Unit 1 Reflection

Learning

This unit introduced students to information security management (ISM) which encompasses people, processes, information, and information technology. I consider these four parts a single whole since no information system exists in isolation but consists of actors that act upon it and upon which it acts. I learned that the triad of information security management namely, Confidentiality, Integrity and Availability (CIA) serves as the foundation of ISM. Confidentiality deals with unauthorized persons' ability to read and take advantage of information stored in the computer; Integrity deals with unauthorized persons' ability to make changes to stored information; Availability deals with preventing authorized users from referring to or modifying information. Considering Non-Repudiation in addition to the triad was interesting because it deals with a system's ability to prove who/what performed actions within the system—frequently monitoring application log files helps here.

Information security considers two important concepts, namely a threat which is an unexpected security breach and a vulnerability which is an attack against an asset that is not secured correctly. Vulnerabilities are classified in public databases such as the National Vulnerability Databases (https://nvd.nist.gov/), Vulnerability Databases (https://vuldb.com/?), Common Vulnerability and Exploits (https://cve.mitre.org/cve/).

To categories and assess threats, I looked at Microsoft's STRIDE[1] threat classification and DREAD[2] risk rating models. Hussain et al. (2014) consider STRIDE as the most widely used threat model, which applies DREAD ratings to each security risk. They also list other models such as STRIDE Average Model, Attack Trees, Fuzzy Logic, SDL Threat Modelling, T-MAP (used for Commercial Off The Shelf software) and CORAS (a UML graphical threat modelling tool). I found these models very enlightening, as they each provide a foundation to assess information system threats. Further, I investigated the Skills Framework for the Information Age (SFIA, https://sfia-online.org/en) to consider skills related to information security and identified several roles applicable to ISM, such as Information Security Technician, Infrastructure Specialist or Operations Support analyst.

Collaborative Discussion

[1] Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege.
[2] Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability.

The collaborative discussion, initiated in this unit, helped me consider threat prevention that takes multiple forms and must involve infrastructure managed by organisations or cloud providers. For example, firewalls, two-factor authentication, intrusion detection systems, password policies, and data encryption. To me, assigning the least privilege to user accounts is the quickest and simplest means to reducing potential threats. Important too is *enabling* customers to easily report new threats and to consider not just software aspects of information systems, but also mundane items such as the buildings, a business's processes and the people that interact.

Team Allocation

This week I was assigned to Group 3 and I was tremendously thrilled to be working with fellow students I worked with previously. This is because I value very much the fellow students who are engaged with the content and with whom study conversations are enlightening and valuable. Team allocation was a little slow in the first week due to circumstances; however, the support team were tremendously helpful to aid the signup process in this module.

References

Hussain, S., Kamal, A., Ahmad, S., Rasool, G. & Iqbal, S. (2014). Threat modelling methodologies: a survey. *Science International,* 26(4):1607-1609.