Shawn's C843 Task Guide

Develop a single submission that includes both parts I and II of the task. No particular format is specified in the requirements (see allowed file types on the Task Overview page). If you prefer to write a paper, I recommend using a truncated version of the task requirements points (A-I) as headers within your paper to ensure you answer all questions being asked and make answers easy for evaluators to locate. Prefer a PPT, see the template I've included. Template options are located in the Templates Folder of the SharePoint page.

Additional General Guidance:

- Make your answers to task requirements easy for the reader to locate and discern. Clearly articulate what you want to convey vs leaving things up for interpretation.
    - Use some variation of the task requirements points as headers for your work.
    - Be blatant in your answers, restate the question if necessary.
- Be specific. Don't be too general, or you'll get your submission returned. Use **specific** instances from the case study to support your points.
- Treat each section as an isolated section (i.e. sometimes you'll be asked to make a similar point in more than one section, in these cases, don't say "as mentioned above [in another section of the paper]", but rather reiterate what you mentioned above to answer the section in question as if it was being turned in without the rest of your work).
- Leverage one of the Templates options

Part I: Incident Analysis and Response

A – Success of the attack

Provide your theory of a plausible cause for the success of the attack based on occurrences stated as having happened, vulnerabilities stated as being present at the company, and conditions stated/eluded to have been introduced in the case study. Use specific people, specific instances, and specific vulnerabilities from the case study to reinforce your points.

Case Study: Bob, using his laptop that has not had OS or AV updates in over a year, visited an unfamiliar gaming website and clicked several links as he navigated it. Bob types an access code he received from one of the pages into the word document titled "ALL PASSWORDS" on his laptop where he keeps credentials and info for his bank account, email, WiFi, and gaming accounts. The next day, Bob noticed his laptop was behaving erratically, the $214.35 he had in his bank account was gone, contents of his ALL PASSWORDS file had been changed, and an unpleasant email had been sent to his email contacts.

Theory of a plausible cause: Due to Bob's lack of security education and poor practices, an attacker likely exploited a vulnerability in his system present due to outdated OS and virus signatures. Bob likely unwittingly installed a program that assisted the attacker. The attacker

likely gained a foothold leading to remote access capability resulting in theft of Bob's money, theft of Bob's credentials to masquerade as him, alteration of Bob's files…

B – CIA and PII Compromise

Provide at least one example of compromise for **each** (confidentiality, integrity, availability, PII) that occurred as a result of the attack. Be sure to use specifics from the case study. Use one or more industry standard frameworks mentioned in the task requirements or one of your choice that is applicable to help support your points for **two** of the compromises.

C – Federal Regulations

For purposes of this assignment, consider Azumer an extension of FEMA and bound to the same federal regulations as FEMA less regulations specific to the actual host federal organizations. Identify a federal regulation that were violated by the company. Discuss the specific instances from the case study that constituted the violations. See table within the task FAQs and Guidance spreadsheet to help identify an applicable regulation.

Note that this section is directly tied to section F. The specific violation you identify here and deem the company non-compliant with, will be the same one you will identify processes for in section F to bring the company into compliance with them.

D – Mitigation Steps

Discuss steps that need to be taken now to prevent the attack from causing further damage and mitigate the current impact. Reference the actions to do first in the NIST or other recognized incident response framework for ideas, but ensure your recommended steps are specific to what happened in the case study.

E – Incident Response Plan

Reference NIST or other recognized incident response framework to articulate how the steps in the plan would have addressed the occurrences in the case study to prevent/reduce impact of the attack, and how implementation of such a plan would prevent/reduce impact of other incidents and heighten company security posture.

Part II: Risk Assessment and Management

F – Federal Regulation Compliance

Provide recommendations of two processes to (1) address the specific violated federal regulation identified in section C that causes the company to be non-compliant with those regulations, and (2) raise overall information assurance levels. Discuss how implementing these recommendations would holistically increase company information assurance levels and security posture.

G – Technical Solutions

Provide recommendations for technical solutions to address remaining effects of the attack. If you addressed all effects of the attack already in sections D & F, specifically speak to the applicable technical solutions in this section (even if just reiterating). Review what type of controls or solutions are considered "technical" in nature (i.e. a *policy* involving encryption is an administrative control, while actually *encrypting* all data at rest is a technical control) to support your claims.

H – Organizational Structure

Identify (1) the positions/teams you recommend making up the structure (2) discuss the functions your recommended positions/teams will perform that address specific issues from the case study (3) articulate the arrangement/relationship the positions/teams have to each other within the organization and (4) articulate how, collectively, the structure will facilitate the efficient discovery and mitigation of future incidents thereby heightening the security posture of the organization.

I – Risk Management

Describe a risk management approach you would recommend the organization implement. I recommendation using a best practice 5-step risk management framework or similar as a baseline to tailor to the case study to assist you with accomplishing this. At a minimum:

- Provide your assessment of **two** specific risks identified in the case study in terms of likelihood, severity, and impact/potential impact to the organization.
- Based on that assessment, discuss how the organization should handle those risks that are in the best interests of the organization to reduce/prevent recurrence.
- Discuss how your recommended risk management approach will heighten overall security posture of the organization.