Southern New Hampshire University

IT 380 Final Project Guidelines and Rubric

Overview

The world we live in is increasingly networked. So much of our vital information exists in digital networks—from financial transactions to social media, criminal records to private emails—that we cannot consider protecting them optional. The Global Risks 2015 report, published by the World Economic Forum, gives this unsettling observation: "Ninety percent of companies worldwide recognize they are insufficiently prepared to protect themselves against [cyberattacks]." With this in mind, it is not surprising that businesses and governments alike are continuing to seek better cyberdefense strategies, including hiring cybersecurity specialists. In this course, you learned the foundational principles and practices applied by these in-demand professionals to keep networked information secure.

For this project, you will assume the role of a training manager at a cybersecurity firm who decides to create a new-hire training manual for current and future information security analysts. The training manual will include a discussion of the purpose and value of cybersecurity, illuminate core tenets of cybersecurity, and illustrate best practices for addressing common cyberthreats.

The project is divided into **two milestones**, which will be submitted at various points throughout the course to scaffold learning and ensure quality final submissions. These milestones will be submitted in **Modules Two and Five.** The final product will be submitted in **Module Seven.**

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

- Articulate the value of cybersecurity principles for effectively assessing and mitigating risk within business environments
- Illustrate the core tenets of cybersecurity as they relate to balancing information security needs with functional business requirements
- Select general network defense policies and practices for safeguarding the confidentiality, integrity, and availability of information for users and organizations
- Compare and contrast methods for detecting, controlling, and mitigating specific types of malicious cyberattacks

Prompt

Scenario: You are the training manager at CyberLeet Technologies, a midsized firm that provides cybersecurity services to other businesses. CyberLeet's core customer base is sole proprietorships and other mom-and-pop shops that are too small to have their own IT departments and budgets. Generally speaking, your clients have a reasonably high risk tolerance, and put a premium on the functionality of their IT systems over stringent security measures. However, you also have clients that must protect highly sensitive information in order to continue operating successfully. For example, CyberLeet supports a few small public-accounting firms that need to maintain important tax-related information, as well as several day-care businesses that must keep children's health records private while allowing necessary access for certain caregivers. In the past year, CyberLeet has experienced rapid growth, which means you can no longer personally provide one-on-one training to every new information security analyst as they are hired. Therefore, you have decided to create a training manual that will explain to the current and future cohorts of new hires the essential principles and practices that they must understand in order to be successful in their role as information security analysts at CyberLeet.

Your training manual should address the following prompt: What are the essential cybersecurity principles and practices that an information security analyst must know and apply in order to be successful in their role? Make sure to use your Final Project Template for your milestones and final submission.

Specifically, the following **critical elements** must be addressed:

I. **Introduction: Welcome to CyberLeet**
   A. Explain the **value of** CyberLeet Technologies as a provider of **cybersecurity** services to its client businesses. Why is there demand for information security in a business environment? How do cybersecurity issues impact business resources, including finances, people, and time?
   B. Describe the overall **role of the new hire** as an information security analyst. What are the main functions of the job? What should be their ultimate goal once they are assigned to clients?
   C. Finally, explain the **purpose for this manual**. Why is it important that information security analysts apply the principles and practices outlined in this manual? What is at stake if they do not appropriately apply their training and provide high-quality services to the client businesses?

II. **Core Tenets of Cybersecurity**
   A. Explain the significance of **confidentiality** as a core tenet of cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context.
   B. Explain the significance of **integrity** as a core tenet of cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context.
   C. Explain the significance of **availability** as a core tenet of cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context.

III. **How to Develop Cybersecurity Policies**
   A. What principles should the information security analyst apply in order to develop appropriate **password policies** for their clients? Make sure you address confidentiality, integrity, and availability of information, as well as each of the following aspects:
      i. Password length and composition of the password (e.g., uppercase, numbers, special characters)
      ii. Time period between resets and ability to reuse a prior password
      iii. Differentiated policies for different types of users (e.g., administrator vs. regular user)
   B. What principles should the information security analyst apply in order to develop appropriate **acceptable use policies** for the client? Make sure you address confidentiality, integrity, and availability of information, as well as each of the following questions:
      i. What should users generally be allowed to do with their computing and network resources? When and why would each example be allowable?
      ii. What should users generally be prohibited from doing with their computing and network resources? When and why would each example require prohibition?
      iii. When and why should users be aware of acceptable use policies and how can organizations keep track of these policies?
   C. What principles should the information security analyst apply in order to develop appropriate **user training policies** for the client? Make sure you address confidentiality, integrity, and availability of information, as well as each of the following:
      i. How to determine who would be trained
      ii. How to determine how often trainings would occur
      iii. How to determine whether certain staff receive additional training or whether they should be held to higher standards

D. What principles should the information security analyst apply in order to develop appropriate **basic user policies** for the client? Make sure you address confidentiality, integrity, and availability of information, as well as each of the following questions:
    i. When and why should users have to display some type of identification while in the workplace?
    ii. What types of physical access (with or without ID) to company areas is acceptable? Why?
    iii. When and why should employees with identification be allowed access to all areas of the company?
    iv. When and why should employees be allowed to take work home or bring guests into the workplace?

IV. **Threat Mitigation Scenarios:** For each of the hypothetical scenarios listed below, illustrate for the new hires the strengths and weaknesses of the different approaches. This will help new hires gain a more practical understanding of how to deal with these types of issues that they are likely to face in their day-to-day job.
    A. **Theft:** In the last month, two break-ins have occurred at a client's office, which resulted in the theft of employee laptops during both incidents. The first incident occurred in the evening when the thieves broke through a ground-floor window. The second incident occurred during the day when the thieves walked right into the business area and removed two laptops. What physical and technical controls would be helpful to address the issue and prevent this type of vulnerability in the future? Compare and contrast the different methods that could be used to mitigate the given threat.
    B. **Malware:** Recently, one of your client's staff has been inundated with phishing emails that are targeted at individuals and related to current business opportunities for the company. These messages are linked to malware and sent by known threat actors. What physical and technical controls would be helpful to address the issue and prevent this type of vulnerability in the future? Compare and contrast the different methods that could be used to mitigate the given threat.
    C. **Your choice:** Create your own illustrative scenario of a common threat that an information security analyst may face. Explain what physical and technical controls would be helpful to address your chosen issue and prevent that type of vulnerability in the future, and compare and contrast the different methods that could be used to mitigate the given threat.

Milestones

Milestone One: *Training Manual Introduction*
In **Module Two**, you will assume the role of a training manager at a cybersecurity firm needing to create a training manual for new information security analyst hires. You will complete the introduction and core tenets of cybersecurity sections of the manual. **This milestone will be graded with the Milestone One Rubric.**

Milestone Two: *Policy Development*
In **Module Five**, you will complete the cybersecurity policy section of the manual. Remember, use the same template you used to complete Milestone One. **This milestone will be graded with the Milestone Two Rubric.**

Final Submission: *CyberLeet Training Manual*
In **Module Seven**, you will submit your final project. It should be a complete, polished artifact containing **all** of the critical elements of the final product. It should reflect the incorporation of feedback gained throughout the course. **This submission will be graded with the Final Project Rubric.**

Final Project Rubric

Guidelines for Submission: Your training manual should be 4 to 6 pages in length using 12-point Times New Roman font and double spacing. While not required, if you do use TestOut or outside sources in your training manual, cite these sources using the latest APA guidelines.

Instructor Feedback: This activity uses an integrated rubric in Blackboard. Students can view instructor feedback in the Grade Center. For more information, review these instructions.

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Introduction: Value of Cybersecurity	Meets "Proficient" criteria and demonstrates deep appreciation for the value of cybersecurity within business environments	Explains the value of cybersecurity services for businesses using specific supporting examples	Explains the value of cybersecurity services for businesses but is lacking in necessary detail or fails to use specific supporting examples	Does not explain the value of cybersecurity services for businesses	8
Introduction: Role of the New Hire	Meets "Proficient" criteria and demonstrates keen insight into the role of cybersecurity within business environments	Describes the role and ultimate goals of an information security analyst using specific detail	Describes the role and goals of an information security analyst but with gaps in accuracy or necessary detail	Does not describe the role and goals of an information security analyst	8
Introduction: Purpose of the Manual	Meets "Proficient" criteria and demonstrates deep appreciation for the value of cybersecurity within business environments	Explains the purpose of the training manual in terms of what is at stake for a business if it does not have appropriate cybersecurity policies and practices	Explains the purpose of the training manual but fails to clearly illustrate what is at stake for a business if it does not have appropriate cybersecurity policies and practices	Does not explain the purpose of the training manual	8
Core Tenets: Confidentiality	Meets "Proficient" criteria and demonstrates nuanced understanding of the core tenets of cybersecurity	Defines and explains the significance of confidentiality as a core tenet of cybersecurity, including specific details and examples to illustrate	Defines and explains the significance of confidentiality as a core tenet of cybersecurity but fails to illustrate with specific details and examples or contains inaccuracies	Does not define and explain the significance of confidentiality as a core tenet of cybersecurity	8
Core Tenets: Integrity	Meets "Proficient" criteria and demonstrates nuanced understanding of the core tenets of cybersecurity	Defines and explains the significance of integrity as a core tenet of cybersecurity, including specific details and examples to illustrate	Defines and explains the significance of integrity as a core tenet of cybersecurity but fails to illustrate with specific details and examples or contains inaccuracies	Does not define and explain the significance of integrity as a core tenet of cybersecurity	8
Core Tenets: Availability	Meets "Proficient" criteria and demonstrates nuanced understanding of the core tenets of cybersecurity	Defines and explains the significance of availability as a core tenet of cybersecurity, including specific details and examples to illustrate	Defines and explains the significance of availability as a core tenet of cybersecurity but fails to illustrate with specific details and examples or contains inaccuracies	Does not define and explain the significance of availability as a core tenet of cybersecurity	8

How To: Password Policies	Meets “Proficient” criteria and demonstrates keen insight into best practices for defending the confidentiality, integrity, and availability of information	Identifies specific principles for developing appropriate password policies that address confidentiality, integrity, and availability of information	Identifies principles for developing password policies but fails to fully address all relevant aspects or there are gaps in logic or accuracy	Does not identify principles for developing password policies	6
How To: Acceptable Use Policies	Meets “Proficient” criteria and demonstrates keen insight into best practices for defending the confidentiality, integrity, and availability of information	Identifies specific principles for developing appropriate acceptable use policies that address confidentiality, integrity, and availability of information	Identifies principles for developing acceptable use policies but fails to fully address all relevant aspects or there are gaps in logic or accuracy	Does not identify principles for developing acceptable use policies	6
How To: User Training Policies	Meets “Proficient” criteria and demonstrates keen insight into best practices for defending the confidentiality, integrity, and availability of information	Identifies specific principles for developing appropriate user training policies that address confidentiality, integrity, and availability of information	Identifies principles for developing user training policies but fails to fully address all relevant aspects or there are gaps in logic or accuracy	Does not identify principles for developing user training policies	6
How To: Basic User Policies	Meets “Proficient” criteria and demonstrates keen insight into best practices for defending the confidentiality, integrity, and availability of information	Identifies specific principles for developing appropriate basic user policies that address confidentiality, integrity, and availability of information	Identifies principles for developing basic user policies but fails to fully address all relevant aspects or there are gaps in logic or accuracy	Does not identify principles for developing basic user policies	6
Threat Mitigation Scenario: Theft	Meets “Proficient” criteria and demonstrates nuanced understanding of the different methods for detecting, controlling, and mitigating threats	Compares and contrasts different methods for mitigating the given threat, using specific examples to illustrate	Compares and contrasts methods for mitigating the given threat but there are gaps in accuracy, logic, or necessary detail	Does not compare and contrast methods for mitigating the given threat	8
Threat Mitigation Scenario: Malware	Meets “Proficient” criteria and demonstrates nuanced understanding of the different methods for detecting, controlling, and mitigating threats	Compares and contrasts different methods for mitigating the given threat, using specific examples to illustrate	Compares and contrasts methods for mitigating the given threat, but there are gaps in accuracy, logic, or necessary detail	Does not compare and contrast methods for mitigating the given threat	8
Threat Mitigation Scenario: Your Choice	Meets “Proficient” criteria and demonstrates nuanced understanding of the different methods for detecting, controlling, and mitigating threats	Identifies a common threat and compares and contrasts different methods for mitigating the chosen threat, using specific examples to illustrate	Identifies a common threat, and compares and contrasts methods for mitigating the chosen threat but with gaps in accuracy, logic, or necessary detail	Does identify a common threat and compare and contrast methods for mitigating the chosen threat	8

Articulation of Response	Submission is free of errors related to citations (if applicable), grammar, spelling, syntax, and organization and is presented in a professional and easy-to-read format	Submission has no major errors related to citations (if applicable), grammar, spelling, syntax, or organization	Submission has major errors related to citations (if applicable), grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations (if applicable), grammar, spelling, syntax, or organization that prevent understanding of ideas	4
				Total	**100%**