Southern New Hampshire University

IT 241: Final Project Document

Overview

The final project for this course is the creation of a presentation in which you will pitch a security awareness program to the executive team of a company. The presentation should include both the human element and the organizational side of operations. You will highlight the differences between intentional and unintentional threats posed by human beings and the organizational factors that impact the level of human error within an enterprise.

The purpose of the final project is for you to apply your knowledge about the human aspects of information security to a real-world scenario. People who work in the field of information technology are asked to provide information to executives so that informed decisions can be made about protecting the company from security threats. Information security training is of utmost importance in every company enterprise. While technologies such as antivirus software and encryption can offer some protection against cybercrime, security breaches are most often the result of human error and carelessness. One of the best ways to prevent employees from making costly errors with information security is to institute company-wide security-awareness training. It will be your job to design a presentation to gain buy-in from the executives in order to obtain approval for creating a security awareness program for the business, as well as raise overall awareness about how human factors can impact the security posture of any organization.

In this project, you will demonstrate the following course outcomes:

- Analyze unintentional human errors and malicious behavior for their impact on the security posture of an organization
- Illustrate potential predisposed and counterintuitive behaviors that affect organizational security postures based on appropriate models of human behavior
- Analyze organizational factors for potential risks from human error that impact the security posture of an organization
- Justify to enterprise stakeholders the importance of a security awareness program for fostering healthy security cultures

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. The milestones will be submitted in **Modules Two and Four.** The final project will be submitted in **Module Seven.**

Southern New Hampshire University

Prompt

Provide justification as to the importance of instituting an information security awareness program. You are not being asked to write the actual program, only to "sell" the idea to your audience. You will need to describe human behaviors that pose risks to organizations, why humans demonstrate these behaviors, and how a security awareness program could address some of the organizational factors that lead to human error, which in turn negatively impacts the security posture of an organization.

Using PowerPoint, Prezi, or a similar program, create a presentation that uses audio and/or slide commenting features. In your presentation, design a security awareness program pitch for the executive team of a company. The pitch should include both the human element and the organizational side of operations. Be sure to highlight the differences between intentional and unintentional threats posed by human beings and the organizational factors that impact the level of human error within an enterprise.

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

I. **Introduction:** Why is it important for a company to foster awareness of and mitigate against human factors in information security?

II. **Unintentional Human Error**
   A. **Human/Cognitive Factors**: What are some examples of human/cognitive factors that influence unintentional human error? How do these factors impact the security posture of the organization?
   B. **Psychosocial/Sociocultural Factors**: What are some examples of psychosocial/sociocultural factors that influence unintentional human error? How do these factors impact the security posture of the organization?
   C. What potential **predisposed and counterintuitive behaviors** are examples of unintentional human error?
   D. How can a company use this information to harden its **security posture**?

III. **Malicious Human Behavior**
   A. **Human/Cognitive Factors**: What are some examples of human/cognitive factors that influence malicious human behavior? How do these factors impact the security posture of the organization?
   B. **Psychosocial/Sociocultural Factors**: What are some examples of psychosocial/sociocultural factors that influence malicious human behavior? How do these factors impact the security posture of the organization?
   C. What potential **predisposed and counterintuitive behaviors** are examples of malicious human behavior?
   D. How can a company use this information to harden its **security posture**?

IV. **Organizational Factors**

A. How can **data flow** factors affect the company's security posture? Provide examples to support your claims.
B. How can **work setting** factors affect the company's security posture? Provide examples to support your claims.
C. How can **work planning and control** factors affect the company's security posture? Provide examples to support your claims.
D. How can **employee readiness** factors affect the company's security posture? Provide examples to support your claims.

V. **Conclusion**

A. What is a healthy **security culture**? Why is it important for a company to have a healthy security culture?
B. How can security **awareness training** programs promote healthy security culture in companies? How can these programs address the needs of various stakeholders?
C. How can security awareness training for enterprise stakeholders mitigate against unintentional human error that negatively impacts security cultures? What kinds of training or remediation strategies could be used in **addressing unintentional behaviors**?
D. How can security awareness training for enterprise stakeholders mitigate against malicious human behavior? What kinds of training or remediation strategies could be used in **addressing malicious behaviors**?
E. How can security awareness training for enterprise stakeholders mitigate against organizational factors that negatively impact security cultures? What kinds of training or remediation strategies could be used in **addressing organizational factors**?

Milestones

Milestone One: *Company Description*

In **Module Two**, you will describe the company that you will discuss in your final project. The company must be a real organization. It can be an organization other than a business, such as a nonprofit organization, a higher education institute, a government agency, or a hospital. **This milestone will be graded with the Milestone One Rubric.**

Milestone Two: *Presentation Summary*

In **Module Four**, you will submit a presentation summary that provides a narrative outline of the security awareness program pitch you will create for your final project. Your outline should summarize how you will address the critical elements listed in the final project prompt. **This milestone will be graded with the Milestone Two Rubric.**

Final Project Submission: *Security Awareness Program Presentation*

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 Product Rubric.**

Southern New Hampshire University

Final Product Rubric

Guidelines for Submission: The final project must be submitted as a presentation in PowerPoint, Prezi, or a similar program. It must use audio and/or slide commenting features. Sources should be cited in APA format.

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Introduction	Meets "Proficient" criteria, and explanation is exceptionally clear and contextualized	Explains why it is important for a company to foster awareness of and mitigate against human factors in information security	Explains why it is important for a company to foster awareness related to human factors but does not address the importance of mitigating against these factors, or the explanation lacks detail or is not accurate	Does not explain why it is important for a company to foster awareness of and mitigate against human factors in information security	5
Unintentional Human Error: Human/Cognitive Factors	Meets "Proficient" criteria and uses examples that are well informed and contextualized	Evaluates human/cognitive factors that influence unintentional human errors with regard to how these factors impact the security posture of the organization	Evaluates human/cognitive factors that influence unintentional human errors but does not connect the human errors to the impact they have on the security posture of companies	Does not evaluate unintentional human/cognitive factors that influence unintentional human errors	5
Unintentional Human Error: Psychosocial/ Sociocultural Factors	Meets "Proficient" criteria, and explanation is exceptionally clear and contextualized	Evaluates psychosocial/sociocultural factors that influence unintentional human error with regard to how these factors impact the security posture of the organization	Evaluates psychosocial/sociocultural factors that influence unintentional human errors but does not connect the human errors to the impact they have on the security posture of companies	Does not evaluate psychosocial/sociocultural factors that influence unintentional human error	5
Unintentional Human Error: Predisposed and Counterintuitive Behaviors	Meets "Proficient" criteria and provides relevant real-world examples to support claims	Determines potential predisposed and counterintuitive behaviors as they relate to unintentional human errors by using appropriate models of human behavior	Determines potential predisposed and counterintuitive behaviors as they relate to unintentional human errors but does not use the appropriate model of human behavior, or the behaviors described are not related to unintentional error	Does not determine potential predisposed and counterintuitive behaviors	5

Unintentional Human Error: Security Posture	Meets "Proficient" criteria, and examples provided are well informed and contextualized	Explains how companies can use information from human behavior models to harden organizational security postures	Explains how companies can use human behavior models but does not relate them to hardening organizational security postures or is not accurate	Does not explain how information from behavior models can be used	5
Malicious Human Behavior: Human/Cognitive Factors	Meets "Proficient" criteria, and description is exceptionally clear and contextualized	Describes human/cognitive factors that influence malicious human behavior with regard to how these factors impact the security posture of the organization	Describes human/cognitive factors that influence malicious human behavior but does not connect how these factors impact the security posture of the organization or the information provided is not accurate	Does not describe human/cognitive factors that influence malicious human behavior	5
Malicious Human Behavior: Psychosocial/ Sociocultural	Meets "Proficient" criteria, and description is exceptionally clear and contextualized	Describes psychosocial/sociocultural factors that influence malicious human behavior with regard to how these factors impact the security posture of the organization	Describes psychosocial/sociocultural factors that influence malicious human behavior but does not connect how these factors impact the security posture of the organization, or the information provided is not correct	Does not describe psychosocial/sociocultural factors that influence malicious human behavior	5
Malicious Human Behavior: Predisposed and Counterintuitive Behaviors	Meets "Proficient" criteria and provides real-world examples to support claims	Determines potential predisposed and counterintuitive behaviors as they relate to malicious human behavior by using appropriate models of human behavior	Determines potential predisposed and counterintuitive behaviors as they relate to malicious human behavior but does not use the appropriate model of human behavior, or the behaviors described are not related to malicious human behavior	Does not describe potential predisposed and counterintuitive behaviors	5
Malicious Human Behavior: Security Posture	Meets "Proficient" criteria, and examples provided are well informed and contextualized	Explains how companies can use information from human behavior models to harden organizational security postures	Explains how companies can use human behavior models but does not connect their use to hardening organizational security postures or is not accurate	Does not explain how information from behavior models can be used	5

Organizational Factors: Data Flow	Meets "Proficient" criteria and provides real-world examples to support claims	Describes data flow factors that influence the level of human error in companies and how these factors impact the company's security posture	Describes data flow factors that influence the level of human error in companies or how data flow factors impact the company security posture, but not both, or the information provided is inaccurate	Does not describe data flow factors that influence the level of human error in companies	6
Organizational Factors: Work Setting	Meets "Proficient" criteria, and the description is well informed and realistic	Describes physical work setting factors that influence the level of human errors in companies and how these factors can impact the company's security posture	Describes physical work setting factors that influence the level of human errors in companies or how these factors impact the company's security posture, but not both, or the information provided is incorrect	Does not describe physical work setting factors that influence the level of human errors in companies	6
Organizational Factors: Work Planning and Control	Meets "Proficient" criteria, and the description is well informed and realistic	Describes work planning and control factors that influence the level of human errors in companies and how these factors can affect the company's security posture	Describes work planning and control factors that influence the level of human errors in companies or describes how these factors affect the company's security posture, but not both	Does not describe work planning and control factors that influence the level of human errors in companies	6
Organizational Factors: Employee Readiness	Meets "Proficient" criteria, and the description is well informed and realistic	Describes employee readiness factors that influence the level of human error in companies and how can these factors affect the company's security posture	Describes employee readiness factors that influence the level of human error in companies or how these factors affect the company's security posture, but not both, or the information provided is incorrect	Does not describe employee readiness factors that influence the level of human error in companies	6
Conclusion: Security Culture	Meets "Proficient" criteria, and the explanation is based on relevant research	Comprehensively explains a healthy security culture and the importance of having a healthy security culture within a company	Explains a healthy security culture or explains the importance of having a healthy security culture within a company, but not both, or the information provided is incorrect	Does not explain a healthy security culture	5

Conclusion: Awareness Training	Meets "Proficient" criteria, and description is exceptionally clear and contextualized	Explains how a security awareness training program promotes a healthy security culture in companies and addresses various stakeholder needs related to information security	Explains how a security awareness training program promotes a healthy security culture in companies but does not address various stakeholder needs, or the information provided is not accurate	Does not explain how a security awareness training program promotes a healthy security culture in companies	5
Conclusion: Addressing Unintentional Behaviors	Meets "Proficient" criteria, and description is exceptionally clear and contextualized	Explains how security awareness training for enterprise stakeholders mitigates against unintentional human error, including details about the kinds of training or remediation strategies that could be used in addressing those behaviors	Explains how security awareness training for enterprise stakeholders mitigates against unintentional human error but does not include details about the kinds of training or remediation strategies that could be used in addressing those behaviors, or the information provided is not accurate	Does not explain how security awareness training for enterprise stakeholders mitigates against unintentional human error	5
Conclusion: Addressing Malicious Behaviors	Meets "Proficient" criteria, and description is exceptionally clear and contextualized	Explains how security awareness training for enterprise stakeholders mitigates against malicious human behavior and the kinds of training or remediation strategies that could be used to address malicious behaviors	Explains how security awareness training for enterprise stakeholders mitigates against malicious human behavior but does not include the kinds of training or remediation strategies that could be used to address malicious behaviors, or the information provided is not accurate	Does not explain how security awareness training for enterprise stakeholders mitigates against malicious human behavior and the kinds of training or remediation strategies that could be used to address malicious behaviors	5
Conclusion: Addressing Organizational Factors	Meets "Proficient" criteria, and description is exceptionally clear and contextualized	Explains how security awareness training for enterprise stakeholders mitigates against organizational factors that negatively impact security cultures and includes details related to the kinds of training or remediation strategies that could be used in addressing organizational factors	Explains how security awareness training for enterprise stakeholders mitigates against organizational factors that negatively impact security cultures but does not include details related to the kinds of training or remediation strategies could be used, or the information provided is not accurate	Does not explain how security awareness training for enterprise stakeholders mitigates against organizational factors that negatively impact security cultures	5

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 understanding of ideas	6
				Earned Total	**100%**