**Questions for IT 570 (2018)**

**Answer any three (3) questions from the listing below!**

1. Cybersecurity law is a branch of information technology law that is primarily concerned with the protection of computers, computer systems, computer networks and related digital technologies from all forms of criminal misuse and malicious threats. Cybersecurity law operates in three areas. Define each area and discuss the extent to which these three areas can be effective in protecting computer networks from criminal misuse and malicious threats. Use examples and cases to aid your response. Include any national or state policies, laws or institutions that may apply to your examples or cases.
2. The *United States International Strategy for Cyberspace (on canvas)* goal is to work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. Discuss the importance of international law in cybersecurity and using this document discuss the role of the Budapest Convention in expanding international cybersecurity laws. Also, discuss the impact of norms and diplomacy in achieving international cybersecurity laws.
3. Cybersecurity programs are developed at many organizational levels. Define cybersecurity policy and discuss the how cybersecurity policy goals can be created in an organization of your choice. Language and tone is an important part of cybersecurity policy. Discuss this importance along with addressing the role of the enforcement, training and awareness sections in cybersecurity policies.
4. Define Cybersecurity Governance/ IT Security Governance and discuss the responsibilities in protecting information assets. Compare and Contrast between the ISO and COBITT Governance framework. Describe each framework the domains they include. Are there advantages and disadvantage to using them?
5. Cyberethics is a fairly new field that covers the legal and morality of cybertechnology. Define Cyberethics and discuss how security professionals can apply professional ethics in their relationships throughout their career. Which ethical framework guides your decision-making process?
6. Do we really have privacy in the United States? Define privacy and the dimensions of privacy. What laws protects our privacy? Explain the anatomy of a privacy policy.
7. Risk Managements is seen an essential part of organizational operations to allocate scare resources. Explain how cybersecurity risk may be assessed whether qualitatively or quantitatively and the effectiveness of using NIST risk management framework. (*NIST 800-30 Rev 1 is on canvas*).
8. Continuous monitoring will aid in risk management processes. Define continuous monitoring and explain how this process aid risk management practice in an organization. Define security metrics and state the value of these metrics? Explain the challenges of establishing meaningful security metrics. (*Use the SANS Institute guide to security metrics to help answer this question).*