**

42

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=133>

[Download \[670.71 KB\]](#)



# Required Reading

Department of Homeland Security (DHS). *Presidential Policy Directive 8: National Preparedness (PPD-8)*. March 30, 2011. Download from <https://www.dhs.gov/presidential-policy-directive-8-national-preparedness>.

Federal Emergency Management Agency (FEMA), Department of Homeland Security (DHS). *National Response Framework*. Third Edition. June 2016. Download from <https://www.fema.gov/media-library/assets/documents/117791>.

Federal Emergency Management Agency (FEMA), Department of Homeland Security (DHS). *National Incident Management System*. Download from [https://www.fema.gov/media-library-data/1467113975990-09cb03e2669b06b91a9a25cc5f97bc46/NE\\_DRAFT\\_NIMS\\_20160407.pdf](https://www.fema.gov/media-library-data/1467113975990-09cb03e2669b06b91a9a25cc5f97bc46/NE_DRAFT_NIMS_20160407.pdf). A copy of the document is also provided below.



Loading...



Taking too long?

↻ Reload document

|

↪ [Open in new tab](#)

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=133>

[Download \[3.06 MB\]](#)

# Module 9 Hands-on Activity

43



# **"hands" Overview**

Students review one NIST case study, either the Olympic Pipeline Explosion or the Maroochy Water Services Incident. They indicate the response steps and describe what went wrong.

## **Hands-on Activity Objectives**

- Identify the 14 response core capabilities covered in the National Response Framework.
- List some of common types of incidents that may occur in SCADA/ICS systems.
- Identify the phases of an Incident Response, as described in NIST SP 800-61.
- Explain the components of an Incident Response Plan.

# Assignment

Download one of the two NIST case studies below.



Loading...



Taking too long?

▢ Reload document

|

[↶ Open in new tab](#)

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=137>

[Download Olympic Pipeline Explosion \[1.14 MB\]](#)

[“Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10 1999.”](#) NTSB/PAR-02/02. PB2002-916502. National Transportation Safety Board.



Loading...



Taking too long?

▢ Reload document

|

[↶ Open in new tab](#)

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=137>

[Download Maroochy Water Services \[150.19 KB\]](#)

This document can also be downloaded from the Internet:  
<https://www.mitre.org/publications/technical-papers/malicious-control-system-cyber-security-attack-case-study-maroochy-water-services-australia>.

Review and assess the case you selected.

Write a short paper describing the response steps and what went wrong in the case study you read.

# Grading Criteria Rubric

- Content
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100



# Module 9 Team Activity

44



## Overview

Teams select one of the risks from their risk assessment and create an Incident Response Plan for their sector-based organization.

### Team Activity Objectives

- Identify the phases of an Incident Response (IR), as described in NIST SP 800-61.
- Define incident containment and describe how it is applied to an incident.
- Discuss the IR reaction strategies unique to each category of incident.

Based on your team's investigation of your chosen sector and fictitious organization, determine which stakeholders to include. Develop a Incident Response Plan document that discusses the steps taken for one of the risks that was identified by your team's CSET Risk Assessment in [Module 7](#).

# Assignment Options

**Option 1:** Write a 2-page abstract summarizing the Incident Response Plan your team has developed.

**Option 2:** Prepare 2–3 presentation slides about your Incident Response Plan.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100

# Module 9 Assessment

45

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 1. Which of the following is **not** a common type of incident in a SCADA/ICS?

- |    |   |   |
|----|---|---|
| a. | Unauthorized access to system controls            | c. Vendor goes out of business and can no longer supply critical components                   |
| b. | A worm infects a network at a nuclear power plant | d. Vendor improperly performs a security assessment, resulting in loss of system availability |

\_\_\_\_\_ 2. In which phase of NIST's SP 800-61 would organizations prioritize response to multiple threat actions?

- |             |             |
|-------------|-------------|
| a.          | c.          |
| Preparation | Containment |
|             | Eradication |

b.  
Detection  
and  
Analysis

and  
Recovery

d. Post-  
Incident  
Activity

# Matching

*Match each core capability of the National Response Framework with its objective.*

- |   |  |
|---|--|
| A. Planning                                 | H. Mass Care Services                        |
| B. Public Information and Warning           | I. Mass Search and Rescue Operations         |
| C. Operational Coordination                 | J. On-Scene Security and Protection          |
| D. Critical Transportation                  | K. Operational Communications                |
| E. Environmental Response/Health and Safety | L. Public and Private Services and Resources |
| F. Fatality Management Services             | M. Public Health and Medical Services        |
| G. Infrastructure Systems                   | N. Situational Assessment                    |

\_\_\_\_\_ 3. Ensure the availability of guidance and resources

\_\_\_\_\_ 4. Relay information on threats and hazards

\_\_\_\_\_ 5. Provide life-sustaining services, including food and shelter

\_\_\_\_\_ 6. Provide communications

\_\_\_\_\_ 7. Establish and maintain an operational structure and process



- \_\_\_\_\_ 8. Provide decision-makers with information
- \_\_\_\_\_ 9. Deliver search and rescue operations
- \_\_\_\_\_ 10. Provide transportation for response
- \_\_\_\_\_ 11. Provide essential services
- \_\_\_\_\_ 12. Engage the community to develop response approaches
- \_\_\_\_\_ 13. Provide lifesaving medical treatment
- \_\_\_\_\_ 14. Stabilize infrastructure
- \_\_\_\_\_ 15. Provide law enforcement and security
- \_\_\_\_\_ 16. Body recovery and victim identification services

*Match the following sections of the ICS Cyber Incident Response Plan with their contents.*

- A. Overview, F. Response Goals, and Actions Objectives
- B. Incident G. Description Communications
- C. Incident Detection H. Forensics
- D. Incident I. Additional Notification Sections
- E. Incident Analysis

- \_\_\_\_\_ 17. Includes media contacts
- \_\_\_\_\_ 18. Incident type classification

- \_\_\_\_\_ 19. Addresses how an incident is prioritized and escalated
- \_\_\_\_\_ 20. Addresses how to evaluate and analyze an incident
- \_\_\_\_\_ 21. Other stuff
- \_\_\_\_\_ 22. Discusses business objectives
- \_\_\_\_\_ 23. The process for collecting, examining, and analyzing incident data, with an eye to legal action
- \_\_\_\_\_ 24. Defines the procedures used for each type of incident
- \_\_\_\_\_ 25. Describes how an incident is identified and reported

## Short Answer

26. Define incident containment and provide an example of how it would be applied to an incident.

27. Discuss how the response strategy for an incident that was sourced from within the organization would differ from one sourced from outside of the organization.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# **Module 10: Policy & Governance**

x

# **Module 10 Description & Objectives**

46

# Description

This module covers policies and governance issues. Topics covered include federal Critical Infrastructure policies and legislation, information sharing of threats among agencies, public/private partnerships, and standards and regulations, as well as compliance. Issues relevant to specific sectors is discussed, such as intellectual property, and the roles of HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and PCI (DSS) are reviewed.

## Objectives

- Identify information-sharing strategies and initiatives as established by the Department of Homeland Security (DHS).
- Describe threat intelligence information sharing among public and private partners, including Information Sharing and Analysis Centers (ISACs).
- Explain the roles that DHS's National Cybersecurity and Communications Integration Center (NCCIC) and National Infrastructure Coordinating Center (NICC) play in infrastructure protection.
- Describe issues relevant to specific critical infrastructure sectors, such as HIPAA and other regulations and laws.

# **Module 10 Presentation & Required Reading**

47

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

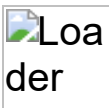
<https://textbooks.whatcom.edu/cwwcic/?p=148>

[Download \[510.62 KB\]](#)



# Required Reading

- Department of Homeland Security. *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. A PDF of this document can be downloaded by clicking the link below or from <https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience>.
- ISAC Council. *INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) AND THEIR ROLE IN CRITICAL INFRASTRUCTURE PROTECTION*. January 2016. PDF available online at [https://docs.wixstatic.com/ugd/416668\\_2e3fd9c55185490abcf2d7828abfc4ca.pdf](https://docs.wixstatic.com/ugd/416668_2e3fd9c55185490abcf2d7828abfc4ca.pdf).
- Congressional Research Service (CRS). *Cybersecurity: Selected Legal Issues*. CRS Report for Congress 7-5700, R42409. April 17, 2013. Available for download in PDF and other digital formats from the Internet Archive at <https://archive.org/details/208169CybersecuritySelectedLegalIssues-crs>.
- Department of Homeland Security. "About the National Cybersecurity and Communications Integration Center." Last Published Date: January 19, 2016. Online at <https://www.dhs.gov/national-cybersecurity-and-communications-integration-center>.
- ThreatConnect. *Threat Intelligence Platforms: Everything You've Ever Wanted to Know But Didn't Know to Ask*. E-book. Arlington, VA: ThreatConnect, 2015. Available for download from <https://www.threatconnect.com/download-ebook/>.



Loading...



Taking too long?

▢ Reload document

|

[↶ Open in new tab](#)

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=148>

[Download NIPP 2013 \(PDF\) \[3.63 MB\]](#)

# Module 10 Hands-on Activity

48

There is no hands-on activity for this module.

# Module 10 Team Activity

49



## Overview

Student teams identify the policy and governance issues for their selected sectors.

### Team Activity Objectives

- Identify information-sharing strategies and initiatives, as established by the Department of Homeland Security (DHS).
- Describe threat intelligence information among public/private partners, including Information Sharing and Analysis Centers (ISACs).
- Explain the roles that DHS's National Cybersecurity and Communications Integration Center (NCCIC) and National Infrastructure Coordinating Center (NICC) play in infrastructure protection.

Based on your team's previous investigations of your chosen sector and fictitious organization, identify the policy and governance issues for your selected sector. Determine what Critical Infrastructure policies and legislation, information sharing of threats among agencies, public/private partnerships, standards and regulations, and compliance requirements would apply to your organization.



# Assignment Options

**Option 1:** Write a 2-page abstract summarizing the governance policies, legislation, partnerships, standards, industry regulations, and compliance requirements that would apply to your sector-based organization.

**Option 2:** Prepare 2–3 presentation slides that share your conclusions concerning governance policies, legislation, partnerships, standards, industry regulations, and compliance requirements.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100



# Module 10 Assessment

50

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 1. \_\_\_\_\_ consists of owners and operators and their representatives, collaborating between government and private sector owners of critical infrastructure.

- |  |   |
|--|---|
| a. Critical Infrastructure Cross-Sector Coordinating Council | c. Regional Consortium Coordinating Council |
| b. Government Coordinating Councils                          | d. Sector Coordinating Councils             |

\_\_\_\_\_ 2. \_\_\_\_\_ is composed of senior officials from federal agencies who facilitate communication and coordination on critical infrastructure security and resilience across the federal government.

- |  |                                      |
|--|--------------------------------------|
| a. Critical Infrastructure Cross-Sector Coordinating Council | c. Federal Senior Leadership Council |
| b. Government Coordinating Councils                          | d. Sector Coordinating Councils      |

\_\_\_\_\_ 3. \_\_\_\_\_ are organizations, including ISACs, that focus on information dissemination and collaboration on a cross-sector basis through a national council.

- |   |  |
|---|--|
| a. Federal<br>Senior<br>Leadership<br>Council | c. Information<br>Sharing<br>Organizations |
| b.<br>Government<br>Coordinating<br>Councils  | d. Sector<br>Coordinating<br>Councils      |

\_\_\_\_\_ 4. Which of the following is **not** one of the NIPP's seven core tenets?

- |   |  |
|---|--|
| a. Identifying<br>and<br>managing<br>risk   | c. Adopting<br>a<br>partnership<br>approach<br>to security<br>and<br>resilience              |
| b. Promoting<br>the public<br>dissemination<br>of an<br>organization's<br>vulnerabilities | d.<br>Promoting<br>security<br>and<br>resilience<br>during<br>design<br>stages of<br>systems |

and  
networks

\_\_\_\_\_ 5. \_\_\_\_\_ is a dedicated 24/7 coordination and information-sharing operations center that maintains situational awareness of the nation's CI, serving as a hub between the government and the private sector when an incident is detected.

- |  |  |
|--|--|
| a. National<br>Infrastructure<br>Coordinating<br>Center<br>(NICC)  | c. Information<br>Sharing<br>Organizations   |
| b.<br>Information<br>Sharing and<br>Analysis<br>Centers<br>(ISACs) | d. National<br>Cybersecurity<br>and<br>Communications<br>Integration<br>Center (NCCIC) |

## Short Answer

6. Define the role of an ISAC in critical infrastructure protection.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 11: Trends

XI

# **Module 11 Description & Objectives**

51

# Description

This module discusses the future of cybersecurity: the Internet of Things (IoT) and how it creates an entirely new set of risks, and emerging technologies like drones, robots, and “wearables.” Increasingly, companies and organizations are exploring a more “active defense” approach to cybersecurity. Traditional incident response—the rapid deployment of a team to remediate breaches to a network, identify additional threats, and restore functionality—is still necessary but is no longer sufficient. The module gives an overview of how the connectedness of our cyber networks demands intelligence-driven tools and processes that equip leaders with an anticipatory edge.

## Objectives

- Identify emerging trends and demonstrate an understanding of emerging technologies.
- Understand the Internet of Things (IoT) and how it expands the cyber “attack surface.”
- Be able to make educated predictions of what the future might look like for the cybersecurity critical infrastructure framework.
- Discuss ethical issues that can arise in relation to new technology and new defense strategies.



# **Module 11 Presentation & Required Reading**

52

# Presentation

One or more interactive elements has been excluded from this version of the text. You can view them online here:

<https://textbooks.whatcom.edu/cwwcic/?p=160>

[Download \[320.41 KB\]](#)

# Required Reading

The President's National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on the Internet of Things*. Nov. 18, 2014. PDF file available for download at <https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf>.

# Module 11 Hands-on Activity

53



# Overview

Individual students write concise reports on a recent trend in the sector they have been studying.

## Learning Objectives

- Identify emerging trends and demonstrate an understanding of emerging technologies.
- Understand the Internet of Things (IoT) and how it expands the cyber “attack surface.”
- Be able to make educated predictions of what the future might look like for the cybersecurity critical infrastructure framework.
- Discuss ethical issues that can arise in relation to new technology and new defense strategies.

Based on your team’s investigation of your chosen sector and created fictitious organization, research recent trends in cybersecurity relevant to your team’s selected sector. Identify at least 5 references on relevant trends.

# Assignment Options

- Write a short paper describing your findings on how these trends will impact your sector.
- Prepare 2–3 presentation slides on your findings on how these trends will impact your sector.

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- References
- Use of American Psychological Association (APA) style in writing the assignment

Grade Points: 100

# Module 11 Team Activity

54





## Overview

Student teams organize the materials on their sector and their fictitious organization into a final presentation to be shared with the class.

### Team Activity Objectives

- Select appropriate vulnerability assessment frameworks and tools as part of a risk assessment of a CI system.
- Identify and describe cybersecurity threats, risks, vulnerabilities, and attacks as they apply to CI systems.
- Identify an appropriate risk management strategy for CISR.

# Assignment

Draw on the past work your team has done on your fictitious organization and its sector:

- Standards and the role of your sector-specific agency, [Module 1 Team Activity](#).
- Industrial control/SCADA and business IT systems used within the organization, [Module 2 Team Activity](#).
- Defense-In-Depth Strategies, [Module 3 Hands-on Activity](#).
- Network diagram, [Module 3 Team Activity](#).
- Risk management framework, [Module 4 Team Activity](#).
- Threat possibilities and risk assessment standards, [Module 5 Team Activity](#).
- Plans for using vulnerability scanning and/or penetration testing, [Module 6 Team Activity](#).
- CSET Risk Assessment, [Module 7 Team Activity](#).
- Security controls to be implemented, [Module 8 Team Activity](#).
- Incidence Response Plan, [Module 9 Team Activity](#).
- Relevant governance and policy issues, [Module 10 Team Activity](#).

Prepare a summary of your team's case study project for the class. Be sure that your team's presentation addresses the following:

- What you discovered about cybersecurity vulnerabilities as they relate to your particular sector
- What mitigation techniques can be used to alleviate these issues
- Suggestions you have for further strengthening your network's security
- The role of government regulation in the functioning of your organization



# Module 11 Assessment

55

# True/False

*Indicate whether the statement is true or false.*

\_\_\_\_\_ 1. Passive defense takes into consideration threat intelligence information that can covertly respond to threat information.

\_\_\_\_\_ 2. Privacy-by-design provides standards for securely collecting and maintaining privacy information, beginning at the point of project initiation.

# Multiple Choice

*Identify the choice that best completes the statement or answers the question.*

\_\_\_\_\_ 3. Attacks continue to evolve. Which of the following is **not** one that was discussed in the presentation?

- a. APTs
- b. Increased attack surfaces associated with the Internet of Things
- c. Increased social engineering attacks
- d. All are evolving threats

\_\_\_\_\_ 4. Which of the following is **not** a problem associated with the Internet of Things?

- a. Sensors might be placed in public locations where they are prone
- b. Protocols have been used for decades and so tend to be unreliable.

to  
tampering.

b. Small  
nature of  
the  
sensors  
makes  
them  
difficult to  
update, or  
patch,  
when a  
problem is  
found.

d. Security  
is not  
usually  
built into  
the  
devices, as  
they are  
considered  
disposable.

# Completion

*Complete the sentence.*

5. An attack in which the attacker has gained access and maintains access for long periods of time before detection is called a/an

\_\_\_\_\_.



## Short Answer

6. The lecture discussed data integrity attacks on power grid or water systems. Identify other critical services that may be vulnerable to a data integrity attack and discuss, generically, how the attack might occur.

7. Discuss at least one of the ethical or privacy issues associated with critical infrastructure protection.

*For the answers to these questions, email your name, the name of your college or other institution, and your position there to [info@cyberwatchwest.org](mailto:info@cyberwatchwest.org). CyberWatch West will email you a copy of the answer key.*

# Module 12: Sector Reports Out

XII

# Sector Reports Out

56

# Description

Each student team presents a summary of its case study project for the class. Team presentations should offer insights into what the students have learned from this course. Depending on the number of teams in the class, it may take more than one class period for all projects to be presented.

## Objectives

- Demonstrate the ability to communicate technical and business information in a presentation format.
- Demonstrate the ability to interact with peers and others.
- Demonstrate that professionalism and soft skills that employers look for in employees.

Team presentations should address the following:

- What the team discovered about cybersecurity vulnerabilities relevant to their particular sector
- What mitigation techniques can be used to alleviate these issues
- Suggestions the team has for further strengthening their network's security
- The role of government regulation in the functioning of their organization

# Grading Criteria Rubric

- Content
- Evidence of teamwork
- Professionalism
- Use of American Psychological Association (APA) style

Grade Points: 100

# Supplemental Materials & Resources

1

## Books

American Psychological Association. [\*Publication Manual of the American Psychological Association\*](#). 16th edition. Washington, DC: American Psychological Association, 2009.

Lewis, Ted G. [\*Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation\*](#), 2nd Ed. Hoboken, NJ: Wiley Publishing, 2015. ISBN 978-1-118-81763-6. The book has a [companion website](#).

Miller, Stephen, and Clark, Richard H. [\*Framework for SCADA Cybersecurity\*](#). Smashwords Edition, eBook ISBN 978-1310-30996-0.

Parfomak, Paul W. [\*Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options\*](#). CRS Report for Congress, RL33206. Updated September 12, 2008.

ThreatConnect. [\*Threat Intelligence Platforms: Everything You've Ever Wanted to Know But Didn't Know to Ask\*](#). E-book. Arlington, VA: ThreatConnect, 2015.

# Videos

*Cyber War: Cybercrimes with Ben Hammersley*. BBC News, 2016. 6 episodes. Videos may be available through the Films on Demand service of [Infobase](#) (check with your insitutional library).



[“Cyber War” link for Whatcom Community College Students.](#)



# Government Resources

[Virtual Learning Portal, Industrial Control Systems Cyber Emergency Response Team](#) (ICS-CERT), Department of Homeland Security. Among the resources available to registered users is the Secure Architecture Design graphic used in the Module 3 Hands-on Activity.

[Industrial Control Systems Cyber Emergency Response Team](#) (ICS-CERT), Department of Homeland Security. Instructor-led and web-based training events on industrial control systems cybersecurity.

# Online Training and Tools

[CSET risk assessment tool](#). The Cyber Security Evaluation Tool (CSET) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed by cybersecurity experts under the direction of the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Also available is a [fact sheet on CSET](#).

[Oracle VM VirtualBox](#). This cross-platform virtualization software makes it possible to set up a virtual PC on a Mac so you can install and run CSET. Documentation in [how to use VirtualBox](#) is also available.

[SCADA Hacker's Toolset](#). This webpage lists online resources and tools for control system security testing and is published by Joel Langill, the Director of Critical Infrastructure and SCADA representative for the Cyber Security Forum Initiative.

[VMware Workstation](#). This application makes it possible to run multiple operating systems as virtual machines on a single PC. A free trial of the software can be obtained by clicking the "Get Free Trial" option under Product Resources.

# Textbook Mapping

2

The following textbook has been mapped to the course modules. Instructors may want to assign specific chapters in addition to the texts listed as Required Reading. Supplemental PowerPoint slides and videos to accompany *Critical Infrastructure Protection in Homeland Security* are available online here:

<http://www.wiley.com//legacy/wileychi/lewis/>.

***Critical Infrastructure Protection in Homeland Security:  
Defending a Networked Nation***

2nd Ed.

Ted G. Lewis

Wiley Publishing

978-1-118-81763-6

| Module #  | Concepts   | Chapter      |
|---|--|--------------|
| Module 1 –<br>Introduction<br>to Critical<br>Infrastructure | <ul style="list-style-type: none"><li>• Define critical infrastructure, protection, and resilience in the context of the National Infrastructure Protection Plan (NIPP).</li><li>• Describe critical infrastructure in communities and the impact Lifeline sector assets have on a community's resiliency.</li><li>• Describe the processes that support critical infrastructure security and resilience.</li><li>• Identify strategies and methods for achieving results through critical infrastructure partnerships.</li><li>• Describe the roles and responsibilities of entities such as the DHS, sector-</li></ul> | Chapter<br>1 |

specific agencies, and state, local, tribal, and territorial governments.

- Discuss common standards bodies, such as the North American Electricity Reliability Council (NAERC) and the National Institute of Standards and Technology (NIST).
- Understand which certifications are required to protect critical infrastructure.

**Module 2 –  
Introduction  
to Control  
Systems &  
SCADA**

Chapter  
10

- Describe the components and applications of industrial control systems.
- Describe the purpose and use of SCADA, DCS, and PCS systems.
- Describe the configuration and use of field devices used to measure critical infrastructure processes, such as flow rate, pressure, temperature, level, density, etc.
- Describe the use and application of Programmable Logic Controllers (PLCs) in automation.

**Module 3 –  
Technologies**

Chapter  
6

- List several types of networking hardware and explain the purpose of each.
- List and describe the functions of common communications protocols and network standards used within CI.
- Identify new types of network applications and how they can be secured.

- Identify and understand the differences between IPv4 and IPv6.
- Discuss the unique challenges/characteristics of devices associated with industrial control systems.
- Explain how existing network administration principles can be applied to secure CIKR.

**Module 4 –  
Risk  
Management**

Chapter  
2

- Describe basic security service principles (confidentiality, integrity, availability, and authentication) and their relative importance to CI systems.
- Explain basic risk management principles.
- Identify various risk management frameworks and standards, such as the NIST Cybersecurity Framework and the North American Electricity Reliability Council (NERC).
- Describe how to use the framework core process.
- Describe how to use the Framework Implementation Tiers to identify cybersecurity risk and the processes necessary to effectively manage that risk.
- Describe the Cybersecurity Framework Assessment Process Model.
- Demonstrate an understanding of how the framework process holistically manages risk.

## **Module 5 – Threats**

- Define threats and threat agents, and explain how risk assessment relates to understanding threats. Chapter 7
- Identify how different threats—including hijacking, denial-of-service attacks, malicious software, SMTP spam engines, Man-in-the-Middle (MITM) attacks, and social engineering—would apply to critical infrastructure.
- Identify different types of malware and their intended payloads.
- Describe social engineering psychological attacks.
- List and explain the different types of server-side web application and client-side attacks relevant to critical infrastructure.
- Describe overflow attacks and provide examples of the impact on CI systems.
- Provide examples of malware attacks, such as Flame, Stuxnet, BlackEnergy, Havex, and Duqu, and discuss their functionality and impact on critical infrastructure systems.

## **Module 6 – Vulnerabilities**

- Identify the common vulnerabilities associated with Control Systems (CS).
- Identify SCADA cyber vulnerabilities.
- Describe how an attacker may gain control of the SCADA system.
- Define vulnerability assessment and explain why it is important.
- Identify vulnerability assessment techniques and tools, such as CSET, Nessus, and other assessment tools.

- Explain the differences between vulnerability scanning and penetration testing.

## **Module 7 – Risk Assessments**

Chapter  
12

- Identify the different risk assessment frameworks.
- Discuss Supply Chain Risk Management (SCRM) principles.
- Explain how regulatory requirements are used in determining additional items to review in a risk assessment.
- Demonstrate an understanding of the CSET tool risk assessment functions.
- Apply the CSET tool to an IT general risk assessment.
- Develop a report using CSET.
- Apply the standard available in the CSET tool to an IT general risk assessment.

## **Module 8 – Remediation**

- Describe how risk management techniques control risk.
- Explain the concept of the Security Design Life Cycle (SDLC).
- List the types of security policies and how these relate to remediation.
- Describe how awareness and training can provide increased security.
- Identify remediation techniques in an ICS network, including routers, firewall technology, and tools for configuring firewalls and routers.
- Describe intrusion detection and prevention systems and web-filtering technologies.

- Explain the importance of digitally signed code for pushes of firmware and other updates to automated devices.
- Demonstrate the ability to evaluate and assess vulnerabilities in ICS networks.
- Explain and make recommendations for remediation strategies in an ICS network.
- Describe the hazards (do and don'ts) of the corporate network process vs. ICS network process.

---

---

## **Module 9 – Incident Response**

- List some common types of incidents that may occur in SCADA/ICS systems.
- Identify the phases of an Incident Response (IR), as described in the NIST SP 800-61.
- Define incident containment and describe how it is applied to an incident.
- Discuss the IR reaction strategies unique to each category of incident.
- Explain the components of an Incident Response Plan.
- Identify the 14 response core capabilities covered in the National Response Framework.

## **Module 10 – Policy & Governance**

- Identify information-sharing strategies and initiatives as established by the Department of Homeland Security (DHS).



- Describe threat intelligence information sharing among public and private partners, including Information Sharing and Analysis Centers (ISACs).
- Explain the roles that DHS's National Cybersecurity and Communications Integration Center (NCCIC) and National Infrastructure Coordinating Center (NICC) play in infrastructure protection.
- Describe issues relevant to specific critical infrastructure sectors, such as HIPAA and other regulations and laws.

## **Module 11 – Trends**

- Identify emerging trends and demonstrate an understanding of emerging technologies.
- Understand the Internet of Things (IoT) and how it expands the cyber “attack surface.”
- Be able to make educated predictions of what the future might look like for the cybersecurity critical infrastructure framework.
- Discuss ethical issues that can arise in relation to new technology and new defense strategies.

# Sample Syllabus

3

Download a Microsoft Word document of this sample syllabus by clicking the link below.

One or more interactive elements has been excluded from this version of the text. You can view them online here:  
<https://textbooks.whatcom.edu/cwwcic/?p=175>

[Download \[50.86 KB\]](#)