Physical Security Module

Module Learning Outcomes:

- #3: Explain different types of attacks on computing systems.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.
- #13: Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

- #4: Least Privilege
- #5: Layering
- #7: Information Hiding

Description:

This module on physical security addresses the cybersecurity threat from a more comprehensive standpoint. Students will be challenged to recognize and understand security concerns from multiple perspectives, ranging from the insider threat, outsider threat, to threats involving the actual physical components. Exposure to a design methodology, associated system components modules, and basic security principles are featured in this module. Students will also be exposed to the private and public responses to computer security problems, and introduced to a number of unique computer crimes and solutions to deal with these crimes. The importance of a sound security policy in the overall management of any organization is addressed.

Upon completion of the module students will:

- ❖ Possess an understanding of physical security system design and evaluation.
- ❖ Gain an understanding of the process of evaluating existing or proposed physical protection systems.
- ❖ Understand the policies and procedures needed to protect an organization and its computer resources from insiders who might do harm.
- ❖ Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

Learner-Centered Classroom:

In this module students will work as teams to test and develop an upgrade to an existing physical security system. Students will be challenged to upgrade a facility to increase its security posture. As part of this team building exercise students will test their upgrade using computer modeling software. A major component of this module will be the introduction of the design and evaluation process as developed by the Department of Energy. Students will be instructed on how to apply this process in their own protection and also the protection of personal assets such as a laptop or computer system. Students will be introduced to the three types of adversaries: outsiders, insiders, and outsiders in collusion with insiders, and the unique challenge each brings. They will also be exposed to the three basic tactics that adversaries might utilize: force, stealth, and deceit.

Assessment:

This module will be assessed by the following criteria - how realistic, budget and cost, probability of interruption from the modeling software, and upgraded policies and procedures. Each group will be challenged to develop an upgrade to a scenario and each group's upgraded will be assessed using a modeling program which assesses its ability to defeat an adversary.

Suitability to various groups:

The principles introduced in this module are applicable for all three groups. The development of sound protection policies and procedures are important for all individuals. Understanding how to model this process and gaining insight into the impact of changes to these policies and procedures will help both students and teachers alike in safeguarding themselves, not just in the cyber world, but in their day-to-day activities.

How the Teachers and Students groups will be interacting:

In this module each group will work independent of the others (middle school, high school, and teachers). The three groups will compete against each other on the best overall upgrade design. Each group will be exposed to the same material and will develop an upgrade to the same factitious facility.