CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #11

Team:

Participants:

Logistics

A. Get together with other students on your assigned team in person and virtually.

B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.

C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1 *(8 points)*

Though the Information Security function is often located in the IT department, many now argue that this is not the best place for it. Why? What factors need to be balanced when selecting the reporting structure of the Information Security function?

Some people think that Information Security shouldn't belong in the IT department because the objectives and values are so distant. The Information Security function focuses on providing security to all the technologies, whereas IT focuses on the technology functioning correctly with no errors. The factors that are needed to balance when you select a reporting structure are figuring out who is reporting to who in Information Security. Within Information Security, they need to have their hierarchy because the items documented are entirely different from IT, so being able to separate allows both groups to guide their factions on what they should do.

Problem 2 *(8 points)*

Exabeam (a SIEM vendor) has an excellent primer on the modern Security Operations Center (SOC). Read it here: https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/.

Compare and contrast the key qualifications and duties of the Tier 1-4 employees of a typical SOC.

The qualifications and duties of Tier 1-4 employees at a SOC vary. A tier 1 employee is focused on alert investigation. Their job is to manage and configure security monitoring tools. They have system administration skills and are knowledgeable in web programming. They often have their CISSP. A tier 2 employee is known as an incident responder. They often have the same skills as tier 1, but experience in incident response as well. They are focused on deep analysis of incidents in order to put together the best possible response plan.

A tier 3 employee is expected to have high levels of incident response experience as well as penetration testing skills. These employees are likely to handle day-to-day vulnerability assessments, penetration tests, and threat-hunting activities. A tier 4 employee is the leader of SOC employees. They have the skills and experience of all tiers below them as well as extensive project management experience. They are the ones to set in place guidelines and policies and train their staff to adhere to the policies.

At what levels of Security Maturity would an investment in a SOC become realistic? *(2 points)*

At levels 4 and 5 investment in a SOC is realistic. At this level you are either considered advanced or security mature and likely have existing security infrastructure. A SOC is an expansion of your abilities to combat threats in an organized fashion.

Problem 3 *(7 points)*

Why would mandatory annual vacations for some (or all) employees be an important personnel control measure to consider?

Mandatory annual vacations for employees are important because it allows for an audit to be done on the employee's work to make sure that they are not misusing information systems or stealing. This also helps somewhat to prevent these actions from occurring because it increases the chances that bad actors will get caught and many bad actors at a company will avoid taking vacations because of fear of getting caught.