Unit 1: Network and Information Security Management: History & Definitions

Objectives:

- Define the four tenets of security and understand how they underpin the field of Information Security.
- Become familiar with the key international standards that define Information Security Management.
- Review the two core concepts of Information Security – vulnerabilities and threats – and understand how they are related and how they can be classified and assessed.
- Identify a range of professional roles available in the Information Security field.

Outcomes:

- Explain the basic principles of Information Security Management.
- Describe the four tenets/ principles of Information Security Management.
- Describe what constitutes a threat and vulnerability.
- List several typical roles within the Information Security profession.

Reflection:

Information security is the identification of individuals who possess information security, the detection of vulnerable areas, the prevention of threats, and the implementation of preventative measures and research to ensure information security and protection against undesirable dangers Ibrahimova, (A.N., 2020). On the other hand network security refers to a collection of rules, procedures, and practices that are implemented to secure computer networks and resources that are accessible over a network from unauthorized access, abuse, modification, or denial of service attacks discussed by (Wikipedia Contributors 2019).

The policies and processes that IT and business organizations implemented to safeguard their information assets from vulnerabilities and threats are what are referred to as information security management, which is a phrase for such policies and practices (Zhang, Nakamura, and Sakurai, 2019). Information security may be broken down into four primary tenets: confidentiality, authentication, integrity, and availability (Alkhudhayr et al., 2019).

A vulnerability is a known weakness in the context of cybersecurity that has the potential to be exploited in order to cause damage or jeopardize sensitive data. The word "vulnerability" is occasionally used to refer to a flaw in software that may be exploited to run operations for which they were not planned. Vulnerabilities may be exploited to perform functions for which they were not intended. An adversary, for

instance, may take advantage of a vulnerability in order to install malware on the computer systems used by the company. An undesirable action or occurrence that may have been caused by exposure to or penetration of a computer system or application may have the potential to damage the system or application in an unintended manner. A vulnerability is a weak point in your system, whether it be in terms of its hardware, software, or operations which is discussed by (Bilgin et al., 2020). Glisson, W.B, (2015) et. al. focuses on the network communication that takes place between the medical mannequin and the computer that is directing it.

Some of the key duties that come under the umbrella of information security include application security, loss prevention, forensics, incident response, network security, security architecture, threat intelligence, vulnerability management, and so on. Another one of your tasks is to keep an eye out for and address weaknesses.

References:

Ibrahimova, A.N., 2020. The defintions of information and security; history of information security development. Vilnius University Open Series, pp.48-57.
Wikipedia Contributors (2019). *Network security*. [online] Wikipedia. Available at:. https://en.wikipedia.org/wiki/Network_security [Accessed 8 May 2022].

Alkhudhayr, F., Alfarraj, S., Aljameeli, B. and Elkhdiri, S. (2019). Information Security:A Review of Information Security Issues and Techniques. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. doi:10.1109/cais.2019.8769504.

Bilgin, Z., Ersoy, M.A., Soykan, E.U., Tomur, E., Comak, P. and Karacay, L. (2020). Vulnerability Prediction from Source Code Using Machine Learning. *IEEE Access*, 8, pp.150672–150684. doi:10.1109/access.2020.3016774.

Glisson, W.B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. and Mary, J. (2015). Compromising a Medical Mannequin. *arXiv:1509.00065 [cs]*. [online] Available at: https://arxiv.org/abs/1509.00065. [Accessed 8 May 2022].

Zhang, H., Nakamura, T. and Sakurai, K. (2019). *Security and Trust Issues on Digital Supply Chain*. [online] IEEE Xplore. doi:10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00069.