

Course Number: XXXX

Critical Infrastructure Protection: The Cyber Dimension

University of XXXXXX

Fall/Spring Semester 20XX

NAME OF SCHOOL:

DEPARTMENT:

PROGRAM:

PROFESSOR:

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

COURSE DESCRIPTION/OVERVIEW:

This course provides a careful examination of the methods necessary to identify and address risks to critical information infrastructures from a variety of human and natural threats. Information infrastructures, comprised of communication networks, computers, databases, management, applications, and consumer electronics, are an essential part of the global critical infrastructure and an integral part of our Nation's economy and national security. What was once a concern of providing security to individual computers now stretches into the realm of providing security for protection of international and national infrastructures from known and unknown human and natural threats.

In order to effectively protect critical infrastructures, governments, infrastructure owners and operators, academia, and technology and policy communities must be able to individually and collectively manage risks by identifying them and determining what is the most effective and feasible operational or strategic approach(es) to address them. Effective protection requires public-private partnerships, both nationally and internationally, between government, law enforcement, industry owners and operators and their respective communities/associations, academia, and other public sector stakeholders, to create and provide a collaborative environment in which complex risks can be addressed. These efforts contribute to a mature, sustainable critical infrastructure protection security program that can better protect operations and assets, minimize recovery time in the event of an attack or natural disaster, identify attack

sources, and provide for successful investigations when attacks occur. The ability to effectively investigate and operate as well as securely communicate, disseminate, and share information will distinguish between success and failure.

The need for professionals in the field of critical infrastructure protection and specifically information infrastructures will only increase as economies and governments become more reliant on information and communication infrastructure. The goal of this course is to produce a more-educated professional with areas of expertise not only in technology and infrastructure protection, but also in law enforcement, policy and law, and cyber forensics. Expertise in any of these areas will be necessary to provide the workforce with the capabilities to overcome the current threats and vulnerabilities to our Nation's cyber infrastructure.

Today's law enforcement or homeland security professional must be able to integrate cybersecurity into their problem solving approaches. These professionals will need baseline technical understanding to safely and securely collect, process, and share intelligence from organizational units across networks, to make intelligent tactical and strategic decisions, and successfully resolve investigations, operations, and prosecutions.

CREDITS CONFERRED: 3

PREREQUISITE: Introduction to Critical Infrastructure Protection and Resilience

LEARNER OUTCOMES/OBJECTIVES (AS MAPPED AGAINST DEPARTMENT OF HOMELAND SECURITY CRITICAL INFRASTRUCTURE CORE COMPETENCIES):

This course is designed to enable learners to:

- 1.** Identify and describe the various components and their functions of the Critical Infrastructure Competency Model, relating to cybersecurity and the protection of information infrastructures.
- 2.** Describe the elements of risk analysis as it pertains to the protection of information infrastructures.
- 3.** Describe the various measures/mitigation and countermeasure strategies utilized to protect information infrastructures.
- 4.** Demonstrate an understanding of the partnership and network building roles and responsibilities of all critical infrastructure partners.
- 5.** Describe the various methods of collecting analyzing and disseminating information (information sharing) amongst critical infrastructure partners.
- 6.** Define and establish program goals and objectives in order to sustain the growth and maturity of a private sector and/or government information security program.

7. Define and establish the collection of metrics necessary to support private sector and/or government information security program objectives by examining public-private sector best practices.

8. Describe the technical and tactical cybersecurity subject-matter expertise necessary to allow professionals to problem solve issues within their respective sectors.

DELIVERY METHOD:

Learners will be provided with course materials through lectures with class participation and discussion, course readings as directed, a research project, and a table-top cybersecurity exercise. Learners are expected to attend all scheduled classes. Learners are responsible for knowing everything that is announced, discussed, or lectured upon in class as well as mastering all assigned reading. Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and multiple perspectives. Learners are also responsible for submitting all assignments, tests, recitations, and unannounced quizzes on time. If a learner misses a class it is their responsibility to get any information provided in class from another learner. At the graduate level, learners are expected to be able to work independently.

The course is designed to be delivered in a typical 15-week semester format (approximately 40-45 hours). The course can be easily adapted to be delivered in alternative formats to include half-semester (7-8) weeks, one week, and through distance learning.

GENERAL COURSE REQUIREMENTS:

1. Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.
2. It is expected that assignments will be turned in on time (the beginning of the class in which they are due). However, it is recognized that learners occasionally have serious problems that prevents work completion. If such a dilemma arises, please speak to the professor in a timely fashion.
3. The completion of all readings assigned for the course is assumed. Because the class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class.
4. According to university policy, all beepers and cell phones should be turned off before class begins.

GRADING:

Learners will be assessed on their post course knowledge through written research and practical exercises/projects. Learners will be required to achieve a passing grade in order to receive credit for completing the course.

Class Participation	15%
Table-Top Security Incident Review	30 %
Research Paper	30 %
Peer Reviews	10 %
Class Presentation	15 %
Total	100 %

ACTIVITIES, EXERCISE, AND RESEARCH PROJECTS:

1. Research Project (30%)

Being able to express yourself verbally and on paper is an important aspect of any career. Equally important is the ability to accept constructive criticism of your work and to constructively review the work of others. Each learner will pick a specific critical infrastructure topic area with cybersecurity as a key component and will discuss how it impacts our national security. The successful research paper will have original ideas and concepts supported by empirical research. Do not be afraid to explore controversial areas and ideas; just be able to support them. The research project is designed to make the learner critically think in regards to their topic area and not just provide a historical perspective. The research component for this class will be in four phases.

Phase 1: Each learner will submit a draft research paper in electronic format.

Phase 2: Each learner will prepare a written peer review of at least three other learners’ research papers. The following instructions will be used as a guide in completing the peer reviews.

Peer Review Instructions:

The reviewer should read the paper(s) assigned to them twice, once to get an overview of the paper, and a second time to provide constructive and professional criticism for the author to use when revising his/her paper. The goals of peer review are to help improve your classmate's paper by pointing out strengths and weaknesses that may not be apparent to the author, and to help improve editing skills. The review should provide the following information and answer the following questions:

Author _____ Reviewer _____

Organization:

- Were the basic sections (Abstract, Introduction, Conclusion, References, etc.) adequate? If not, what is missing?
- Did the writer use subheadings well to clarify the sections of the text? Explain.
- Was the material ordered in a way that was logical, clear, and easy to follow? Explain.

Citations:

- Did the writer cite sources adequately and appropriately? Note any incorrect formatting.
- Were all the citations in the text listed in the Literature Cited section? Note any discrepancies.

Grammar and Style:

- Were there any grammatical or spelling problems?
- Was the writer's writing style clear? Were the paragraphs and sentences cohesive?

Content:

- Did the writer adequately summarize and discuss the topic? Explain.
- Did the writer comprehensively cover appropriate materials available from the standard sources? If no, what's missing?
- Did the writer make some contribution of thought to the paper, or merely summarize data or publications? Explain.

Phase 3: Each learner will prepare and deliver an oral presentation of their research. Audience will be able to ask questions of the presenter.

Phase 4: Each learner will submit a final copy of their research paper. The learner will incorporate changes based on peer reviews and feedback from presentations.

Each phase of the research project will be graded as follows:

Phase 1 and Phase 4 – 100 points

Phase 2 – 60 points (20 points per review)

Phase 3 – 50 points

Total: 210 points

All submitted work **MUST** be the original work of the learner.

A. Paper Requirements:

- Each learner will be required to write and submit a research paper.
- Topic must have the cybersecurity aspect of a critical infrastructure area as a key component
- Topic must be approved.
- Paper must be 12-15 pages in length.

- At least 10 references must be utilized
- Paper must have an abstract (not included in page count)
- Paper must have a reference page (not included in page count)

B. Grading Guidelines for Papers

Content:

- Substance of the material/references
- Relevance of topic
- Inclusion of all necessary information
- Organization of argument

Grammar/Spelling:

- Complete sentences
- Proper usage of vocabulary
- Grammatical correctness
- Spelling

Structure

- Format
- Margins
- Headings
- Abstract page
- Reference page

2. Tabletop Incident Response Project (30%)

The objective of this exercise is to develop hypothetical security incident response scenarios to assist organizations in assessing their level of preparedness and ability to respond to security incidents. The class will be divided into teams of 3-4 learners for this exercise. Each team will develop a scenario, which details a realistic, but hypothetical, cyber based attack against an organization or multiple organizations within one of the critical infrastructure sectors. The scenario must have a minimum of three “injects” designed to build on the scenario. An “inject” is a new element introduced into the scenario, such as a new attack vector or the outcome of an attack. Each team will submit a written paper detailing their scenario. The team will then lead the class through a tabletop discussion and review of their scenario.

Learners will be familiarized with The Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP is a capabilities and performance-based exercise program that provides a standardized methodology and terminology for exercise design, development, conduct, evaluation, and improvement planning. The Homeland Security Exercise and Evaluation Program (HSEEP) constitutes a national standard for all exercises and is maintained by the Federal Emergency Management Agency’s National Preparedness Directorate, Department of

Homeland Security. Learners will be required to complete the online tutorial IS-120.a “An Introduction to Exercises” located at <http://training.fema.gov/EMIWeb/IS/IS120A.asp>. Due to time constraints, learners will not be required to stringently adhere to the standards as described in the training, but should be familiar enough with them to develop and deliver a professional project in the timeframe allotted.

The Tabletop Security Incident Response Scenario Development Project will be graded as follows:

Written Paper – 25 points
Tabletop – 25 points
Total: 50 points

Grading Guidelines for Scenario Papers:

- Substance of the material/references
- Relevance of topic
- Inclusion of all necessary information

Reference page (if necessary)

INCORPORATION OF FEEDBACK:

Performance measures consist of a formal Program Evaluation & Assessment participant evaluation. All course participants will evaluate the overall course presentation, instructor, and the applicability to their work, if applicable. Participants are given evaluations at the beginning of the course so that they may add comments at any time. Evaluation results drive revisions, corrections, additions, and modifications to existing content, as well as individual instructors. Learner and faculty evaluations are a major component in rating the overall effectiveness of courses with respect to learner’s post course knowledge. The Instructor will lead class participants in course debriefs in order to determine the general level of the learner’s understanding of the material presented. Based on this data, course materials will be updated and made relevant on an on-going basis.

COURSE TEXTBOOKS:

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003. ISBN: 1-55558-306-7.

Volonino, Linda and Robinson, Stephen R., *Principles and Practice of Information Security*, Pearson Prentice Hall, 2004. ISBN: 0-13-184027-4.

RECOMMENDED RESOURCES FOR PAPER TOPICS:

Black Hat: <http://www.blackhat.com/>

The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, Cybersecurity: http://cip.gmu.edu/archive/CIPHS_TheCIPReport_January2011_Cybersecurity.pdf

DEF CON: <http://www.defcon.org/>

Georgetown University's Institute for Law, Science, and Global Security Cyber Project:

<http://lsgs.georgetown.edu/programs/CyberProject/>

Events: <http://lsgs.georgetown.edu/events/>

IEEE: <http://www.ieee.org/index.html>

International Telecommunications Union, Cybersecurity: <http://www.itu.int/cybersecurity/>

International Telecommunications Development Sector, Cybersecurity:

<http://www.itu.int/ITU-D/cyb/cybersecurity/>

The Internet Engineering Task Force (IETF): <http://www.ietf.org/>

NATO Cooperative Cyber Defence Centre of Excellence: <http://www.ccdcoe.org/>

National Defense University's Center for Technology and National Security Policy (CTNSP):

Cyber Security Seminars:

<http://www.ndu.edu/CTNSP/index.cfm?secID=22&pageID=2&type=section>

National Security Threats in Cyberspace: A Workshop Jointly conducted by the American Bar

Association Standing Committee on Law and National Security and National Strategy Forum:

http://www.americanbar.org/content/dam/aba/migrated/natsecurity/threats_in_cyberspace.authcheckdam.pdf

RSA Conference: <http://www.rsaconference.com>

Critical Infrastructure Blog: <https://365.rsaconference.com/blogs/critical-infrastructure>

Workshop on Economics of Information Security (WEIS):

WEIS 2011: <http://weis2011.econinfosec.org/index.html>

Past Workshops: <http://weis2011.econinfosec.org/past.html>

COURSE OUTLINE:

LESSON 1 TOPIC: INTRODUCTION TO INFORMATION INFRASTRUCTURE PROTECTION

1. Lesson Goals/Objectives:

- Introduction of course requirements, instructional methodology, evaluation criteria, and feedback processes
- Explanation of course projects: Research Project, and Tabletop Security Incident Response Scenario Development Project
- Become familiar with the various statutes and Presidential policy documents governing the application of National Cybersecurity in the United States
- Define key terms as they relate to cybersecurity and infrastructure protection
- Understand the evolution of cybersecurity strategy as a national policy
- Understand the significance that cybersecurity plays in regards to our economic health and national security
- Discuss how existing cybersecurity programs and initiatives are going to evolve in the future and the influence they will have on our national standing

2. Discussion Topics:

- What are the definitions of cyber infrastructure, information technology, information infrastructure, and cybersecurity? How are they alike and how are they different?
- Why is cybersecurity one of the most challenging issues we face in regards to our economy and national security?
- Have our Nation's cybersecurity strategies done enough to extend cyber protections into the critical infrastructure sectors?
- Are current U.S. cybersecurity programs designed to keep pace with fast changing, quick growth technology?
- What are the differences between and what are the strengths and weaknesses of the various Presidential policies focused on cybersecurity and critical infrastructure.
- Have industry compliance standards kept pace with the need for cybersecurity?

3. Required Reading:

United States Department of Homeland Security, National Infrastructure Protection Plan, 2009, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. Pages 1-15

Appendix 1: Special Considerations, Appendix 1A: Cross-Sector Cybersecurity, Pages 113-123.

The Comprehensive National Cybersecurity Initiative, 2010,

<http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

Volonino, Linda and Robinson, Stephen R., *Principles and Practice of Information Security*, Pearson Prentice Hall, 2004, Chapter 1.

Congressional Research Service Report, *Critical Infrastructures: Background, Policy, and Implementation*, June 2010, http://assets.opencrs.com/rpts/RL30153_20100607.pdf.

National Strategy for Trusted Identities in Cyberspace (2011):
http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

White House Cybersecurity Legislative Proposal (2011):
<http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf>.

International Strategy for Cyberspace (2011):
http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

Cyberspace Policy Review (Obama Administration):
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

LESSON 2 TOPIC: INTERNET AND NETWORK TECHNOLOGY

The way information is transmitted between people and machines today was science fiction 30 years ago. The latter half of the 20th century was known as the space age but this has morphed into the Information Age that we now live in. “Knowledge is power” is an old saying that still applies today; those who know how to harness knowledge are the most powerful. Just as war fueled the arms race, today technology is fueling the information command and control race. As software developers write new applications to enhance the cyber-experience, criminals and terrorists are constantly seeking new ways to exploit the technology. A thorough understanding of how and why the Internet works will give you the necessary background to enable you to conduct investigations and operations on the Internet in a more effective and safe manner.

1. Lesson Goals/Objectives:

- Describe the Internet and its fundamental governing elements
- Define the role of TCP/IP in Internet Communications as well as Internet Protocol (IP) addressing technology
- Describe complexities associated with product and service development as well as their associated response requirements and challenges
- Describe the various connection and hardware devices utilized by networks
- Define the Internet software structure
- Understand and describe the critical functions and sub-functions that producers/providers of IT hardware, software and services have defined. The functions are as follows and can be found in the IT Sector-Specific Plans from 2007 and 2010:
 - Produce and provide IT products and services
 - Provide incident management capabilities
 - Provide domain name resolution services
 - Provide identity management and associated trust support services;
 - Provide Internet-based content, information, and communications services
 - Provide Internet routing, access, and connection services

2. Discussion Topics:

- What are the basic components of the Internet and its associated technologies?
- How does information transit the Internet? What is the name of this protocol?
- Why is it important to understand the basic components of Internet technology when working in or studying the cybersecurity field?

3. Required Reading:

Warriors of the Net Internet video, <http://www.warriorsofthe.net/index.html>.

After Action Reports for Cyber Storm I, Cyber Storm II, and Cyber Storm III (if published):

Cyber Storm I: http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf.

Cyber Storm II: http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf.

Cyber Storm III Fact Sheet:

<http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf>.

IT Sector-Specific Plan 2007: <http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech.pdf>.

LESSON 3 TOPIC: CYBERSECURITY BASICS

Project Due Date: Must have research paper topic approved by this lesson

1. Lesson Goals/Objectives:

- Understand the meaning of Information Assurance (IA)
- Understand what components comprise an information infrastructure
- Understand the three principles of Defense-in-Depth
- Understand the role that access control plays in cybersecurity
- Understand the three concepts of access control: security policy, accountability, and assurance

2. Discussion Topics:

- What is meant by information assurance?
- What is access control? What are reasons why we need access control?
- What is an information infrastructure? What are the different components that can comprise an information infrastructure? At what level can an information infrastructure exist?
- Explain the three principal aspects of defense-in-depth. If one layer of the defense is unsuccessful in stopping an attack, do the other layers fail also?
- What are the three concepts of access control?

3. Required Reading:

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 2 and 3.

LESSON 4 TOPIC: SECURITY AND PRIVACY

1. Lesson Goals/Objectives:

- Define Security
- Define Privacy
- Understand the 4th amendment as it pertains to an individual's right to privacy
- Understand what is meant by expectation of privacy
- Understand privacy and compliance issues

2. Discussion Topics:

- What is the difference between security and privacy?
- Do individuals have the right to security and/or privacy? If so from whom?
- What guarantees that right?
- What is an expectation of privacy? Is it a guaranteed right?
- Explain how *Katz v. United States* is associated with an individual's expectation of privacy?
- What types of information are protected under compliance statutes and what are the statutes?

3. Required Reading:

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 1.

Volonino, Linda and Robinson, Stephen R., *Principles and Practice of Information Security*, Pearson Prentice Hall, 2004, Chapter 11.

Cornell University Law School, 4th Amendment,
http://www.law.cornell.edu/anncon/html/amdt4toc_user.html.

Katz v. United States:
http://www.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZS.html.

LESSON 5 TOPIC: CYBERSECURITY THREATS, VULNERABILITIES, AND RISK

1. Lesson Goals/Objectives:

- Understand the major elements of risk in the context of critical infrastructure
- Understand the type and severity of cyber threats
- Understand the meaning of vulnerability in respect to the cyber domain
- How to determine an organization's risk using threat and vulnerability data
- Understand the key concepts of performing audits against your Information infrastructure

2. Discussion Topics:

- What are the major elements of risk as they pertain to the critical infrastructure mission?
- Define the term threat and what are some examples?
- From the cyber perspective, what types of threats would we need to be aware of?
- Define the term vulnerability and give some examples?
- How do we determine our risk in regards to our cyber infrastructure?
- How do we mitigate such risk?
- What is meant by the term vulnerability assessment? Penetration testing? Audits?
- How are audits used to help mature and sustain an organization's security program?
- Introduction to Tabletop exercises

3. Required Reading:

National Infrastructure Protection Plan 2009, Chapter 3 and Appendix 3.

Volonino, Linda and Robinson, Stephen R., *Principles and Practice of Information Security*, Pearson Prentice Hall, 2004, Chapter 3.

Rittinghouse, John W. and Hancock, William M., *Cybersec.urity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 2, 3, and 14.

IS-120.a An Introduction to Exercises interactive web-based course,
<http://training.fema.gov/EMIWeb/IS/IS120A.asp>.

LESSON 6 TOPIC: CYBER OPERATIONS SECURITY (OPSEC)

1. Lesson Goals/Objectives:

- Define operations security (OPSEC) and cyber operations security (OPSEC).
- Describe the OPSEC method
- Describe the five elements of the OPSEC process
- Define the term indicator and how it applies to operations security in the cyber world.
- Define the term countermeasures and how it applies to operations security in the cyber world.

2. Discussion Topics:

- What are the definitions of the terms OPSEC and Cyber OPSEC
- How does Cyber OPSEC differ from OPSEC?
- Explain the various stages of the OPSEC process
- What are indicators?
- What is a countermeasure used for? How would we apply this to the cyber domain?
- Which critical infrastructure sectors would OPSEC apply to?

3. Required Reading:

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 3.

National Security Decision Directive 298, <https://www.iad.gov/ioss/media/pdf/nsdd298.pdf>.

LESSON 7 TOPIC: ENCRYPTION, KEYS, SIGNATURES, AND PUBLIC KEY INFRASTRUCTURE (PKI)

Project Due Date: Draft of Research Paper due by end of this lesson

1. Lesson Goals/Objectives:

- Understand cryptography and why it is needed in the cyber domain
- Identify the types of cryptography
- Understand the concept of public-private key cryptography
- Understand the function of digital signatures
- Understand cryptanalysis and cryptographic attack techniques
- Understand the concept of steganography
- Define the process of encrypting and decrypting data
- Understand the function of digital certificates

2. Discussion Topics:

- Is encryption a key solution to deterring cyber attacks?
- What is the difference between a digital signature and a digital certificate?
- Is the process the same for encrypting data as it is for decrypting data? What are some of the different processes involved?
- How does public-private key encryption work and why is it so strong?
- Define steganography and its association with covert channels.
- Can encryption be cracked? If so by whom?

3. Required Reading:

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 7 and 8.

LESSON 8 TOPIC: CYBERSECURITY AND SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) VULNERABILITIES

1. Lesson Goals/Objectives:

- Understand the nature of the cyber threats in relation to SCADA and SCADA Vulnerabilities
- Understand the challenges represented by information technology and SCADA systems vulnerabilities
- Understand how SCADA is a prevalent technology within most critical infrastructure sectors

2. Discussion Topics:

- What are the principal threats and challenges of cybersecurity as they pertain to SCADA? Is this a — real and present danger? Why or why not?
- What is SCADA? How do cyber and SCADA concerns relate to the critical infrastructure sectors? How are the sectors structured to deal with this evolving threat?
- How do the various critical infrastructure sectors address the issues of cyber and SCADA vulnerabilities?
- How does each critical infrastructure party communicate and coordinate with the others to jointly address cyber risk and SCADA vulnerabilities?

3. Required Reading:

U.S. Government Accountability Office, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, <http://www.gao.gov/new.items/d04354.pdf>.

Stouffer, Falco, and Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrialized Control Systems Security*, 2006, Chapter 1-4.
<http://cs-www.ncsl.nist.gov/groups/SMA/fisma/ics/documents/DraftSP800-82.pdf>.

LESSON 9 TOPIC: CYBER CRIME AND CYBER TERRORISM AND CYBER WARFARE

Project Due Date: Peer reviews are due by the end of this lesson

1. Lesson Goals/Objectives:

- Understand computer crime and computer related crime
- Understand the concept of computers as targets of crime
- Understand the concept of computers as instruments of crime
- Understand what is meant by cyber terrorism vs. terrorist use of cyber technology to further their goals
- Understand the concept of cyber warfare

2. Discussion Topics:

- What is the definition of a cyber crime? Are there any new crimes created by computers?
- What is meant by a computer related crime?
- Which is more common, the computer crime or the computer related crime?
- Explain the difference between a computer being used as an instrument of a crime or being the target of a crime.
- What is the goal of cyber terrorism?
- For what other purposes might a terrorist organization use computer technology
- How does cyber warfare correlate to computer crime and cyber terrorism?

3. Required Reading:

Volonino, Linda and Robinson, Stephen R., *Principles and Practice of Information Security*, Pearson Prentice Hall, 2004, Chapter 10.

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 1 and 9.

4. Recommended Reading

U.S. Army War College Quarterly, *Parameters*,
<http://www.carlisle.army.mil/usawc/Parameters/default.cfm>

P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, 2009, Chapters 5, 11, 13-14, 16, and 19-22.

LESSON 10 TOPIC: INCIDENT RESPONSE/CONTINUITY OF OPERATIONS

1. Lesson Goals/Objectives:

- Understand the stages of incident response and why it is a necessary part of your cybersecurity program
- Understanding the purpose that incident response serves
- Creating a computer incident response team and understanding the role of each member
- Developing procedures for responding to incidents
- Understanding the types of incidents
- Understand the various incident response support organizations
- Understanding the legal aspects of conducting a cyber investigation
- Understand computer forensic capabilities
- Understand the continuity of operations/continuity of government concept

2. Discussion Topics:

- Is incident response the same as an investigation? Does every incident response end with an investigation?
- Why does an organization need a strong incident response program?
- How would you go about setting up a computer incident response team? How many members would it have and what are their roles?
- Is DHS a response support organization? Name some of the organizations under DHS that provide assistance both before and after incidents occur.
- When would you use computer forensics?
- What are some of the legal issues associated with incident response?
- Why is a continuity of operations plan necessary?

3. Required Reading:

Volonino, Linda and Robinson, Stephen R., *Principles and Practice of Information Security*, Pearson Prentice Hall, 2004, Chapter 7.

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 10, 11 and 13.

LESSON 11 TOPIC: TABLETOP INCIDENT RESPONSE PROJECT

Project Due Date: Tabletop scenarios paper due by the end of this lesson

The objective of this exercise is to develop hypothetical security incident response scenarios to assist organizations in assessing their level of preparedness and ability to respond to security incidents. The class will be divided into teams of 3-4 learners for this exercise. Each team will develop a scenario, which details a realistic, but hypothetical, cyber based attack against an organization or multiple organizations within one of the critical infrastructure sectors. The scenario must have a minimum of three injects designed to build on the scenario. Each team will submit a written paper detailing their scenario. The team will then lead the class through a tabletop discussion and review of their scenario.

1. Scenario Requirements:

- Each team will be required to write and submit a security incident response scenario paper.
- The scenario must detail a realistic cyber based attack against an organization or multiple organizations within one of the critical infrastructure sectors.
- Minimum of three injects.
- Paper has no specific length.
- Any references must be properly cited.

2. Scenario Summary:

- Background: Overview of the scenario.
- The Event: Details of the actual attack.
- The Results: Details of the outcome of the attack.
- Intended Participants: Details of the participants within the critical infrastructure sector that the scenario would pertain to and would possibly have a responsibility to respond in regards to the attacks.

You may wish to consider hypothetically including:

- Corporate personnel
- Federal officials
- State officials
- Local officials

3. Running the Exercise:

- Prepare all materials (digital and hard copy) ahead of time.
- Provide overview and background of scenario (set the stage).
- There are no right or wrong answers. The scenarios are designed to invoke discussion.
- Begin the exercise by delivering the first inject. Then, provide time for discussion. Continue with the delivery of the additional injects, each followed by discussion.
- Be sure to take notes during the discussions. These notes will help with your after action briefing.

- Perform an after-action review. That may lead to changes in the way the participants conduct their daily and emergency operations.

4. Discussion Points:

Tabletop scenarios are designed to be dynamic in nature and to invoke discussion amongst the participants. There are however some topic points that are salient to every incident response and should be included in discussions. The facilitators should prompt the participants with these questions if they are not brought up for consideration.

Points that should be covered in the discussion include:

- Is the attack still in play or has it been contained?
- If the attack is still occurring, how do we get it stopped?
- Who assumes responsibility and leadership roles?
- Who would be notified immediately?
- Are there requirements under the National Response Plan (NRP) and National Incident Management System (NIMS) to make notifications?
- Who else should be included in notifications?
 - Law Enforcement
 - First Responders/EMS
 - Utilities
- How would the media be dealt with?
 - Should the public be notified?
 - Discuss appropriate ways to get information out to the public, and when and why information is provided.
- What effect will this event have on the public perception? Will this have additional consequences amongst the citizens by a loss of trust or confidence in industry or government?
 - Panic?
- How do we minimize the impact?
- What are the Continuity of Government or Business Continuity issues?

5. Required Reading:

National Preparedness Guidelines, 2007, <http://www.fema.gov/pdf/government/npg.pdf>.

National Infrastructure Protection Plan, Chapter 5.

**LESSON 12 TOPIC: TABLETOP SECURITY INCIDENT RESPONSE SCENARIO DEVELOPMENT
EXERCISES**

- Continuation of Lesson 11

LESSON 13 TOPIC: CYBERSECURITY PROGRAM MANAGEMENT NOW AND FOR THE FUTURE

Project Due Date: Final Research Paper due by the end of this lesson

1. Lesson Goals/Objectives:

- Become familiar with potential future critical infrastructure operational risk and related challenges
- Become familiar with emerging technologies and emerging threats
- Understanding that there are few if any elements of our critical infrastructure that does not rely on cybersecurity and this will only continue to become more prevalent.
- Understanding that the best offense is a good defense
- Understand that cybersecurity will have to adapt to new technologies at an ever increasing pace.
- Become aware of the blended attack scenarios, where cyber may be only a small aspect or piece of the overall attack.

2. Discussion Topics:

- What will the critical infrastructure operational environment look like 10-20 years from now?
- What will be the principal threats and challenges to critical infrastructure in the future? Will cyber warfare trump the individual hacker or will the individual hacker become an agent for those engaged in cyber war?
- How do we continue to finance our cybersecurity initiatives with technology growing at astronomical rates?
- With cyber being an integral part of all key resource sectors, how can we integrate cyber critical infrastructure planning in the future? How can we administer cyber critical infrastructure goals and objectives within and across sectors, jurisdictions, and geographic regions?
- What are the core elements of an effective cyber critical infrastructure awareness, education and training program? And at what levels should these be taught?
- What are the keys to effective cyber critical infrastructure program management today, tomorrow, and in the future?

3. Required Reading:

National Infrastructure Protection Plan, Chapters 6 and 7; Appendix 6.

Rittinghouse, John W. and Hancock, William M., *Cybersecurity Operations Handbook*, Elsevier Digital Press, 2003, Chapter 18.

LESSON 14 TOPIC: PRESENTATIONS

1. Lesson Goals/Objectives:

- Each learner will prepare and deliver an oral presentation of their research on a specific critical infrastructure topic area with cybersecurity as a key component and its impact on our national security. Audience will be able to ask questions of the presenter.

2. Discussion Topics:

- Presentations

3. Required Reading:

- As required for research paper and presentation

LESSON 15 TOPIC: PRESENTATIONS

1. Lesson Goals/Objectives:

- Each learner will prepare and deliver an oral presentation of their research on a specific critical infrastructure topic area with cybersecurity as a key component and its impact on our national security. Audience will be able to ask questions of the presenter.

2. Discussion Topics:

- Presentations

3. Required Reading:

- As required for research paper and presentation.