# ISEC 325 Homework 02

Answer the following questions based on your reading of the text books, the module key points, and the instructor’s presentation this week.

1. [3 points] What is information security and how does it differ from network security? How does network security fit into the McCumber cube (i.e. which cells does it cover)?

Information security is the protection of information while the network security is focused on the protection of the network itself. The network security would fall under the information security as its focus is the protection of the network, the information security will also look at the computer and data security. Network security falls under the security countermeasures of the McCumber cube which are training and education, policy and practice, and technology.

1. [3 points] What is the difference between an exploit and a vulnerability? A threat, a threat agent, and the subject of an attack? An asset and an object of an attack?

An exploit is a method that is used to compromise a system or take advantage of a vulnerability. A vulnerability is a weakness in a system that is open to attack. A threat is when something or someone presents danger or harm to an asset. A threat agent is an instance of a threat or part of a threat. The subject of an attack is the entity that is used to carry out the attack. An asset is the resource that is being protected while the object of an attack is the target for the attack.

1. [3 points] What is management’s role regarding information security policies and practices?

The management’s role is to protect the functionality of an organization through the enforcement of policies and practices.

1. [2 points] What are the components of an effective EISP? How does the EISP differ from the ISSP and the two SysSPs?

The components of an effective EISP is the development, implementation, and management of the security program through specified requirements. The EISP is used for the direction of the security for the organization overall while the ISSP is to guide the employees on how to use the technology. The managerial guidance SysSPs is made by management to guide the implementation and set up of technology and the behavior of the workers within the organization. The technical specifications SysSPs is created by the manager and the systems administrator to create the managerial policy for the different equipment.

1. [2 points] What is a security perimeter and what are the different types of perimeters organizations should look to implement?

A security perimeter is the boundary of the security for an organization. It can be pictured like an imaginary fence that reaches the end of the area in which the security can reach. The different types of security perimeters are the electronic security perimeter which is the end of the reach of the exterior network or internet connection or the physical security perimeter, which is usually a gate or fence that surrounds the perimeter of an organization.

1. [4 points] Compare and contrast “spheres of security” (figure 1-10 on page 29) against “defense in depth,”

The spheres of security are considered the foundation of the security framework. It is split into two spheres, the sphere of use and the sphere of protection. The sphere of use shows how people can access information. The sphere of protection shows that between each layer there needs to be a layer of protection. The defense in depth is similar as it is also a layered implementation of security. It focuses on having layers of security controls and safeguards which can be organized into policy and training. It helps train the people with how to defend against attacks but may not prevent them like the spheres of security. It also mentions adding redundancy at numerous points for protection.

1. [8 points] Research the ISO 27000 series of standards and the NIST 800 series of standards. Briefly compare and contrast the two. Include information about the goals of each, the approach each takes, and the applicability of each to, say, a midsize healthcare organization. *Note: I would expect to see some citations in this answer; please go beyond Wikipedia.*

The ISO 27000 series of standards is a family of standards that give an overview of information security management systems. The goal is to recommend the best practices for dealing with information risks through the implementation of security controls. The series is made up of several different standards and documents. The ISO 27000 series claims to be able to be applied by any size organization from any industry. The NIST 800 series of standards gives an overview for network security and policies. The series focuses on applicability to government and private organizations with a focus in the United States, unlike the ISO 27000 series which has a farther applicability range. The goal is to support the security and privacy of the federal government. The approach the NIST 800 takes is that it is reports on the guidelines for the Information Technology Laboratory.

-citation at bottom of the homework.

1. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about.  In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This week we investigated what exactly is information security. The meet and slides helped explain how while it protects the information, it also includes other groups such as network security and data security. I think that at first glance a person is likely to see information security as more of a data security and not realize that network security falls under the same umbrella. The software is important for security of information, but the hardware is just as important. A person can have their computer be an access point for a very secured server that is fortified from outside attacks but if someone managed to take their computer then they could have easy access. There is also the idea of a physical data bank that is inside a building and holds all the information for a company. If that data bank ends up breaking, then the company would lose all its information. Thinking more about the threats against information helps with the understanding of what is information security. I find that I like learning about security as there are a lot of scenarios that need to be covered and went through to make sure the system is not vulnerable.

Citation

*ISO IEC 27000*. ISMS.online. (n.d.). Retrieved May 29, 2022, from https://www.isms.online/iso-27000/

Thelma.allen@nist.gov. (2018, May 21). *NIST Special Publication 800-series general information*. NIST. Retrieved May 29, 2022, from https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information