**CIS-481: Introduction to Information Security**

**InfoSec Chapter Exercise #11**

**Team: Project Team 11**

**Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson**

**Logistics**

1. Get together with other students on your assigned team in person and virtually.
2. 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.
3. 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**

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? *(8 points)*

**Answer**: The Information security is related to Information Technology, but an Information Technology specialist cannot deal with Information security as a whole. The both endeavors are totally difficult than each other, for information security of any organization the authorities should make another department having all possible specialists of data security such as a cyber security expert, cloud engineers, penetration testers, vulnerability assessor's, contingency planning experts and an IoT expert. This whole team in the organization should be considered as another department within any organization to secure digital assets of the organization (Sensitive information of organization, financial information of organization, client data of organization and almost all business confidential tasks of organization). In case if organization is at mid-scale or small-scale in which IT and Information security should be in a single department, then in this case the only remedy is the organization should be dynamic – the tasks should be carried out by specialized teams. The mid-scale organizations should even hire the cyber-security experts to procure the information security of the organization along with Information Technology experts. The security for the organizations is necessary in any case if the organization has digital promulgation of sensitive tasks of an organization

**Problem 2**

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. *(8 points)*

There are actually tier 1-4 employees obstructed by SOC

The tier-1 employee should be qualified in system administration skills such that he would be expert in programming languages such as python and ruby, the tier-1 employees configures security (overlooking), he overlooks security issues to be occurred in the organization , the basic security related tasks are carried up by tier 1 employee. He investigates the security alerts and vulnerabilities.

The tier-2 employee is a bit more experienced than tier 1 employee, he’s liable for incident or in case if any security issue occurs. The Tier-2 employee would manage this condition by planning and copes with the threat intelligence, he overlooks all the security issues and pertain a particularizing aspect of generating a better congregation of threat response.

The tier-3 employee is a bit more experienced than tier-2 employee. The high security officials cope with the high vulnerabilities within an organization. The vulnerability assessors, penetration testers or one can also count them as the threat hunters, no matter how harsh the vulnerability is? They cope a best initiative for better security measures for the organization, they have the same qualification but are more experienced to perform an outcome for these issues.

The tier-4 employee is most experienced that that of all previous tiers. They are responsible of hiring all the professionals and training for the project management

The tier-5 employee is an employee who is a specialist of hardware and software used in order to design information security policies.

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

Yes, it is realistic because it can might help an organization to ensure better security measures, no matter what the situation actually is, it can be proved helpful for the organization

**Problem 3**

Why would mandatory annual vacations for some (or all) employees be an important personnel control measure to consider? *(7 points)*

**Answer**: The mandatory annual vacation is necessary for the employees, but not all the teams should be given vacations together such that a chain might exist that if one employee is at vacation, the backup or other employee should regain his responsibilities to cope with the important control measures within the organization such that if they shouldn’t be given vacations than the task-productivity will be lost as a person needs a break after sometime to rewire himself, so that he could work more efficiently for the organization.