Southern New Hampshire University

ISE 640 Final Project One Guidelines and Rubric

Overview

As a cybersecurity practitioner, understanding the practice and application of digital forensics principles are necessary skills in all aspects of incident response. You will need these skills to effectively manage and resolve incidents that involve aspects of cybercrime, regulatory compliance, and legal concerns that arise in your organization. Additionally, you will often need to act as a domain expert communicating to a non-expert (as in a lawyer, executive, etc.)

In this course, you will perform basic forensic tasks in order to "walk a mile in the shoes" of a forensic practitioner. You will use the knowledge you gain in the practice activities to address a scenario. Your tasks will be to develop a technical investigative report and a non-technical memorandum (Final Project Part 2) that will assist your executive stakeholders and organizational attorneys in managing and addressing the aftermath of a particular incident.

You will complete a **milestone** for Final Project One in Module Seven, which is a draft of the Final Project One: Report. Ensure you review the feedback received on this milestone when your instructor returns it to you. **Final Project One** will be submitted in **Module Nine.**

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

- ISE-640-01: Apply chain of custody processes and procedures used by practitioners for maintaining evidentiary integrity [MS.CSE.CORE.04]
- ISE-640-02: Employ digital forensic tools and investigative practices to augment and enhance organizational incident response capabilities [MS.CSE.CORE.04]

Prompt

Write a clear analysis report of a specific security incident based on a provided scenario and template and exemplar based on experiences in lab(s).

Scenario: A management, director-level employee appears to have stolen intellectual property from a manufacturing company. The company is heavily involved in high-end development of widgets. This employee has access to corporate secrets and files. The employee is planning on leaving the company, taking the intellectual property with them, and going to work for a competitor. Due to some suspicions on the part of several managers, human resources (HR) notified the information technology (IT) department to monitor the employee's past history. An internal investigation is launched due to the employee's abnormal behavior. The IT department confirms that they have found large files and emails. Forensics identified unauthorized access, transmission, and storage of intellectual property by the employee. Evidence found will be used to support legal civil and criminal proceedings. Read the full forensic memo for all the necessary details.

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

I. **Executive Summary:** Set the stage for your report, providing a brief overview of the situation and the stakeholders who are involved.

II. **Legal Concerns:** Describe the problem(s) and objectives you are working with the company's attorneys to solve. [ISE-640-01]

III. **Relevant Procedures:** In this section, you will outline the steps that (hypothetically) you will have to take prior to or as you investigate in order to maintain evidentiary integrity. Use your experiences from other situations you engaging in within the lab environment to inform your responses.
   A. **Processes and Procedures:** Describe processes or procedures necessary for handing a criminal situation by internal employee. [ISE-640-01]
   B. **Chain of Custody:** Explain how to maintain the chain of custody as you investigate the various aspects of the incident. Support your response with specific examples. [ISE-640-01]

IV. **Details of Investigation:** Based on your experiences in the labs, there will be specific resources, methods, and tools necessary to support the investigation in the scenario.
   A. **Resources Needs:** Explain what resources (team knowledge, skills, and abilities) are necessary for gathering the evidence for this forensic investigation. Provide examples based on your experiences from the labs. [ISE-640-02]
   B. **Methods**: Describe the specific forensic method or approach you used to effectively leverage your available resources. [ISE-640-02]
   C. **Findings:** Describe the specific findings and the forensic tactics and technologies you employed to reach them. [ISE-640-02]

Milestones

Milestone One: *Report Draft*
In **Module Seven**, you will submit a complete draft of this report. **This milestone will be graded with the Milestone One Rubric.**

Final Submission: *Report*
In **Module Nine**, you will submit your Final Project One. 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 One Rubric.**

Final Project One Rubric

Guidelines for Submission: Your investigative forensic report must be 3–5 pages in length (plus a cover page and references) and must be written in APA format. Use double-spacing, 12-point Times New Roman font, and one-inch margins. Include at least 3 references cited in APA format.

Southern New Hampshire University

Critical Elements	Exemplary (100%)	Proficient (90%)	Needs Improvement (70%)	Not Evident (0%)	Value
Executive Summary	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Sets the stage for report, providing a brief overview of the situation and stakeholders involved	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	5
Legal Concerns [ISE-640-01]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes the problem(s) and objectives you are working with the company's attorneys to solve	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	15
Processes and Procedures [ISE-640-01]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes processes or procedures necessary for handling a criminal situation by an internal employee.	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	15
Chain of Custody [ISE-640-01]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Explains how to maintain the chain of custody while investigating the various aspects of the incident and supports response with specific examples	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	15
Resource Needs [ISE-640-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Explains what resources (team knowledge, skills, and abilities) are necessary for gathering the evidence for this forensic investigation and provides examples based on experiences from the labs	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	15
Methods [ISE-640-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes the specific forensic method or approach used to effectively leverage available resources	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	15

Southern New Hampshire University

Critical Elements	Exemplary (100%)	Proficient (90%)	Needs Improvement (70%)	Not Evident (0%)	Value
Findings [ISE-640-02]	Meets "Proficient" criteria and addresses critical element in an exceptionally clear, insightful, sophisticated, or creative manner	Describes the specific findings and the forensic tactics and technologies employed to reach them	Addresses "Proficient" criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	15
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%**