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

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
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:
When considering where the IT department should be placed; we must first consider the goal of the IT department in an organization. IT functions as a help desk that is able to handle the everyday troubles of regular employees in a corporation. Information security (IS) is the act of protecting intellectual property. This intellectual property can be protected through the various software and hardware implementations. After defining the IT departments function and the goal of information security; it is apparent that IT and IS have conflict ideals and should be located in different locations. IS protects intellectuals and should be kept away from regular employees and moved to a more secure location.

These are some factors that must be considered when selecting the reporting structure of the information security:

- Insurance and risk management: Will these changes cause more risk, and will insurance need to be applied for if something goes wrong?
    - Changes need to be risk free for the company to agree upon it.
- Legal department: Will the legal department agree with these structural changes?
    - These changes need to follow the legal structure of the company.
- Staffing: Who is going to work in this department?
    - Cyber security experts, cloud engineers, penetration testers, vulnerability assessor's, contingency planning experts and IoT experts are just a few individuals that will need to be selected.

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)*

Employee tiers:
Information was taken from a table located on this website: https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/

- **Tier 1 Analyst (Alert Investigator):** This sort of analyst should know some web programming languages, scripting languages and have a security certification. Alert investigators will need these skills to perform various tasks such as, monitoring SIEM alerts and configuring security monitoring tools. They monitor security issues that will occur in the system and designate the importance of alerted issues. Basic security related tasks are covered by tier one analysts.
- **Tier 2 Analyst (Incident Responder):** This analyst is similar to a Tier one analyst, but has more experience dealing with and responding to incidents. Incident responders must be able to perform advanced forensics, malware assessments, and threat intelligence checks. They also must be certified with a white-hat hacker certification or trained on it. Incident responders will be able to respond to the incident and perform an analysis on it. They will identify the attacker, the type of attack, and what system was attacked.
- **Tier 3 Analyst (Subject Matter Expert / Threat Hunter):** This analyst is similar to a Tier two analyst, but has more experience dealing with and responding to higher level incidents than tier two. Must be able to use penetration testing tools and cross-organization data visualization. They also need to know how to perform Malware reverse engineering. They will need to have previous experience dealing with identifying and developing responses to new threats and attack patterns. Subject matter experts or threat hunters will actively search for threats and vulnerabilities in their network in a regular workday. If an incident escalated they will join forces with incident responders and work together to stop the attack.
- **Tier 4 SOC Manager (Commander)**: Similar to tier three when considering qualifications. An additional qualification would be having a background in management, so that they can effectively communicate with the people that they are managing. They will distribute the workload among the employees. If an incident occurs employees should report to the commander. The commander will then contact and inform the appropriate to act upon the incident.

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

When security maturity reaches level 3-5 a company should consider investing in SOC. At level 3 the company is concerned about their security, but they do not have a budget. At level 4 they have a budget, but they do not have enough personnel to deal with incidents. Finally, at level 5 they have reached security maturity and can deal with all incidents that will occur.

Problem 3
Why would mandatory annual vacations for some (or all) employees be an important personnel control measure to consider? *(7 points)*

Answer: Mandatory annual vacation is necessary for employees. The CISO should work with the HR department to make sure that all of the employees are given an appropriate amount of off time. If an employee has time off they will have a clear mind when they come into work again. Information security is known to be a taxing job that requires many work hours. Vacation needs to be spread out appropriately so that an entire department doesn't lack personnel. 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. Every task must be documented regularly so the next employee can continue where the previous one left off.