# LECTURE 1

18700714

JAMIN ANDONG

# CYBERSECURITY

- Cyber security involves the storing of data, securing it, and it's use of information and storage of it. It' significance lies in how widespread it is and why it should be regarded seriously; it can be used for good (ethical) or malicious intent.
- Common types of attacks in cyber security include viruses, malware, phishing, denial of service (DOS), and advance persistent threats.

- **Viruses** are strips of codes that cause a computer to malfunction; they can be disguised in many forms.
- **Malware** are installable files that are also disguised to a user that then stay within a computer's operating system; they can block off computer networks and take over them.
- **Phishing** is a type of attack in the form of e-mails that steal the user's data if the links within them are followed.
- **Denial of Service** is when a network or server is overloaded with requests that eventually crash it. DDos refers to Distributed Denial of Service when these requests come from multiple system.
- **Advance persistent Threats** are specifically planned to invade a network and eventually gain knowledge of a system's ins and outs so as to take over the system.

# CYBER SECURITY PROFESSIONALS

- There are different fields in cyber security with different roles, and they include:
  - **Security Analysts** – study vulnerabilities with in networks, software, and hardware and come up with tools to deal with said vulnerabilities.
  - **Cryptographer/Cryptologists –** research stronger encryption algorithms for better security and protection.
  - **Security Architect –** as the name implies, they create security systems and focus mainly on policies, ethics, and frameworks of a system/network.
  - **Security Software Developer –** create tools and software to detect and prevent attacks.
  - **Chief Information Security Officer –** head of information security and manages all that goes on within it.

# CIA TRIANGLE IN CYBERSECURITY

- **Confidentiality** – this involves who has access to sensitive information; it needs to be the right person and not the wrong one.
- **Integrity –** data must not be changed or modified by those who are not authorized.
- **Availability –** the data must be accessible by an authorized user at required times.

# FULLY DIGITAL ENTERPRISE

- A fully digital enterprise is an organization that is completely automated. This increases efficiency and speed in productivity.
- It does come with it's faults, as posited by Spremic and Simunic in their article of the same topic. There have been several catastrophic breaches made in digitized companies due to it's reliance on technology. If a company's security is breeched, they are on track to lose up to billions of dollars worth of money, loss of customers and their trust, and just an unfavorable image in general. Their security network would virtually need to be built up again avoid future risks.
- It is important to routinely update security and check for vulnerabilities.

# RESOURCES

- https://www.techtarget.com/searchcio/definition/Digital-enterprise
- http://www.iaeng.org/publication/WCE2018/WCE2018_pp341-346.pdf