**Module 1 (30 points) – Chapters 1 & 2**

1. (Whitman & Mattord, 2016, p. 41) What are the three components of the CIA triangle? What are they used for? What are the limitations of the CIA triangle?

Three components of the CIA triangle are confidentiality, integrity, and availability. The limitations for the CIA triangle are its inability to handle the evolved events and threats to security from human and inhuman threats to accidental or intentional damage. The three components are used as a means of determining if an information system is secure.

1. (Whitman & Mattord, 2016, p. 41) Identify the six components of an information system. Which are the most directly affected by the study of computer security? Do these components change over time? Give an example?

The six components of an information system are hardware, software, networks, people, procedures, and data. The ones most directly affected by the study of computer science are the people as they can improve the security with new knowledge of computer security or cause problems through human error. The six components stay the same meaning that it won’t change the type of components however within the components there are changes like how hardware will advance with the technological improvements made to the physical systems. An example of a change would be the floppy disks and how hardware has surpassed them meaning that the floppy disk reader was removed from the computer box. The disk drive was later removed as well when most of the games and applications went digital.

1. List and describe the phases of the SDLC. In your own words, summarize the additional requirements involved in the SecSDLC phases. Name some other development tools.

The different phases of the SDLC are investigation, analysis, design, implementation, and maintenance. Investigation starts with looking into the plan that will be use for the process. Analysis looks at the information gathered in the previous phase and determines what the new system will need to do. Design is split into logical and physical as it starts with planning out what is needed to create the new system during logical then physical will help decide on the specifics and work to acquire them. Implementation creates the needed software and helps put together the physical components gathered during the design phase. Maintenance will be a longer process as it keeps the system up to date and works on solving and problems that occur in its life. Additional requirements involved in the phases would include determining the life expectancy for the parts used to create the system and any future updates that would be needed. Other development tools would include some software tools like DevOps and RAD.

1. (Whitman & Mattord, 2016, p. 41) Why is a methodology important in the implementation of information security? How does a methodology improve the process? How does an organization determine which methodology to use?

Methodology is important as it creates steps to follow that the person can use during the implementation process. The methodology helps improve the process as it keeps steps from overlapping and causing confusion in the structure like if a section is to be implemented prior to another for the latter to work, the structure will help stop problems like this and help with pacing. Organizations can determine which model to use based off what they plan to implement and the connections each part has with one another. The waterfall methodology follows a step by step which helps when the different parts rely on the previous one to function like how the SDLC will start with investigation and needs this part to be able to work on analysis.

1. (Whitman & Mattord, 2016, p. 103) How is technological obsolescence a threat to information security? How can an organization protect against it? What would you do as a security manager if you are required to maintain legacy technology?

Technological obsolescence is when the technology is outdated or antiquated. This is a threat as most outdated technology will not have continued support from the companies meaning that fixes to help solve problems will not be implemented. For example, a computer that runs the latest Windows version will have an updated firewall as Microsoft continues to account for new threats, however, a system that runs Windows vista will not have these updates and are more susceptible to hackers and breaks into the systems. Organizations would be best able to protect against this by updating their systems and technology. If I was required to maintain legacy technology I would see about using newer technology as an access point to the legacy. To access the legacy technology if we have access points using the same technology then it would lead to multiple weak points with possible attack sites that can not be reinforced. If we use newer tech as the access point to the legacy technology and have the other access means offline then it would help create a smaller means of access that can be updated to protect the technology.

1. (Whitman & Mattord, 2016, p. 103) What methods does a social engineering hacker use to gain information about a user’s login id and password? Is it a good idea for a security manager to be widely seen on many social media sites?

Social engineering hackers will pretend to be IT workers for an organization to get the user’s information by offering help to low-level employees. It is a good idea for a security manager to be seen as it helps the workers to know who the manager is and to eliminate hackers pretending to be the security managers.

1. (Whitman & Mattord, 2016, p. 104) Using the categories of threats mentioned in Chapter 2, and the various attacks described, review several current media sources and identify examples of each threat.

The first threat is compromises to intellectual property with a current example of pirating sites used for movies and music such as Bitlord where people can upload the copyrighted property and let others download it without following the laws in place to protect the intellectual property. The second threat is deviations from quality of service can be shown in the internet speed that a company will sell to users being different from what the systems will run. Espionage or trespass is a topic that covers data collection which lately has been a discussion about Facebook and what they collect from the users. Forces of nature can be shown through the latest articles of the hurricanes hitting the south coast and the towns that are without power or internet through this storm. Human error comes in the form of a person accidentally leaking information like Tom Holland with the Spiderman movies or how a subway has been out due to human error across an entire city. Information extortion has been happening in the medical field lately with hackers obtaining people’s medical files and threatening to leak it unless the hospitals can comply. Sabotage can be seen with companies that have had multiple system wipes leading to the fall of some major companies. Software attacks are threats that can be found a lot when it comes to new software updates as they have yet to have patches to cover possible holes. Technical hardware failures have problems such as lately causing blackouts within cities. This could cause big problems if there is hardware failure in a dangerous place like a nuclear power plant. Software failures can be found with the code problems when a site it unreachable after it drops an update, this is seen in a lot of social media sites and can last a short or long time. Technological obsolescence can be seen with the example of Apple and their support for older IOS systems and phones being dropped so they can focus on the newer technology. Theft can be shown with people loosing their accounts or having their tech stolen.

**Bibliography**

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