CIS-481: Introduction to Information Security

Module 7 - Security and Personnel

Exercise #10

Team: 3
Participants: Ashley Aguilera Rico, Raveen Bryant, Ryan Foster, Yen Hsieh Hsu, Abby Nguyen

Logistics

A. Get together with other students on your assigned **Team** in person and/or 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 and may impact your performance on assessments, especially with respect to the essay questions.
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 *(9 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?

Information security is about managing the risk of using information, which involves almost everyone in the company. It shouldn't be located solely in one department, as it is involved all throughout the organization, since the practice of protecting information isn't only for one area. Factors that need to be balanced when selecting the reporting structure of the Information Security function are enforcing policy, consistent knowledge, and management structure (role specific job duties) as there needs to be consistency and upkeep for every area and step, in order to maintain order and upkeep. It needs to balance its duty to monitor compliance with its ability to provide education, training, awareness, and customer service needed to make information security an integral part of the organization's culture. It requires a top security office to report to an executive management group instead of the chief information officer.

Problem 2 *(10 points)*
Exabeam (a SIEM vendor) has an excellent primer on modern Security Operations Centers (SOC). Learn more about SOC roles and responsibilities here:

https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/

a) Compare and contrast the key qualifications and duties of the Tier 1-4 employees of a typical SOC. (*8 pts.*)

The SOC team continuously monitors and analyzes security procedures of an organization, where they defend against security breaches, and isolates and mitigates security risks. There are 4 tiers to SOC analysts. Tier 1 analysts monitor, prioritize, and investigate the alerts. Tier 1 analysts should have system administration skills, security certifications such as CISSP or SANS SEC401, web programming languages, and scripting languages. Tier 2 analysts are those that receive the incidents from Tier 1 and conduct further analysis to identify a strategy to deal with the threat. This tier requires more experience than Tier 1, may know advanced forensics and malware assessment, and may possibly have ethical hacker certification or training. Tier 3 analysts are those that conduct vulnerability assessments, review the threat, and actively hunt for the threats that have made it into the organization's network. Tier 3 analysts have similar skill sets and qualifications as Tier 2, but with even more experience to deal with high-level incidents. Lastly, there are the Tier 4 analysts. They are the SOC managers that are responsible for hiring and training of the staff and with strategizing. They are the organization's point of contact for security incidents. Tier 4 analysts' qualifications are similar to Tier 3's but with more management training and strong communication skills.

b) What differentiates a computer security incident response team (CSIRT) from a SOC team? *(2 pts.)*

CSIRTs are responsible for handling security incidents that arise. SOC teams are responsible for monitoring and analyzing security procedures of an organization.

Problem 3 *(6 points)*
Look up two (2) of the popular security certifications mentioned in Module 7 of the text and describe the requirements necessary to earn the certification and current associated cost for each.

To take the CISSP, it will require a minimum of 5 years of work experience as a security professional and it has to fall within 2 or more of the following 8 domains/areas of CISSP CBK: Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Domain 5. Identity and Access

Management (IAM), Security Assessment and Testing, Security Operations, Software Development Security. One year of the work experience can be replaced by either a 4 year college degree (or equivalent), or with an approved credential.

For CISM, similar to above, there is a need of 5 years of work experience also in the information security field, where at least 3 years of it should be related to information security management.

Prices:

- CISSP: $699
- CISM: $575 member/ $760 non-member