REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Networking Fundamentals 1.1
Topic: Understand core security principles
(One 50-minute class period)
File name: SecurityFund_RL_1.1

Lesson Objective

1.1: Understand core security principles. *This objective may include but is not limited to:* confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering.

Preparation Details

Prerequisite student experiences and knowledge

This MTA Certification Exam Review lesson is written for students who have learned about security fundamentals. Students who do not have the prerequisite knowledge and experiences cited in the objective will find additional learning opportunities using resources such as those listed in the Microsoft® resources and Web links at the end of this review lesson.

Instructor preparation activities

- Download and install the MS Office timeline template from: *http://office.microsoft.com/en-us/templates/TC010162661033.aspx* Either have the students use MS Office or print out paper copies and also provide colored pencils for drawing the timeline.

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_1.1

Teaching Guide

Essential Vocabulary

CIA triangle (confidentiality, integrity, availability)—

> ***confidentiality***—ensuring the prevention of unauthorized disclosure of information.
>
> ***integrity***—ensuring the prevention of erroneous modification of information.
>
> ***availability***—ensuring the prevention of unauthorized withholding of information or resources.

principle of least privilege—a principle that requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

social engineering—any type of behavior that can inadvertently or deliberately aid an attacker in gaining access to a user's password or other sensitive information.

threat and risk principles—risk management is a systematic and analytical process to consider the likelihood that a threat will endanger an asset, individual, or function and to identify actions to reduce the risk and mitigate the consequences of an attack. A threat assessment identifies and evaluates threats based on various factors, including capability and intentions as well as the potential lethality or severity of an attack.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes)

1. Student prompt: On a sheet of paper, list as many "network attacks and threats" that you can think of. Separate into two columns. See PowerPoint® slide 3.
2. Give students a few minutes to respond, allowing them to work until they have finished.
3. As time permits, call on a few students to report to the group with their responses.

Lesson activity (40 minutes)

1. Teacher Instruction (20 minutes)
   a. Use the included PowerPoint slideshow to review the different core security principles.
   b. Stop at Slide 12 and allow students to move onto next step.

c. In groups of two or three, have the students create a timeline explaining the history of computer security and how it evolved into information security.

- Be sure to include important information security developments during each decade beginning with the 1960s through today.

d. Students complete the timeline, identifying the different phases of computer security.

e. Finally, have each group of students share their flowchart with the group.

f. If time allows, you may review all or part of the flowchart, discussing student responses to the questions.

Assessment/lesson reflection (10 minutes)

1. Discuss "What is the defining difference between computer security and information security?"
2. On the back of the timeline document, tell students to write down any questions they have or any topics about which they would like more assistance.
3. After class, look through the student responses and follow up with any student requiring additional help.

Microsoft resources and Web links

- **Sample Timeline**
  http://www.scmagazineus.com/a-brief-history-of-internet-security/article/149611/
- **How to Protect Insiders from Social Engineering Threats**
  http://technet.microsoft.com/en-us/library/cc875841.aspx