Unit 1 Critical Thinking Questions

1. **Define cybersecurity in your own words. Describe at least ONE way in which cybersecurity is relevant to how you are taking this very course.**

Cybersecurity to me is the protection of internet-connected systems. The ultimate goal is to protect against unauthorized access to data centers and other computerized systems. Cybersecurity is relevant to this course, as different students are always submitting assignment online onto the same server. Cybersecurity allows the protection against the tampering of the students' assignments, and the exposure of anything they are submitting which could contain some personal information.

2. **You read about six categories that make up computer crime. Choose three of these categories and describe a specific example of cybercrime in the real world related to each of your three chosen categories.**

Three categories that make up cybercrime include **malware, social engineering, and DDoS**. **Malware** is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. A real-world example of Malware is WannaCry. WannaCry is a form of ransomware, noted as one of the worst ransomware attacks in history. This threat encrypts data on Windows computers and demands Bitcoin payment for your data to be "unencrypted." **Social engineering** is the psychological manipulation of people into performing actions or divulging confidential information. A real-world example of a social engineering attack is during the 2016 presidential election. This attack led to the leak of emails from the Democratic Party that may have influenced the result of the election. Phishers created a fake Gmail account, inviting users through a link, to change their passwords due to unusual activity on their accounts. These phishers then had access to hundreds of emails containing sensitive information about the Clinton campaign. A **DDoS** (Distributed Denial-of-Service Attack) occurs when multiple systems flood the bandwidth or resources of a targeted system, resulting in the resource being unavailable to its intended users. A real-world example of a DDoS attack was in 2020, in which AWS (Amazon Web Services) suffered this kind of attack. This was the most extreme recent DDoS attack ever and it targeted an unidentified AWS user using a technique called Connectionless Lightweight Directory Access Protocol (CLDAP) Reflection. This technique relies on vulnerable third-party CLDAP servers and amplifies the amount of data sent to the victim's IP address by 56 to 70 times. This prevented the user from being able to load

into the service. The attack lasted for three days and peaked at an astounding 2.3 terabytes per second.

3. **Imagine you have borrowed your friend's computer to work on a class project. Checking the computer out, you notice they've left their web browser open and are signed into their email account. Would it be considered a computer crime to read their email, even though you didn't "hack" their password? What if they had left a text file on their desktop that included personal information, like their social security number, banking and credit card information, passwords for sites, etc., but didn't have it password protected—would accessing that file be a computer crime, even though there was no password protection on it? Explain your answers.**

Theoretically it would be a computer crime, even though no hacking was needed. The reason for this is because you still are accessing private information that should not be accessed by anyone else but you. This creates the risk that their accounts could be signed into by other people. Let's say this situation happened to me and I saw my friends personal information, since I now know the information I could share it with other people. Because of this, other people would now also now their personal information. Another reason is because this is an Invasion of Privacy, which is a defined computer crime. In California, invasion of privacy is a misdemeanor. The crime is punishable by imprisonment in county jail for up to six months, and/or a maximum fine of $1,000.

4. **Name at least two types of businesses that need to practice information assurance (IA) and explain why it is important to them.**

Information assurance is very important for tech organizations such as Microsoft, Google, or Apple. This is because most of the world uses devices made by them. This means that the world is dumping their personal information onto these devices, which means if they were to get hacked lots of personal information would be exposed. Information assurance is also very important for agencies of the federal government. This is because so much sensitive top-secret data is stored on government devices, which many users having access to them. So if the users' data were to be exposed, the top-secret info within the government could be exposed to the world and other countries could use that to their advantage.

5. Describe the concept behind a digital signature and explain how it relates to cybersecurity by providing a hypothetical example of a situation in which a digital signature could enhance cybersecurity.

A digital signature is a is a mathematical scheme for verifying the authenticity of digital messages or documents. It relates to cybersecurity, because they reduce the risk of duplication, alteration, or interception of the information being sent from one computer to another. Digital signatures ensure that signatures are verified, authentic and legitimate. Suppose there is a XYZ company, which is a client of ABC consultancy. They decide to use an authentication protocol, so that reliable communication is possible. The use of a digital signature would be beneficial in this case since the company would know that their messages are verified and not from someone else pretending to be them, as they would be alerted if anything of the message has been changed after the signing.