CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #11

Team: 3
Participants: Brandon Crosier, Aaron Gordon, Kitrina Justus, Sam Steele, Marvin Weaver

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)*

One major reason why people say the Information Security function shouldn't be located in the IT department is that Info Security has a different overall goal compared to Info Technology. The main goal of Info Security is to protect business assets while the main goal of Info Technology is to make the system run effectively. Some of the main factors they need to balance when selecting the reporting structures are education, training, awareness, and customer service.

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)*

A tier 1 employee is an alert investigator. The qualifications needed by an alert investigator are system administration skills, programming and scripting languages, and security certifications. The duties of an alert investigator are to monitor security information event management, or SIEM, as well as configure and manage the security monitoring tools. They also prioritize the alerts and ensures that a real incident is taking place.

A tier 2 employee is an incident responder. They need all the qualifications from the previous tier, as well as experiences with incident response, like advanced forensics, malware assessment, and threat intelligence. Certifications in white hat hacking are also recommended. The duties of the incident responder are to receive incidents and perform deep analysis, identify the threat, and identify the affected systems.

A tier 3 employee is a subject matter expert. The qualifications are similar to the previous tier but with even more experience including high-level incidents. They should also have experience with penetration tools and cross-organization data visualization and also be able to reverse engineer malware. A tier 3 employee duties include penetration testing, reviewing alerts and industry news. They also actively hunt for threats that have made it into the network. When a major incident happens they will join the tier 2 analyst in responding and containing it.

A tier 4 employee is a Commander. The qualifications are similar to the previous tier but include experience with project management skills, incident response management training, and strong communication skills. The duties of a Commander include hiring and training of SOC staff, they are in charge of the offensive and defensive strategy. They also manage resources, priorities, and projects and act as the point of contact for the business for security incidents.

A Security Engineer works with support and infrastructure. The qualifications to become a security engineer is a degree in computer science, computer engineering, or information assurance, also not uncommon to have the CISSP certification. The duties of a security engineer include being a hardware or software specialist, who specializes in the design of information systems and help create solutions and tools that help with the disruption of operations or hackers. Sometimes they are employed by the SOC and sometimes apart of support teams within the organization. While this is not one of the tiers, it is very important to the SOC.

The tiers all build on each other, getting more complex as they move up the ladder. The simplest role is the tier one alert investigator. It gets more complex as you move along, meaning that tier two, the incident response, performs tasks a little more complex, like identifying the nature of the threat. Tier three, subject matter experts, go through the system to identify threats instead of reacting to them like in tier 2. Tier 4, the commander, is the manager of all the other staff, meaning they must be well versed in all of the areas of the previous tiers. They are similar in that they all have the same base skills, but differ in the additional skills required by the job.

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

At Security Maturity levels 4 and 5 an investment in SOC would become realistic. Level 4 is where an organization has a budget to invest in this type of security. At this level, personnel is limited and potential needs to be maximized. In level 5 an organization can invest in this security as the company is knowledgeable about security and wants to continuously improve their program.

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

Mandatory annual vacations allow the company to review the employee's work while they are away. This measure is used to look at employees' behavior and evaluate whether they are acting ethically or not. Employees who are acting illegally, like those that steal from the

company, will be reluctant to take vacations as they will not be there to cover their tracks. Mandatory vacations act as a deterrent as it makes the employees consider the consequences of their actions, such as termination or criminal charges. This control measure is not typically thought of as one as it is a more subtle way of looking after your employees. Many employees who don't commit wrongdoings will see it as a benefit of their jobs, but an unethical employee will see it as a risk, leading to the company being able to identify those who may be misusing their access.