Launching into Cybersecurity – Units 1 through 3

This 12-week module comprises an introduction of the various core elements of the 2-year Master of Science in Cybersecurity program at University of Essex, Colchester England. Class of 2023. It intends to ensure a basic understanding of the primary skills that will be covered in greater detail during subsequent modules. It also provides insight and understanding of how the various specialties and occupational roles combine to provide a robust body of knowledge and skillset required to succeed in the field. While the student's final niche of practice may focus on only a few of the areas covered, 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 up on another and contain summary review and reflection every few units, these journal entries will follow a similar track and cover three units in each.

This initial unit summary covers units 1-3 and the stated learning objects are:

- Understand the key concepts of Confidentiality, Integrity and Availability (CIA) in Cyber Security.
- 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.

Initial, Pre-unit Baseline

As I have been working in the cybersecurity space for over 10 years, much of the info in these first 3 units are already known, understood, and used regularly in the normal course of my daily occupation. But as a lifetime learner, I know there will be valuable nuggets within these modules and approach them with that in mind. I look forward to gaining perspective from my cohorts as they represent many nations, cultures, and industry sectors.

Progressive Learning Experience.

As predicted, the curriculum is familiar and remedial to me. I can quote the definitions of Confidentiality, Integrity and Availability in my sleep. And I have vast experience in conducting risk assessments, vulnerability scans and selecting appropriate controls based on risk tolerance and client priorities. However as expected, the diversity of viewpoints and experiences of my cohorts provides the opportunity for growth. Much of the focus in these first 3 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 risk in arguing a position or thesis.

These interactions of collaborative learning discussions are an exciting exchange and I gain insight and expanded methods of critical examination. This experience extends well beyond the 3 or 4 required peer

interactions in that I am engaged equally in the reading of the other peer interaction as the ones in which I participate. From what was to be a remedial review, I have gained much to prepare for my return to school at a late age and subsequent quest for excellence in my field.

Personal Take-Away for Units 1-3

Of value in the collaborative learning discussion and the lecture-cast is the various viewpoints on privacy across the diverse body of cohorts. Geographic origin, 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. While the implementation of GDPR implies a strong value on privacy for Europe, it leads the globe with highest coverage of surveillance cameras. Meanwhile, the United States has a much simpler set of rules for protecting individual privacy, the American public is constantly on the alert for abuses and stands up watch-dog groups for oversight and reporting outside of regulatory systems. For one who plans to operate in companies with international presence, this is an important awareness and should be noted for further study.

Core Reading

During these units reading assignments were completed from the following

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