07 March 2024

From: Marita R. Trammell

To: Course Coordinators at Center for Cyber Security Studies

Subj: Report of Findings from Data Analysis and Proposed Changes to SY110 Course Learning Objectives

1. Introduction
    a. The purpose of this report is to present the findings from the data analysis of the SY110 course and propose changes to the Course Learning Outcomes (CLOs) based on these findings. The analysis aims to enhance the effectiveness of the learning objectives and align them with the needs of the students and the evolving cyber domain. The report includes insights derived from statistical analysis, visualizations, and advanced analytics techniques applied to the course data.

2. Data Analysis Summary
    a. Course Performance Overview:
        i. The overall average score across all assessments in the SY110 course was 69%.
        ii. Scores varied significantly across different question types and topics, indicating varying levels of understanding and difficulty.
    b. Question Type Analysis:
        i. Single-Select Questions: High performance with an average score of 90%.
        ii. Multiple Select Questions: Moderate performance with an average score of 80%.
        iii. Fill-in-the-Blank Questions: Lower performance with an average score of 70%.
        iv. True/False Questions: Average performance with a score of 70%.
        v. Match Questions: Varied performance with scores ranging from 70% to 100%.

      vi. Solve Questions: Moderate performance with scores around 75%.

   c. Topic Analysis:
      i. Cyber Domain Importance: Students scored high on understanding the importance of the cyber domain.
      ii. Technical Understanding: Moderate scores on understanding computers, operating systems, and networks.
      iii. Program Analysis: Lower scores in analyzing and explaining the output of programs and shell commands.
      iv. Defensible Systems: Moderate understanding of principles and properties of defensible information systems.
      v. Reconnaissance and Defense: Students performed well in basic actions related to reconnaissance, attack, defense, and forensics.
      vi. User Decisions and Security: Mixed performance on scenarios where user decisions affect security.

   d. Advanced Analytics:
      i. Predictive Modeling: Identified key factors contributing to student performance, including prior knowledge, engagement with course materials, and participation in practical exercises.
      ii. Cohort Matching: Showed that students who engaged more with hands-on exercises performed better in practical assessments.

3. Proposed Changes to SY110 Course Learning Objectives
   a. Based on the findings from the data analysis, the following changes to the SY110 Course Learning Outcomes are proposed to address identified gaps and enhance the learning experience:
      i. Refine CLOs to Focus on Practical Skills:
         1. Current CLO: "Analyze and explain the output of programs and the results of shell commands and infer why certain actions are permitted or not in an information system."

    2. Proposed Change: "Analyze and interpret the output of programs and shell commands, and troubleshoot issues in information systems to determine the reasons for permitted or restricted actions."

ii. Enhance Understanding of Technical Foundations:

    1. Current CLO: "Describe computers, operating systems, networks, the Internet and the Web with respect to: digital representations of information, their basic operation and associated tools, and the underlying architectures and protocols and how they may be vulnerable to attack."
    2. Proposed Change: "Explain the fundamental components and operations of computers, operating systems, networks, the Internet, and the Web, and identify their vulnerabilities to various types of cyber attacks."

iii. Strengthen Focus on Defense Mechanisms:

    1. Current CLO: "Identify and describe the principles and desired properties of defensible information systems, and the techniques and tools that are used to provide them. Explain representative attacks and their prevention and mitigation measures."
    2. Proposed Change: "Identify and evaluate the principles and properties of defensible information systems, and apply techniques and tools for their implementation. Analyze representative cyber attacks and develop strategies for their prevention and mitigation."

iv. Improve User-Centric Security Awareness:

    1. Current CLO: "Describe cyber domain scenarios in which user decisions affect security, identifying the user's versus the technology's responsibilities, and explain the consequences of potential user actions

in terms of risk and the tradeoff between services and security."

2. Proposed Change: "Analyze cyber domain scenarios where user decisions impact security, distinguish between user and technology responsibilities, and evaluate the consequences of user actions in terms of risk and the balance between services and security."

v. Incorporate Advanced Defensive Techniques:

1. Current CLO: "Explain, differentiate, and perform basic actions related to reconnaissance, attack, defense, and forensics of information systems."
2. Proposed Change: "Demonstrate advanced techniques in reconnaissance, attack, defense, and forensics of information systems, and apply these techniques in simulated environments.”

4. Conclusion

a. The data analysis of the SY110 course has provided valuable insights into student performance and the effectiveness of current learning objectives. By refining and enhancing the CLOs to focus more on practical skills, technical understanding, defense mechanisms, user-centric security, and advanced techniques, the course can better prepare students to meet the challenges of the cyber domain.

b. These proposed changes aim to bridge identified gaps, improve student engagement and performance, and ensure that the learning outcomes are aligned with the evolving requirements of the field of cybersecurity.

Very Respectfully,
Marita R. Trammell