Southern New Hampshire University

IT 552 Final Project Guidelines and Rubric

Overview

The final project for this course is the creation of a **security awareness program proposal.**

In any type of enterprise, the security of property, information, products, and employees is of critical importance. Many security threats are caused by malicious intent, but, more often than not, security threats occur because of unintentional human error. In the final project for this course, you will evaluate the current security climate of an organization and develop a plan for mitigating against both malicious and unintentional human errors that could compromise the security of the organization. In addition to developing mitigation strategies, you must appropriately communicate those plans to the diverse, affected stakeholder groups for effective implementation. Ultimately, this assessment prepares you to successfully develop security awareness programs that not only protect the security of an organization's information, but also enhance the health of the overall security culture.

The project is divided into **four 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, Four, Six, and Eight.** The final proposal will be submitted in **Module Nine**.

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

- Determine the current security postures of various organizations by evaluating relevant human factors and applicable information security policies, practices, and processes
- Devise mitigation strategies that effectively protect against potential malicious and unintentional threats to organizations' security postures
- Propose strategies for appropriately resolving inoperative organizational factors that contribute to unhealthy security cultures in organizations
- Communicate key components of information technology security awareness programs to diverse stakeholders for effectively fostering healthy security cultures in organizations

Prompt

You were just hired as the new chief information security officer for a large corporation whose security posture is low. The first thing your chief executive officer tells you is that he has recently seen a presentation by one of the information security team members emphasizing the importance of having a security awareness program. As a result, you have been asked to develop a security awareness program based on the specific needs of the organization. To that end, you will make recommendations for enhancing security policies, practices, and processes that are currently contributing to a dysfunctional security culture. Your chief goal is to build a program that will foster a healthy security culture and ensure continuous improvement. Your final project is to create a **security awareness program proposal** that addresses the needs of this case.

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

Southern New Hampshire University

I. **Introduction**
   a) What is the **purpose** of your proposal? Why is the new security awareness program vital for the organization? Use specific examples to illustrate your claims.
   b) Overall, how would you characterize the **security posture** of the organization? What were the major findings in your risk assessment of the organization's current security awareness policies, practices, and processes?
   c) Specifically, are there **human factors** that adversely affect the security climate within the organization? If so, how? Be sure to consider unintentional and intentional threats to a healthy security culture.
   d) Specifically, are there **organizational factors** that contribute to an unhealthy security culture in the organization? If so, how? Be sure to consider organizational data flow, work setting, work planning and control, and employee readiness.

II. **Proposal**
   a) What is your proposal for mitigating the identified **human factors** that pose a threat to the organization's security posture? Describe the specific policies, processes, and practices that must be in place to address each of the following.
      i. **Unintentional Threats**: What strategies can protect against human errors made due to cognitive factors? What strategies can protect against human errors made due to psychosocial and cultural factors?
      ii. **Intentional Threats:** What strategies can protect against social engineering?
   b) What is your proposal for resolving inoperative **organizational factors** that pose a threat to the organization's security posture? Describe the specific policies, processes, and practices that should be in place to address each of the following.
      i. **Data Flow**: How do you make sure that the data sender and the data receiver have a sound connection? How do you ensure that data is not tampered with or altered from its intended meaning? What strategies do you propose to address poor communication?
      ii. **Work Settings**: What strategies do you propose to address distractions, insufficient resources, poor management systems, or inadequate security practices?
      iii. **Work Planning** and Control: What strategies do you propose to address job pressure, time factors, task difficulty, change in routine, poor task planning or management practice, or lack of knowledge, skills, and ability?
      iv. **Employee Readiness**: What strategies do you propose to address inattention, stress and anxiety, fatigue and boredom, illness and injury, drug side effects, values and attitudes, or cognitive factors (e.g., misperception, memory, or judgment)?

III. **Communication Plan**
   a) What **messaging strategies** should be used to ensure that stakeholders understand, buy into, and support the continuous improvement of your proposed security awareness program? Provide specific examples of the types of communication you are proposing.
   b) In a broader sense, how would you convince diverse stakeholders of the overall need for a healthy **security culture**? How do you make it real and relevant for nontechnical audiences?

Southern New Hampshire University

Milestones

Milestone One: *Statement of Work*

In **Module Two**, you will create a **statement of work (SOW)** based on the scenario provided in the Case Document. Be sure to include the purpose of the proposal, address the security concerns of the chief executive officer, explain why the security awareness proposal will be vital to the organization, describe how the security posture will be addressed, clarify how human factors will be assessed, and list any organizational factors that will contribute to the status of the security posture. The SOW should also address the scope of the work, project objectives, business needs, business goals, technical requirements, deliverables, tasks to achieve the deliverables, high-level schedule of completing the deliverables and tasks, and personnel and equipment requirements. The SOW will serve as the basis for developing the final proposal. The format of this assignment will be a two- to four-page Word document. **This assignment will be graded using the Milestone One Rubric.**

Milestone Two: *Security Policies Development*

In **Module Four**, you will submit 10 **security policies** as part of the planned solution to mitigate the security gaps identified in the Case Document. This assignment will include a list of access control policies addressing remote access, encryption and hashing (to control data flow), auditing network accounts, configuration change management (to reduce unintentional threats), segregation of duties, mandatory vacation (to mitigate intentional threats), personally identifiable information breaches, media protection, and social engineering. This milestone focuses on security functionality, and each policy should be no longer than one page. **This assignment will be graded using the Milestone Two Rubric.**

Milestone Three: *Continuous Monitoring Plan*

In **Module Six**, you will submit a **continuous monitoring plan** laying out the foundation for continuously monitoring the organization against malicious activities and intentional and unintentional threats. This milestone also focuses on work setting techniques and work planning policies to help employees improve their stress anxiety, fatigue, and boredom. As part of the planned solution, you will propose to mitigate the security gaps for the corporation given in the Case Document. You will need to explain what security tools (firewall, intrusion prevention system/intrusion detection system, antivirus, content filtering, encryption, etc.) and employee readiness strategies (training programs, rewards systems, physical wellness programs, etc.) will be used. The format should be a four- to five-page Word document. **This assignment will be graded using the Milestone Three Rubric.**

Milestone Four: *Communication Plan*

In **Module Eight**, you will submit a **communication plan** that addresses and summarizes the importance of a security awareness program. How can it enhance the success of the organization? The goal of the communication plan is to find and implement messaging strategies to gain senior management's buy-in and support of the security program. Cyber laws, personally identifiable information breaches and implications, costs of security breaches, and advantages of awareness programs should be addressed. The plan should also include how the awareness training and the security policies and procedures will improve the security posture and culture throughout the organization. The format of this assignment will be a Word document. **This assignment will be graded using the Milestone Four Rubric.**

Final Submission: *Security Awareness Program Proposal*

In **Module Nine**, you will submit the **security awareness program proposal**. It should be a complete, polished artifact containing **all** of the critical elements of the final proposal. It should reflect the incorporation of feedback gained throughout the course. The proposal will consist of the executive summary, communication

plan, statement of work, policies and procedures, proposed solutions to the security vulnerabilities, schedule for completing the proposed solutions, budget, and plans to continuously monitor the organization for malicious behaviors. This assignment will be graded using the **Final Product Rubric**.

Deliverables

Milestone	Deliverables	Module Due	Grading
1	Statement of Work	Two	Graded separately; Milestone One Rubric
2	Security Policies Development	Four	Graded separately; Milestone Two Rubric
3	Continuous Monitoring Plan	Six	Graded separately; Milestone Three Rubric
4	Communication Plan	Eight	Graded separately; Milestone Four Rubric
	Final Submission: Security Awareness Program Proposal	Nine	Graded separately; Final Product Rubric

Final Product Rubric

Guidelines for Submission: Written components of projects must follow these formatting guidelines when applicable: double spacing, 12-point Times New Roman font, one-inch margins, and APA citations. Page-length requirements: 25–30 pages (not including cover page and references).

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 (90%)	Needs Improvement (70%)	Not Evident (0%)	Value
Introduction: Purpose	Meets "Proficient" criteria and demonstrates keen insight or a nuanced perspective on the significance of security awareness programs	Illustrates the purpose of the proposal using specific examples that demonstrate why the program is vital for the organization	Describes the purpose of the proposal, but either does not include specific examples or those examples do not demonstrate why the program is vital for the organization	Does not describe the purpose of the proposal	8
Introduction: Security Posture	Meets "Proficient" criteria and demonstrates keen insight or a nuanced perspective in the evaluation of the overall security posture	Makes a justifiable claim about the overall security posture of the organization and supports using specific findings from the risk assessment	Makes a claim about the overall security posture of the organization, but it is either not justifiable or not well supported by findings from the risk assessment	Does not make a claim about the overall security posture of the organization	8

Introduction: Human Factors	Meets "Proficient" criteria and demonstrates keen insight or a nuanced perspective on the impacts of human factors on the security climate	Identifies specific human factors that adversely affect the security climate and illustrates their impacts using examples of relevant unintentional and intentional threats	Identifies human factors that adversely affect the security climate, but does not illustrate their impacts using examples of relevant unintentional and intentional threats	Does not identify human factors that adversely affect the security climate	8
Introduction: Organizational Factors	Meets "Proficient" criteria and demonstrates keen insight or a nuanced perspective on the impacts of organizational factors on the security climate	Identifies organizational factors that contribute to an unhealthy security culture and illustrates their impact using relevant examples of data flow, work setting, work planning and control, and employee readiness	Identifies organizational factors that contribute to an unhealthy security culture, but does not illustrate their impact using relevant examples of data flow, work setting, work planning and control, and employee readiness	Does not identify organizational factors that contribute to an unhealthy security culture	8
Proposal: Human Factors: Unintentional	Meets "Proficient" criteria and proposal reflects keen insight or includes creative solutions for effectively protecting against unintentional human errors	Proposes specific policies, processes, and practices to protect against unintentional human errors, including cognitive, psychosocial, and cultural factors	Proposes policies, processes, or practices that would not effectively protect against unintentional human errors, including cognitive, psychosocial, or cultural factors	Does not propose policies, processes, or practices for protecting against unintentional human errors	8
Proposal: Human Factors: Intentional	Meets "Proficient" criteria and proposal reflects keen insight or includes creative solutions for effectively protecting against intentional human threats	Proposes specific policies, processes, and practices to protect against intentional human threats, including social engineering	Proposes policies, processes, or practices that would not effectively protect against intentional human threats, including social engineering	Does not propose policies, processes, or practices for protecting against intentional human threats, including social engineering	8
Proposal: Organizational Factors: Data Flow	Meets "Proficient" criteria and proposal reflects keen insight or includes creative solutions for effectively protecting against inoperative organizational factors associated with data flow	Proposes specific policies, processes, and practices for protecting against inoperative organizational factors associated with data flow	Proposes specific policies, processes, or practices that would not effectively protect against inoperative organizational factors associated with data flow	Does not propose policies, processes, or practices for protecting against inoperative organizational factors associated with data flow	8

Proposal: Organizational Factors: Work Settings	Meets "Proficient" criteria and proposal reflects keen insight or includes creative solutions for effectively protecting against inoperative organizational factors associated with work settings	Proposes specific policies, processes, and practices for protecting against inoperative organizational factors associated with work settings	Proposes specific policies, processes, or practices that would not effectively protect against inoperative organizational factors associated with work settings	Does not propose policies, processes, or practices for protecting against inoperative organizational factors associated with work settings	8
Proposal: Organizational Factors: Work Planning	Meets "Proficient" criteria and proposal reflects keen insight or includes creative solutions for effectively protecting against inoperative organizational factors associated with work planning and control	Proposes specific policies, processes, and practices for protecting against inoperative organizational factors around work planning and control	Proposes specific policies, processes, or practices that would not effectively protect against inoperative organizational factors associated with work planning and control	Does not propose policies, processes, or practices for protecting against inoperative organizational factors associated with work planning and control	8
Proposal: Organizational Factors: Employee Readiness	Meets "Proficient" criteria and proposal reflects keen insight or includes creative solutions for effectively protecting against inoperative organizational factors associated with employee readiness	Proposes specific policies, processes, and practices for protecting against inoperative organizational factors around employee readiness	Proposes specific policies, processes, or practices that would not effectively protect against inoperative organizational factors associated with employee readiness	Does not propose policies, processes, or practices for protecting against inoperative organizational factors associated with employee readiness	8
Communication Plan: Messaging Strategies	Meets "Proficient" criteria and proposal represents highly effective or creative strategies for ensuring stakeholder comprehension and buy-in	Proposes messaging strategies for ensuring stakeholder comprehension and buy-in and illustrates with specific examples of proposed communications	Proposes messaging strategies that either would not ensure stakeholder comprehension and buy-in or does not illustrate with specific examples of proposed communications	Does not propose messaging strategies for ensuring stakeholder comprehension and buy-in	8
Communication Plan: Security Culture	Meets "Proficient" criteria and justifications are highly compelling or reflect a nuanced perspective on the importance of a healthy security culture	Justifies the overall need for and importance of a healthy security culture in a way that would be likely to persuade even nontechnical audiences	Justifies the overall need for and importance of a healthy security culture, but arguments are not compelling for nontechnical audiences	Does not justify the overall need for and importance of a healthy security culture	8

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