IAS INFORMATION ASSURANCE and SECURITY

Name: Mary Rose M. dela Torre **Section:** BSIT 3C (T209)

Activity A

Instruction:

Recall the History of information security and provide what is asked on the statements below. Write your answer on the space provided.

Guide questions:

1. During the early years, what were the primary threats to information security?

During the early years were information security was a straightforward process which composed of pre-dominantly of physical security and simple document classification schemes. The primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage**.**

Physical theft takes other people's property by force or without them knowing. Theft can take place on all the items making up the stock of computer equipment. Such thefts may be committed in the premises of a company or while computer hardware is in transit. The theft of IT equipment can lead to serious consequences. The damage suffered can be, Identity theft, loss of productivity, access to networks and so on.

Espionage against the products of the systems, refers to the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. This activity is a covert practice often done by an insider or an employee who gains employment for the express purpose of spying and stealing information for a competitor. Industrial espionage is conducted by companies for commercial purposes rather than by governments for national security purposes.

IT sabotage is the type of crime many people associate with insider threat. We define IT sabotage as cases in which current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of harming a specific individual

2. What is ARPANET and what was its relationship to the internet?

Arpanet was the first wide-area packet switching network with distributed control and one of the first network to implement the TCP/IP protocol sites. The Arpanet and

Internet were primarily computer network that established the technical groundwork and social expectation for wide area networking in the United States.

Arpanet was a testing ground for innovative concept such as pocket switching. The Arpanet and internet were socially constructed artifacts whose design was shape by interest and worldview of their creator.

Arpanet and internet are further illuminated by contrast with alternative networking system.

3. During World War II the Enigma was used to decrypt information transmissions. Why?

Enigma was a type of enciphering machine used by the German armed forces to send messages securely. Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. The rotor mechanism changes the electrical connections between the keys and the lights with each key press. It is primarily used for security purposes. he security of the system depends on a set of machine settings that were generally changed daily during the war, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station has to know and use the exact settings employed by the transmitting station to successfully decrypt a message.

4. When was the concept of computer security evolved into the more sophisticated system we call information security?

Computer security consisted of securing a system's physical location with badges, keys, and facial recognition. To ensure total security, the information itself, as well as the hardware used to transmit and store it, needed to be protected.

It was during the 1960s when organizations started to become think and more protective of their computers. Accordingly, there was no internet or network to worry about, so security was largely focused on more physical measures, and preventing access to people with enough knowledge about how to work a computer. Passwords and multiple layers of security protection were added to devices. Fire safety measures were also implemented, to ensure that the stored data was protected.

5. Describe the changes that happened during:

a. 1990s?

With the internet becoming available to the public, more and more people began putting their personal information online. Because of this, organized crime entities saw this as a potential source of revenue, and started to steal data from people and governments via the web.

- By the middle of the 90s, network security threats had increased exponentially and, as such, firewalls and antivirus programs had to be produced on a mass basis to protect the public.

- It was a NASA researcher who created the very first firewall program design, following a computer virus attack at their California base.
- Firewalls and antivirus programs helped protect against this, but the web was a mostly unsecured and rapidly burgeoning network.

b. 2000 to Present?

While governments had been pursuing cyber criminals for decades, most punishments were light, often being limited to a confiscation of computer equipment and a ban from computer use for a certain period of time.

- This changed in the 2000s as governments started to recognize the dangers of hacking.

Hackers were jailed for years as punishment for cybercriminal activity.

- By 2010, high-profile hackers were getting decades in prison for cybercrimes.
- Encryption occurs at multiple levels, including on digital files, networks and during data transmissions.
- Organizations now also implement comprehensive information security policies that prevent their employees from making any mistakes that make data accessible to intruders.