Insider Threats: Factors and Responses

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #3: Explain different types of attacks on computer 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.
- #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: (Please include explicit references to the First Principles - Appendix 1)

- #4: Least Privilege
- #7: Information Hiding
- Ethics

Description:

This module focuses on insider threats and their role in developing effective cybersecurity systems. Humans are the weakest link in cyber security and this will be exemplified in this module. Specifically, this module defines insider threats (versus errors), discusses characteristics of becoming a threat, examples of used threats, and how to prevent the damage caused by this group. The context of this discuss meets the least privilege cyber security principle, as well as ethical considerations.

The module will begin with a discussion of defining a crime and whether or not employees can commit crimes, though businesses tend to focus on the 'stranger' or customer committing a crime, such as stealing. Specific 'real life' examples will be provided with every point, such as employee theft examples with Walmart and UPMC. Discussion will address factors and motivations (i.e. criminological theories) in why employees would 'steal' from their employer, as well as tactics they have used in past events. Known risks factors provided by various federal and private agencies will be discussed and analyzed in possible prevention techniques. Least privilege will be discussed as a viable tactic to limit insider threats, as well as other mechanisms.

L**earner-Centered Classroom:**

This module is relevant to K-12 teachers, as their co-workers can be potential insider threats that impact their grading, curriculum plans, websites, personnel files, and other significant information. Various scenarios focused on K-12 issues for teachers will be provided for discussion, such as hiring protocols, computer access in school, sharing of password with co-workers and students, leaving computer unattended, and other events. Small group discussion will ensue with these scenarios that will lead to application of possible prevention techniques currently used and those that may need to be considered in the future.

In discussing insider threats with middle to high school aged students, scenarios will also be provided, though designed for relevance in their experiences, for small group discussions. Events such that can occur at home, school or place of employment will be addressed. Motivations and outcomes of security breaches will be discussed in relation to prevention. For example, if they know a student who works closely with a teacher and has the teacher's password and plans to look at an exam, what should the student do? Online video examples will also be used in showing the 'costs and damage' of these actions, which are provided by CERT.

Assessment:

For both teachers and students, a quiz will be given to them at the beginning of the session (pre), as well as at end (post), to gauge what they have learned about insider threats. Another tool used to assess their learning is a small group project. The groups will provide a 'real' scenario of an insider threat situation and outcome. The event, characters, location, security threat technique, and outcome will be developed and shown to the entire group as a performance that will be evaluated by the audience. Key concepts will be portrayed in the small group project and a rubric will be given to everyone to evaluate the group and for the groups to understand how they will be assessed.

Suitability to Various Groups:

The main concept and points in the understanding of insider threats are relate to all persons. The content will be adapted with relevant examples to students, as well as for teachers. Teachers will further understand the significance of their actions in the classroom, such as the potential threat when students share passwords with each other (or teachers to students) and allowing students to have full access to their computer system. Middle and high school students will understand the importance of following computer security protocols, such as not sharing passwords with others, and the significance of ethical decision making in having computer access beyond their home.

How the Teachers and Students Groups will be Interacting:

This module will have each group work independently to create a scenario where other groups will need to 'guess' who the insider threat is in the situation. The covered material will be the same for each group, though the scenario they devise will be unique to each group.