Southern New Hampshire University

CYB 200 Project Two Guidelines and Rubric

Overview

This project is the creation of an **incident analysis brief** for your manager. Regardless of the level of protection and prevention an organization has in place, cybersecurity incidents occur. It is the response to the incident that may make or break an organization. As you progress through your degree, you will build your skills to prepare for all stages of incident response: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

A critical aspect of incident response is the ability to use information gained from an incident to improve the organization's security posture. The insight gained helps security professionals develop solutions that reduce the likelihood of similar incidents in the future while balancing the potential negative impacts those solutions will have on the people, processes, and technologies they ultimately affect. In this project, you will examine an incident that has occurred and use the Fundamental Security Design Principles to develop recommendations that will protect the organization in the future.

In this assignment, you will demonstrate your mastery of the following course competency:

- CYB-200-03: Describe fundamental principles of cybersecurity

Scenario

In a course announcement, your instructor will provide you with a scenario on which your work will be based. You will situate yourself as the security analyst in one of the provided scenarios, creating an incident analysis brief that explains to the security/IT director how the Fundamental Security Design Principles can be applied to strengthen the organization's security posture following the incident described in the case. You do not require specific technical information from the system beyond those supplied for you within the scenario. Rather, you should address each critical element in the Project Two prompt, speaking broadly to what your analysis and recommendations would be, based on your research from the course materials collected in previous modules.

Prompt

Using evidence from the scenario, prepare an incident analysis brief for your manager. In your brief, you should limit your analysis by selecting one security objective and two Fundamental Security Design Principles from the table below.

Security Objective (Choose One)	Fundamental Security Design Principles (Choose Two)
• Confidentiality • Integrity • Availability	• Separation (of domains/duties) • Isolation • Encapsulation

	• Modularity • Simplicity of design (economy of mechanism) • Minimization of implementation (least common mechanism) • Open design • Complete mediation • Layering (defense in depth) • Least privilege • Fail-safe defaults/fail secure • Least astonishment (psychological acceptability) • Minimization of trust surface (reluctance to trust) • Usability • Trust relationships

Specifically, you must address the **critical elements** listed below. Most of the critical elements align with a particular course competency, shown in brackets.

I. **Scenario Analysis:** Using your work in the case study analyses (Modules Two through Four) and other course resources as reference, select the security objective you think is most relevant to the organization in the case.
   A. Describe why the loss of your selected security objective (confidentiality, integrity, or availability) reflects the **greatest overall negative impact** on the organization. Use evidence from the scenario and your coursework to support your selection.
   B. Summarize the **negative impacts** on people, processes, and technologies associated with the loss of your selected security objective.

II. **Recommendations:** Select two Fundamental Security Design Principles as criteria, and recommend solutions to remedy the loss of the selected security objective based on your assessment of the incident.
   A. Explain how your solution **implements the selected Fundamental Security Design Principles**. Provide evidence from the scenario and your coursework to support your selections.
   B. Describe how your solution **balances impacts** on people, processes, and technologies.
   C. Explain which aspect of your solution you would recommend to your manager as the **most important to the organization**. Support your response with evidence from the coursework or scenario.

Southern New Hampshire University

Project Two Rubric

Guidelines for Submission: Your submission should be 3 to 5 pages in length (plus a cover page and references) and should be written in APA format. Use double spacing, 12-point Times New Roman font, and one-inch margins. Include at least three references, which should be cited according to APA style. Use a file name that includes the course code, the assignment title, and your name—for example, CYB_200_Project_Two_Neo_Anderson.docx.

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Scenario Analysis: Greatest Overall Negative Impact [CYB-200-03]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes how the selected security objective is most relevant to the incident's impact on the organization with evidence from the scenario and coursework to support the selection	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	19
Scenario Analysis: Negative Impacts [CYB-200-03]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Summarizes the negative impacts on people, processes, and technologies caused by the loss of the selected security objective	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	19
Recommendations: Implementation of Fundamental Security Design Principles [CYB-200-03]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Explains how the solution reflects the selected Fundamental Security Design Principles with evidence to support the selections	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	19
Recommendations: Balancing Impacts [CYB-200-03]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes how the solution balances impacts on people, processes, and technologies	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	19
Recommendations: Importance to Organization [CYB-200-03]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Explains which aspect of the solution is most important to the organization with evidence to support the explanation	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	19

Southern New Hampshire University

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Articulation of Response	Submission is free of errors related to citations, grammar, spelling, and organization and is presented in a professional and easy-to-read format	Submission has no major errors related to citations, grammar, spelling, or organization	Submission has some errors related to citations, grammar, spelling, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, or organization that prevent understanding of ideas	5
				Total	**100%**