Info for educators – Cybersecurity Concepts – Fall 2019

Module Description

This module introduces students to the terms and concepts common to the field of cybersecurity. Students will develop a broad understanding of cybersecurity and gain an understanding of the fundamental mission of cybersecurity programs. This is one of a series of modules designed to introduce young adults to cybersecurity concepts.

Module contents

1) Recorded lecture (approx. 36 minutes)
2) Slide deck materials (pdf)
3) Discussion topics (below)
4) Suggested quiz questions (below)

Student Learning Outcomes

- Develop student knowledge of the fundamental concepts of terms within the field of cybersecurity.
- Understand how cybersecurity professionals view common activities and organizational needs.
- Understand the concepts of risk, threat and vulnerability.

Time/Effort

- Recorded lecture – approx. 40 minutes
- Reading/reviewing the posted links – approx. 2 hours
- Discussion: 30 – 60 minutes

Suggested Discussion Topics

1) Consider the concept of integrity for an information asset. Write out three different scenarios where an organization's information has lost integrity. Example:

   Organization: Payroll processing firm
   Data: Salary and personal information for employees
   Integrity loss: Someone accessed their payroll database and changed salary amounts for people

2) Review the information about the threat and vulnerability concepts. Similar to the scenario with the rising water (threat) and crack in the wall (vulnerability), make up your own scenario and describe it in terms of threat and vulnerability.

3) Many of these concepts were developed before the "Internet of Things". Consider some of the internet-connected devices in your life and describe them in terms of confidentiality, integrity and availability. (Don't reveal any private or sensitive

information!). Describe what the impact or harm would be if there was a breach of your device's confidentiality, integrity or availability.

4) Think about the "CIA" of voting in an election. Who is motivated to breach confidentiality? Who is motivated to breach integrity? And who to breach availability? For each of these, what is their hoped-for outcome?

Quiz Questions

1) Hacker X is hired by rival to compromise an aerospace company's website and alter the marketing photos of their rocket motors. This is an attack against the _____ security goal.
    a. Integrity
    b. Confidentiality
    c. Availability
    d. All of the above
    e. Both B and C

2) Hacker X is hired by a rival to compromise an aerospace company's database and steal a copy of the new, secret rocket motor plans. This is an attack against the _____ security goal.
    a. Integrity
    b. Confidentiality
    c. Availability
    d. All of the above
    e. Both B and C
3) Hacker X is hired by a rival to compromise an aerospace company's database and delete the new, secret rocket motor plans. This is an attack against the _____ security goal.
    a. Integrity
    b. Confidentiality
    c. Availability
    d. All of the above
    e. Both A and B
4) A flaw or weakness in a system is a(n)
    a. Exploit
    b. Vulnerability
    c. Threat
    d. Risk
    e. Control
5) An action or technology or procedure or policy used to reduce a threat, vulnerability or attack is a(n)
    a. Protocol
    b. Countermeasure
    c. Program

    d. Deception
6) Which are the following are NOT examples of harm from a human threat?
    a. Interception of data
    b. Interruption of operations
    c. Modification of data
    d. Fabrication of data
    e. Collision of information
    f. Earthquake damage
    g. Both A and D
    h. Both E and F
7) Confidentiality means that attackers cannot change or destroy information. (T or F)
8) Detective countermeasures identify when a vulnerability is being exploited and especially when it is succeeding. (T or F)
9) Preventative countermeasures keep attacks from succeeding. (T or F)
10) Detective countermeasures keep attacks from succeeding. (T or F)

Suggested reading:

Books:

- Charles Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies. "*Security in Computing*", Prentice Hall, 2015 (ch 1)