**Module 2 (30 points) – Chapter 3**

1. (Whitman & Mattord, 2016, p. 147) What is the difference between law and ethics? Why are laws and ethics relevant to information security?

The difference between law and ethics is how they are created and withheld. Ethics falls under philosophy and solves dilemmas based on moral judgements which can be seen as a gray area because people can have different morals. Laws are created rules that must be abided as failure to abide by them can result in a prechosen punishment. For example, an ethical dilemma in information security would be informing staff of a potential data leak. Ethics would have different possible outcomes with the choices and pros and cons for each choice. This could be telling them could cause panic or not telling them puts their information in danger. The laws would come into with the protection of the information. If a past employee has signed a nondisclosure, then proceeds to disclose that information then the law would hold them accountable for breaking this agreement as the company can take them to a court of law.

1. (Whitman & Mattord, 2016, p. 147) What is privacy in an information security context? Why does an organization need a Chief Privacy Officer (CPO)?

Privacy in an information security context is that people have the right to protect their information from others. The Chief Privacy Officer helps with protecting the information and determining when information is allowed to be disclosed. For example, a customer wants their information disclosed, the CPO would deem what information can be disclosed to follow this request.

1. (Whitman & Mattord, 2016, p. 148) How does the Sarbanes-Oxley Act of 2002 affect information security managers? Has the Sarbanes-Oxley Act failed?

The Sarbanes-Oxley Act affect information security managers by giving them the ability to determine which information is confidential and the integrity of the information. The act leads to the IT managers to verify the information through the information security managers. The SOX Act has failed when not delineating IT from the non-IT workers’ control which leads to problems as the controls are expected to be for IT.

1. (Whitman & Mattord, 2016, p. 148) How is due diligence different from due care? Which is most important?

Due diligence is the steps that are taken to meet the obligations set in place by the law while due care are steps employees follow for the rules that the organization set in place. The most important of these two step groups would be due diligence as the steps are regulated by the states or countries that the organizations reside in.

1. (Whitman & Mattord, 2016, p. 148) What is a policy? How is it different from a law? Give an example of a policy.

A policy is a guideline that organizations will use to determine procedures the company will follow. This is different from a law as these are set by the organizations and ignorance of a policy is acceptable while ignorance of a law is not. An example of a policy would be that the employees must sign out during their breaks and sign in once it is done. This is in place so if a company pays hourly then they would not need to include the hour the person is on break. Being ignorant of this will lead to a scolding or having someone explain the policy while the law would have led to a punishment.

1. (Whitman & Mattord, 2016, p. 148) What is the best method for preventing an illegal or unethical activity at a business?

The best methods for preventing an illegal or unethical activity are educating others on the ethics and laws, working to lessen the chances of accidents occurring, and deter people who are intent on not following the ethics and law.

1. (Whitman & Mattord, 2016, p. 148) Using the resources available in the library or online, find out what laws Ohio has passed to prosecute computer crime. What is the value of the following website in relationship to information security: <http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx> ?

Based on the website, the value in relationship to information security is well covered and protected. The sections explain what they consider to be computers and the threats that could occur like the Trojan horse or worm.

**Bibliography**

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