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 will allow students the opportunity to develop an upgrade to the physical security system of an office building. These upgrades will included changes to policy, procedures and personnel actions within the organization. The upgrades suggested will be performance tested (validated numeric characteristics through computer simulation) to assess the impact that those upgrades have to the overall security posture of the organization. Students will be given an overview of the Design and Evaluation Process Outline (DEPO) as developed by the Department of Energy and how it applies to the protection of computer hardware and storage devices. 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 learn the importance of integrating people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks. Students will be challenged to provide an upgrade of the security system for a simulated data storage facility. 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 and how they apply to cybersecurity.
- ❖ 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 in teams to test and design 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 for 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 challenges 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 upgrade will be assessed using a modeling program which assesses its ability to defeat an adversary. Students will also critique the other groups' upgrades and offer suggestions on how improvements could have been made.

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.