**Module 11 (30 points) – Chapter 12**

1. (Whitman & Mattord, 2016, p. 651) List and define the factors that are likely to shift or be subject to change in an organization’s information security environment.

The factors that are likely to shift or change in an organization’s information security environment are new assets, a shift in priorities, new partners, new hires, loss of old hires, and loss of old partnerships.

2. (Whitman & Mattord, 2016, p. 651) List and briefly describe the five domains of the maintenance model.

The five domains are external monitoring which looks at external threats, the internal monitoring that looks at the information assets inside an organization, planning and risk assessment that focuses on ongoing information security, vulnerability assessment that looks for vulnerabilities, and finally the readiness and review which looks over the program.

3. (Whitman & Mattord, 2016, p. 652) What is the difference between configuration management and change management? Give an example of systems that provide this functionality. Why are these management tools critical to cyber security?

Configuration management is the identity, inventory, and documenting of the info system. The change management is used to address changes to the base configuration. Ansible is an example of a configuration management tool, while changegear is an example for change management. These management tools are critical to cyber security because it keeps information on the system and changes that can be used to help find problems for possible threats.

4. (Whitman & Mattord, 2016, p. 652) List and describe four vulnerability intelligence sources. Which seems the most effective? Why?

Four vulnerability intelligence sources are vendors that provide support and communities to support each other, CERT organizations which provide notification services, public network sources which provide mailing lists and websites that are available for use, and finally the membership sites that offer more detail and the ability to filter. The most affective would-be vendors as they provide a direct and indirect means of support that also allows different communities to interact with and support each other.

5. (Whitman & Mattord, 2016, p. 652) Do the organizations NIST and SANS provide training? Give an example of a digital forensics resource available from NIST or SANS.

The organizations provide training and handbooks to help the workers. An example of a digital forensics resource available would be the national information security conference where they can teach the worker sent about digital forensics.

6. (Whitman & Mattord, 2016, p. 652) List and describe the five vulnerability assessments described in the text. Describe how ENCASE could assist in working with vulnerabilities?

The first is the internet vulnerability assessment which finds vulnerabilities in the public network. The second is the intranet vulnerability assessment that finds vulnerabilities within the internal network. The third is platform security validation which finds vulnerabilities in misconfigured systems of the organization. The fourth is the wireless vulnerability assessment that finds vulnerabilities within the wireless local area networks. The final one is documenting vulnerabilities which stores and tracks information about potential vulnerabilities. ENCASE could assist in working with vulnerabilities by helping analyze the images for potential EM.

**Bibliography**

Whitman, M. E., & Mattord, H. J. (2016). *Principles of Information Security*. Course Technology.