RISK LESSON

Nancy Stevens – First Flight High School, Kill Devil Hills, NC

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

RISK

The Impact of Computing Big Idea is based upon understanding the risks to privacy from collecting and storing personal data on a computer system. It contains learning objectives for understanding how unauthorized access is gained, and how computing resources can be misused and protected.

The NIST Risk Management Framework provides policy and standards to help secure information systems. A simplified version of a cybersecurity risk model is presented in this CCL and it is based upon the NIST Framework.

The first lesson provides an overview of the cybersecurity risk model, and the next four lessons provide activities exploring risk in more detail. If time is a consideration, the first lesson can be a standalone lesson. If time allows, the sequence of five lessons provides an introduction to risk management.

OVERVIEW

Prerequisite Knowledge: Students should be familiar with Internet concepts, the CIA Triad, and Identification, Authentication, and Authorization concepts.

Length of Completion: The CCL is designed to take approximately 300-350 minutes.

Learning Setting: Traditional face-to-face setting or a blended classroom.

Lab Environment: Students will need a device with Internet access.

Activity/Lab Tasks: PowerPoint slides provide the lesson warm-ups, vocabulary terms, sequence and guidance for the learning activities.

01.Risk_Overview.docx
02.Risk_Presentation.pptx
03.Risk_RiskandConsequences_Activity.docx
04.Risk_RiskandConsequences_ActivityExampleSolutions.docx
05.Risk_Scenarios_Activity.docx
06.Risk_AssetIdentification_Activity.pdf
07.Risk_AssetIdentification_ActivityExemplar.pdf
08.Risk_NationalVulnerabilitiesDatabase_Activity.docx
09.Risk_NationalVulnerabilitiesDatabase_ActivitySolutions.docx

10.Risk_DefenseInDepth_Activity.docx
11.Risk_DefenseInDepth_ActivitySolutions.docx

Access to the following websites is needed:

- National Vulnerability Database,
- Glossary. National Initiative for Cybersecurity Careers and Studies. NIST. U.S. Dept. of Commerce, and
- research of security controls.

LEARNING OBJECTIVES AND AP CSP ALIGNMENT

Lesson Learning Objectives

In this CCL students will:

1) understand how computing resources can be misused,
2) identify how computing resources and information assets can be vulnerable to attack,
3) explain the role and types of protection mechanisms to achieve confidentiality, integrity, and availability of computing resources and information assets, and
4) summarize security and privacy risks from collecting and storying personal data on a computer system.

ASSOCIATED AP CSP SUB LEARNING OBJECTIVES

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 1: CREATIVE DEVELOPMENT

- CSN-1.D Describe the differences between the Internet and the World Wide Web.
    - CSN-1.D.1 The World Wide Web is a system of linked pages, programs, and files.
    - CSN-1.D.3 The World Wide Web uses the Internet.
- CSN-1.E For fault-tolerant systems, like the Internet:
        - Describe the benefits of fault tolerance.
        - Explain how a given system is fault-tolerant.
        - Identify vulnerabilities to failure in a system.
    - CSN-1.E.2 Redundancy is the inclusion of extra components that can be used to mitigate failure of a system if other components fail.
    - CSN-1.E.3 One way to accomplish network redundancy is by having more than one path between any two connected devices.

- CSN-1.E.5 When a system can support failures and still continue to function, it is called fault-tolerant. This is important because elements of complex systems fail at unexpected times, often in groups, and fault tolerance allows users to continue to use the network.

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 5: IMPACT OF COMPUTING

- IOC-2.A Describe the risks to privacy from collecting and storing personal data on a computer system
  - IOC-2.A.1 Personally identifiable information (PII) is information about an individual that identifies, links, relates, or describes them. Examples of PII include: social security number, age, race, phone number(s), medical information, financial information, biometric data.
  - IOC-2.A.2 Search engines can record and maintain a history of searches made by users.
  - IOC-2.A.3 Websites can record and maintain a history of individuals who have viewed their pages.
  - IOC-2.A.4 Devices, websites, and networks can collect information about a user's location.
  - IOC-2.A.5 Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and institutions.
  - IOC-2.A.6 Search engines can use search history to suggest websites or for targeted marketing.
  - IOC-2.A.7: Disparate personal data, such as geolocation, cookies, and browsing history, can be aggregated to create knowledge about an individual.
  - IOC-2.A.8 PII and other information placed online can be used to enhance a user's online experiences.
  - IOC-2.A.9 PII stored online can be used to simplify making online purchases.
  - IOC-2.A.10 Commercial and governmental curation of information may be exploited if privacy and other protections are ignored.
  - IOC-2.A.11: Information placed online can be used in ways that were not intended and in ways that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, social media posts can be viewed by potential employers.
  - IOC-2.A.12 PII can be used to stalk or steal the identity of a person or to aid in the planning of other criminal acts.

    - IOC-2.A.13It is difficult to delete information once it has been placed online.
    - IOC-2.A.14: Applications can collect your location and record where you have been, how you got there, and how long you have been at a given location.
- IOC-2.B Explain how computing resources can be protected and can be misused.
    - IOC-2.B.1 Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include strong passwords and multifactor authentication.
    - IOC-2.B.2 A strong password is something that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user.
    - IOC-2.B.3 Multifactor authentication is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in at least two of the following categories: knowledge, possession, and inheritance.
    - IOC-2.B.4 Multifactor authentication requires at least two steps to unlock protected information; each step adds a new layer of security that must be broken to gain unauthorized access.
    - IOC-2.B.5 Encryption is the process of encoding data to prevent unauthorized access to information. Decryption is the process of decoding the data.
    - IOC-2.B.6 Certificate authorities issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.
    - IOC-2.B.7 Computer virus and malware scanning software can help protect a computing system against infection.
    - IOC-2.B.8 A computer virus is a malicious program that can copy itself and gain access to a computer in an unauthorized way. Computer viruses often attach themselves to legitimate programs and start running independently on a computer.
    - IOC-2.B.9 Malware is software intended to damage a computing system or to take partial control over its operation.
    - IOC-2.B.10 All real-world systems have errors or design flaws that can be exploited to compromise them. Regular software updates help fix errors that could compromise a computing system.

    - IOC-2.B.11 Users can control the permissions programs have for collecting user information. Users should review the permission settings of programs to protect their privacy.
- IOC-2.C Explain how unauthorized access to computing resources is gained.
    - IOC-2.C.1 Phishing is a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.
    - IOC-2.C.2 Keylogging is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.
    - IOC-2.C.3 Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point.
    - IOC-2.C.4 A rogue access point is a wireless access point that gives unauthorized access to secure networks.
    - IOC-2.C.5 A malicious link can be disguised on a web page or in an email message.
    - IOC-2.C.6 Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised.
    - IOC-2.C.7 Untrustworthy (often free) downloads from freeware or shareware sites can contain malware.

LESSON DETAILS

Overview of Lessons: There are four units within this lesson. Each lesson includes a warm-up activity. The first unit frontloads information on a simplified Cybersecurity Risk Model. The next three units have both information and an active learning activity.

- Lesson 1 Basic Cybersecurity Risk Concepts
- Lesson 2 Cybersecurity Risk Model-Assessing Risk
- Lesson 3 Cybersecurity Risk Model-Vulnerabilities
- Lesson 4 Cybersecurity Risk Model-Security Controls

LESSON 1 BASIC CYBERSECURITY CONCEPTS

02.Risk_Presentation.pptx
03.Risk_RiskandConsequences_Activity.docx
04.Risk_RiskandConsequences_ActivityExampleSolutions.docx

Upon completion of this lesson: Students will be able to define risk, and describe the benefits and potential harm from the online collection of personally identifiable information. Students will be able to differentiate between threats and vulnerabilities.

Warm Up: The warm-up activity explores the meaning of risk, and whether or not it is tangible. This activity can be "popcorned" around the classroom or it can be delivered as a think-pair-share. Student responses regarding situations involving risk may include uncertainty, loss, threats, behaviors, insurance, finance, and consequences. The outcome of the warm-up should be an understanding that risk is an abstract concept.

Lesson Details: The PowerPoint slides guide the exploration of basic cybersecurity risk concepts. Following the warm-up activity, a formal definition of risk is presented. Risk involves threats, vulnerabilities, and consequences. Risk is initially explored in terms of personal data. A discussion prompt asks students, "How is your online, personal data at risk?" The initial discussion is intended to help students explore their personal digital footprint as the starting point for understanding threats and vulnerabilities. Students should recognize that there are benefits to the collection of personal information online and there are potential harmful effects.
The CIA Triad can be reinforced as threats and vulnerabilities compromise the confidentiality, availability, and integrity of personal information. Statistics from the Department of Justice and the FBI are presented so students can see the scope of identity theft. The vocabulary terms, threat, threat actor, and vulnerability are defined according to NIST. Students are then asked to brainstorm threats to their online personal data. A slide is included which lists potential threats to online personal data. The consequences of risk are presented. Risk assessment and a simplified Cybersecurity Risk Model are presented at the conclusion of the first lesson. This model is the foundation of the remaining lessons.

LESSON 2 RISK MODEL

02.Risk_Presentation.pptx
05.Risk_Scenarios_Activity.docx
06.Risk_AssetIdentification_Activity.pdf
07.Risk_AssetIdentification_ActivityExemplar.pdf

Upon completion of this lesson: Students will be able to identify assets that can be attacked and describe how vulnerabilities are exploited in attacks.

Warm Up: Students are prompted to consider the following: "Do the potential risks to your data (collected by businesses) outweigh the benefits? What do you get in return for the data that is collected about you?" This discussion should get to the transactional nature of web browsing and social media.

Lesson Details: The results of a recent Pew Research Center poll reveal that the majority of Americans are concerned about online privacy. The Cybersecurity Risk Model is presented as a framework for understanding the risks to privacy and security. The model is a simplified version of the framework developed by the National Institute of Standards and Technology (NIST). The first step in the model examines what items of value (assets) are at risk. The next step explores the concept of misuse, which includes threats and vulnerabilities. Misuse has consequences and the following terms are defined: deception, disruption, disclosure, and usurpation. Examples are provided to help students understand the peril or injury types. The Risk Scenarios activity provides students with an opportunity to identify and assess the probability of peril or injury. The Asset Identification activity requires students to examine one of the risk scenarios and identify who and what is at risk. The one-pager format is intended for students to define terms and to apply their understanding of assets and risks.

Active Learning Activity: The Risk Scenarios handout contains 4 risk scenarios and an exercise that students complete.

Active Learning Activity: The Asset Identification handout is a one-pager that students will complete.

LESSON 3 RISK MODEL-VULNERABILITIES

02.Risk_Presentation.pptx
08.Risk_NationalVulnerabilitiesDatabase_Activity.docx
09.Risk_NationalVulnerabilitiesDatabase_ActivitySolutions.docx

Upon completion of this lesson: Students will be able to describe the role of the National Vulnerability Database.

Warm Up: The opening activity is to poll students with the following 3 questions:

1) Do you regularly update your phone's OS?
2) Have you ever connected to a public WiFi access point?

3) Have you ever suspected the authenticity of an email? These everyday activities represent vulnerabilities and potential attacks.

Lesson Details: Lesson 3 examines vulnerabilities or weaknesses. The activity in this lesson will require some guided instruction. The National Vulnerability Database (NVD) is a government repository of standards-based vulnerability management data launched in 2005. NVD is a product of the National Institute of Standards and Technology (NIST) which is within the U. S. Department of Commerce. The Security Content Automation Protocol (SCAP) is the standards-based method used to provide security guidance. The CVE (cybersecurity vulnerabilities and exposures) is a dictionary developed by the Mitre Corporation. The PowerPoint slides walk students through a search for "Pulse SSL" in the database. SSL stands for Secure Sockets Layer. It is the security standard for establishing an encrypted link between a web server and a web browser client. SSL keeps data confidential during transit between the server and the browser. Pulse SSL is used for VPN connections. The NVD entry reports than "an unauthenticated, remote attacker can conduct a session hijacking attack." This vulnerability had a critical score of 10 when this lesson was developed. The entry provides references to advisories, solutions, and tools to mitigate the effects of an attack.

Active Learning Activity: The National Vulnerability Database Activity requires the use of the "National Vulnerability Database" and the handout.

LESSON 4 RISK MODEL-SECURITY CONTROLS

02.Risk_Presentation.pptx
10.Risk_DefenseInDepth_Activity.docx
11.Risk_DefenseInDepth_ActivitySolutions.docx

Upon completion of this lesson: Students will be able to describe how privacy and security are interrelated. Students will be able to identify security control measures and describe how they work.

Warm Up: The prompt asks students if they have any IoT (Internet of Things) devices in their home. If students do not have these devices, ensure that they understand that Amazon's Alexa, Google Home, and Facebook Portal are becoming commonplace in many homes. The point of this activity is to explore what students know about the security of these devices. For example, there have been reports of the hacking of security cameras within people's homes.

Lesson Details: This lesson examines security controls. The PowerPoint contains a video from NIST on the security of IoT devices. The relationship between privacy and security, and the need for security controls is the focus of this lesson. The

concept of "defense in depth" or a layered approach to security is introduced. Examples of bank security and network security controls are provided. The Defense in Depth activity returns to the risk scenarios in Lesson 2. Students are now tasked to identify security controls or measures that could be implemented into a layered strategy. The PowerPoint slides conclude with a look at ways to deal with risk: avoidance, mitigation, transfer, or acceptance. Some examples of ways to mitigate risk are provided in the conclusion.

Active Learning Activity: The Defense in Depth handout requires students to identify 5 security controls or measures that could be implemented in one of the risk scenarios introduced in Lesson 2. In this activity students define the security measures, identify the type of measure, and provide a justification for the selection of the measure. Additionally, (slide 79) guides a discussion on ethical considerations of security controls, specifically concerning AI.

ACKNOWLEDGEMENTS

Resources:

Glossary. National Initiative for Cybersecurity Careers and Studies. NIST. U.S. Dept. of Commerce

"Guide for Conducting Risk Assessments". NIST Special Publication 800-30. Revision 1. U.S. Department of Commerce. September 2012.

Risk Management Framework (RMF) Overview—FISMA Implementation Project | Computer Security Resource Center | NIST. November 30, 2016.

Cybersecurity Framework. NIST (National Institute of Standards & Technology). U.S. Dept of Commerce.