Assignment 2: Group Assignment and Presentation
INFO 6010 Fall 2024

Weight: 15% of final grade
Due date: (See FOL Submission Box)

Welcome to your second research assignment in this course! In this assignment, your group must consider a realistic and complex scenario in industry (see options below). The reason for this group-based assignment is to teach the benefits of working and learning in a group. In industry, you will often be asked to work in groups to solve complex security problems.

As in the first assignment, you and your group must apply the knowledge gained in your many ISM courses (as well as the CISSP CBK) and apply that learning to a real-world scenario. Your group's task is to read the scenario, identify the key elements, and identify the information you need to research to respond to the scenario.

Once your group has read the scenario and identified potential problems you want to solve by applying your CBK knowledge and the relevant literature/research, your group will write and submit a research paper and present your group's work and results to our INFO 6010 class. The presentation schedule is posted in Week 10 of the CISSP course.

Here's the wrinkle I promised in class. As a group, you will meet and discuss the three scenarios below and select the one that interests your group the most. The wrinkle is that **only two groups** can choose the same scenario. You must register your group's scenario choice by posting in the "**Assignment 2 Scenario Registration**" Discussion Forum in FOL.

Use of Generative AI

You are welcome – even encouraged – to use ChatGPT, Grammarly AI, or other GenAI tools to assist you with brainstorming, ideation, outlining, and creative problem-solving. However, AI-powered writing tools **may not be used in the written portion of this assignment in any form** – this includes using GenAI to edit/improve your written submission. Evidence of GenAI in the written component constitutes an academic offense.

Submission Instructions

This assignment has two submission requirements: 1) a written research paper, and 2) an in-class presentation. Please submit the group's research paper (.doc or .pdf) and your presentation slides in your group's FOL submission box. There is no option to pre-record your presentation – **it must be delivered live, in class**.

Written Assignment:

- Connect your answers/decisions to the CBK **as much as you can.**
- Your research paper must be **APA (7th Ed) compliant** (student version) in style and formatting. In other words, both a title page and a references page are required. Please do not need to include an abstract or a Table of Contents.

- Critical/key factual statements **and decisions** you make must be properly supported by the literature using in-text citations (with a corresponding source on the References page) from credible literary sources. You are encouraged to use the course content/resources/lessons, but also other resources you find through your own research. Be prepared to look *outside* the course content for relevant journal articles, scholarly papers, etc.
- Please minimize the use of "popular" sources such as blogs, wikis, and online forums. Instead, prioritize professional or academic/scholarly sources for your references. The course textbook *and lesson slides* need to be cited if you use them.
- Be concise in your writing – there is no maximum word or page count. I expect your assignment will be about 5 pages long (not including the title and references pages)

Online Presentation Requirements:

- Groups will present their findings in an in-class presentation that is **no longer than 10 minutes**. After 10 minutes your instructor will stop your presentation. You will be allowed up to 5 minutes to answer questions from the class.
- I highly recommend your presentation include visual elements, such as PowerPoint slides, graphics/images, charts/graphs, infographics, props, and interactive elements.
- **Avoid reading from a script or slides**. You should know your work well enough to talk about it without reading. Avoid "word walls" in your slides as well.
- Every member of your group must speak. Take the time to organize who will talk about what and when.
- If your group includes any part-time or online students, you ***may*** pre-record your presentation instead of presenting it live in class. Include a link to the video in your group's submission box and be prepared to share that link with the class when it's your turn to present. **Please note:** registered full-time (in-person) students must be in class on presentation day to answer questions from the class.

Tips for Success:

- Your group can interpret problems/elements of the scenario as you see fit. Feel free to add whatever information you need that isn't in the scenario description.
- ALL group communication must happen via your group's private/confidential discussion forum. PLEASE DO NOT USE EMAIL as I cannot help you with group issues!

ONE MORE THING!

At the end of the assignment (as part of your conclusion), you must include a "Reflection Section". Before writing this section, your group should reflect on your work and learning in this course. Has your collective/individual perspective on the application and interconnectedness of the CBK domains changed as a result of this exercise? If so, how? Justify your response with examples. Your reflection section could also discuss the challenges your group faced (and how you overcame them) in completing this assignment.

The scenario options are listed below (one option per page). Read them all before choosing!

Scenario Option #1: ROAR Comp - Underwater Robot Sports League and Smart Stadium

A new sports league, the RObotic Augmented Reality Competition (ROAR Comp), has been created where the "athletes" are advanced humanoid robots designed to play underwater in a giant aquarium stadium. These robots are equipped with cutting-edge AI and connected via a sophisticated network to enhance their performance and coordination. The league's flagship stadium, located in Austin, Texas, is a state-of-the-art smart stadium designed to provide an immersive experience for fans, with advanced IoT devices, biometric security, and real-time data analytics.

The owners of the Austin Aquamen, the premier team in the ROAR Comp, have received credible intelligence about an underground hackathon. This competition challenges malicious hacking groups to infiltrate the stadium's network, the robotic players, and/or the augmented reality (AR) environment used for fan engagement. To pre-emptively address this threat, the owners have hired your team to develop a comprehensive security strategy.

Consider the various elements of this scenario and identify how you would add to the scenario (along with your justification for any changes) so you can proceed with your research and planning. Using your knowledge of the domains of the CISSP CBK and the available literature, identify the threats, risks, vulnerabilities, attack vectors, and defense options, then respond to the questions below:

Scenario Questions for Option #1

Your submission for this assignment should be in the form of a research paper and presentation that includes the following:

1. Develop a comprehensive strategy to secure the ROAR Comp's operations and the smart stadium against potential cyber-attacks. This strategy should consider threat analysis, security measures, incident response plans, stakeholder communication, and ethical/legal considerations. Justify the decisions you made in your answer
2. Which assets are most likely at risk, and why?
3. What strategies would you develop and implement to protect the stadium, robot players, fans, and game from both AI-driven and traditional cyber threats?
4. What would you look for in a Threat Landscape, Risk Assessment, or Vulnerability Analysis?
5. How would you prepare to conduct a thorough penetration test that identifies vulnerabilities (ex entry points) in any of these systems?

Scenario Option #2: Protecting Nuclear Fusion Technology in a Small Country

The government of a small country, Energia, has secretly developed a groundbreaking nuclear fusion technology that will revolutionize energy production. This technology has the potential to provide a nearly limitless supply of clean energy, significantly reducing the country's reliance on fossil fuels would make Energia a global leader in sustainable energy.

As the project nears completion, the government becomes increasingly concerned about the security of its critical infrastructure, particularly the power generation facilities that will utilize the new nuclear fusion technology. They fear that cyber attacks could disrupt these facilities, leading to widespread power outages and compromising national security.

Additionally, there are growing fears that foreign entities or malicious actors might attempt to steal the research data, which is stored in highly secure but interconnected systems. The integrity and confidentiality of this data are paramount to maintaining the technological edge and ensuring the project's success. Moreover, the safety of the scientists and engineers working on the project is also a priority. The government is worried that these key personnel could be targeted for kidnapping or coercion to gain access to sensitive information, putting both the individuals and the project at risk.

Consider the various elements of this scenario and identify how you would add to the scenario (along with your justification for any changes) so you can proceed with your research and planning. Using your knowledge of the domains of the CISSP CBK and the available literature, identify the threats, risks, vulnerabilities, attack vectors, and defence options, then respond to the questions below:

Scenario Questions for Option #2

Your submission for this assignment should be in the form of a research paper and presentation that includes the following:

1. Propose a multi-layered security strategy to protect the power generation facilities, research data, and researchers that incorporates cybersecurity measures, physical security, data protection, and personnel security measures. Justify your answers.
2. Develop a detailed plan for responding to any security incidents, ensuring minimal disruption to the power generation facilities and maintaining the safety of the researchers.
3. Create a communication plan to inform government officials, power generation facility managers, and the public about the potential threats (and the measures being taken to address them).
4. Energia is concerned about Critical Infrastructure Security, Research Data Protection, and the safety of their researchers. How would you conduct a thorough penetration test that identifies vulnerabilities (ex entry points) in any of these systems?
5. Discuss any ethical and legal issues related to the protection of the nuclear fusion technology, research data, and researchers.

Scenario Option #3: Cybersecurity in Smart Farming

A farmer named Tania Glenedge, is 51 years old. Tania owns a large farming operation spread out over several miles and multiple properties. Since the passing of her husband, Tania has been running the farm – mostly on her own but she was struggling. Shortly after her husband's death, an organization, AgriTech AI (ATAI), approached Tania with an offer to help her keep the farm running smoothly by integrating advanced technologies (sensors, robotics, etc) into her farming operations. They provided drones for crop monitoring, autonomous tractors for plowing and planting, sensors for animal needs/activities, and robots for various tasks such as feeding animals and crops. The equipment, devices, and sensors are connected via satellites to ensure seamless operation across the vast farm.

With the help of AgriTech Solutions, Tania's farm became popular (albeit controversial) and started to make a lot of money. However, Tania is not tech-savvy and relies heavily on AgriTech Solutions to manage and maintain the technology. Recently, Tania has become increasingly concerned about her heavy reliance on AgriTech Solutions and her own lack of cyber literacy. She worries about the potential risks to her farm's operations and data security. Additionally, Tania received an anonymous text claiming that AgriTech was skimming money and was selling the data generated by the machines without her consent.

Scenario Questions for Option #3

Your submission for this assignment should be in the form of a research paper and presentation that includes the following:

1. Identify and analyze **potential threats** to the farm's technology infrastructure, including cyber attacks on drones, autonomous tractors, robots, and satellite communications. Justify your answers.
2. Propose a multi-layered **security strategy** to protect the farm's technology infrastructure. Include cybersecurity measures, physical security measures, and data protection.
3. Develop a detailed plan for responding **to a specific security incident** (you choose one), ensuring minimal disruption to farm operations and maintaining data integrity.
4. Propose a plan to improve Tania's cyber literacy, including training and resources to help her better understand and manage the technology on her farm.
5. Develop a strategy to investigate Tania's concerns about AgriTech Solutions potentially skimming money or selling data. This should include auditing financial transactions and data usage and ensuring transparency in their operations.

Regardless of which option your group chooses, the most important thing is to have fun working and learning together on this assignment! 😊