Launching into Cybersecurity – Units 1 - 3

This 12-week module introduces the various core elements of the MSc. Cybersecurity programme at the University of Essex Online. It intends to ensure a basic understanding of the primary skills covered in complete detail during all relevant modules. It also provides insight and understanding of how the different practices and occupational roles combine to offer a robust body of knowledge and skillset required to succeed in the field. Furthermore, it is beneficial to all who would master this critical field to gain a fuller understanding of the contribution and importance of all elements. As the units tend to build one upon another and contain summary review and reflection every few units, these note entries will follow a similar track and cover three units in each.

This unit summary covers units between 1 - 3, and the stated unit outcomes are:

- Understand the fundamental concepts of Confidentiality, Integrity and Availability (CIA) in Cybersecurity.
- Develop an awareness of the implications of security breaches.
- Critically evaluate the implications of vulnerabilities and threats in software and networks.
- Appreciate the competencies required to be able to address Cyber Security issues.
- Evaluate available techniques and technologies at database and metadata levels dealing with privacy and data disclosure.
- Develop knowledge about approaches to identify vulnerabilities and threats.
- Gain awareness of the ethical and governance frameworks around information systems security and data protection acts.
- Apply knowledge to mitigate the identified issues.
- Develop an awareness of emerging trends in Cyber Security.

Progressive Learning Experience

As predicted, the module study is well-known to me. I can describe and explain definitions of different terms such as Confidentiality, Integrity and Availability easily. Also, I possess solid experience in conducting risk assessments, vulnerability scans and selecting appropriate controls based on risk tolerance and client priorities. However, the diversity of viewpoints and experiences of other students provides the opportunity for growth. Much of the focus in these first three units is around collaborative learning discussions. Unlike traditional undergraduate courses, which rely on exams, this type of learning requires more critical thinking and a willingness to take risks in arguing a position or thesis. These interactions of collaborative learning discussions are an exciting exchange and provide invaluable insight and expanded methods of critical examination. This experience extends well beyond the 3 or 4 required peer interactions.

Personal Take-Away for Units 1 - 3

Based on the collaborative learning discussions and the taken lecture casts during these units, I developed the following outcome: Geographic origin, the home system of Government and cultural differences affect the value and expectation of personal privacy rights. And the level of privacy willing to be exchanged for a feeling of security does not always match the baseline privacy expectation. Thus, for example, while the

implementation of GDPR implies a substantial value on privacy for Europe, it also causes the most severe surveillance-related concerns. For one who plans to operate in companies with an international presence, this is important and should be noted for further study.

Essential Readings

During these units, following reading assignments are completed

- *Department of Computer Science (2019) Cybersecurity Roles and Job Titles. School of Engineering & Applied Sciences, The George Washington University.*
- *Iintersoft consulting (2019) General Data Protection Regulations.*
- *Troncoso, C. (2019) Privacy & Online Rights Knowledge Area Issue 1. The Cyber Security Body of Knowledge.*
- *VanSyckel, L (2018) Introducing Cybersecurity. Sealevel Systems, Inc.*
- *Department for Digital, Culture, Media and Sport (2019) Cyber Security Breachers Survey.*
- *Brookshear, J. G (2020) Computer Science: an overview. 13th ed. Addison Wesley Longman Inc.*
    - *Chapter 4*
    - *Chapter 9*
- *Anderson, R. (2008) Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd ed. Wiley Publishing Inc.*
    - *Chapter 2*
    - *Chapter 4*
    - *Chapter 15*
    - *Chapter 21*
- *Howard M. and LeBlanc. D. (2003) Writing Secure Code. 2nd ed. Microsoft Press.*
    - *Chapter 2*
    - *Chapter 4*