Network and Information Security Management – Units 7 - 9

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 7 - 9, including the following outcomes:

- Describe the purpose of risk assessment.
- Explain how to mitigate risks.
- Describe the difference between business continuity and disaster recovery.
- List common security standards and select the appropriate one(s) for a given situation.
- Explain which GDPR regulations are applicable to the project assignment.
- Describe which other standards the project assignment needs to meet.
- Advise on mitigations to help a website meet any of the standards applicable to its specific industry, such as data and privacy (GDPR) or financial (PCI-DSS).
- Explain how and why logging is used in security systems.
- Describe which tools to use for logging and analysis.
- Explain how logging is used in incident investigations.
- Describe the best forensic techniques to use.

Progressive Learning Experience

Risks and Standards were particular focus areas of these units. Advancing further in assigned tasks and performing scanning exercises provided an opportunity to gain hands-on experience with various active and passive information-gathering tools. Furthermore, identifying applicable GDPR requirements based on the scanning output and discussing potential mitigations further expanded understanding of how grifted relation exists between data security and privacy, particularly in the legislative area. In addition to that, the diversity of viewpoints and experiences of other students provided the opportunity for growth.

Personal Take-Away for Units 7 - 9

Security Incident investigation techniques such as logging and forensics of Unit nine has been entirely new to me, especially forensics. Digital forensics is a must to develop new capabilities, especially to counter adversaries and avoid potential data breaches. Thus, the forensic techniques studied in Unit nine provided solid background and helped in gaining practical experiences.

Required Reading

The following reading assignments were available during these units:

- Campbell, T. (2016) *Practical Information Security Management.* 1st ed. APRESS.
    - Chapters 5 and 6.
- Bhatt, D. (2018) Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper. *International Journal of Scientific & Technology Research* 7(4): 233-237.
- Bhingardeve, N. & Franklin, S. (2018) A Comparison Study of Open Source Penetration Testing Tools. *International Journal of Trend in Scientific Research and Development* 2(4): 2595-2597.
- ICO (2020) Guide To The General Data Protection Regulation (GDPR)
- PCI Security Standards.org (2020) Official PCI Security Standards Council Site - PCI Security Standards Overview.
- HIPAA (2020) HIPAA For Dummies - HIPAA Guide.
- Data Protection Commission (2020) CaseStudies|DataProtection Commission.
- HIPAA (2020) HIPAA For Dummies – HIPAA Guide.
- PCI Security Standards.org (2020) Official PCI Security Standards Council Site - PCI Security Standards Overview.
- ICO (2020) Guide to the General Data Protection Regulation (GDPR).
- Campbell, T. (2016) Practical Information Security Management. 1st ed. APRESS.
    - Chapters 10 and 11.
- Swift, D. (2010) Successful SIEM and Log Management Strategies for Audit and Compliance. SANS Information Security Reading Room.

Additional Reading

The following reading assignments were available during these units:

- Leroux, S. (2020) The Kali Linux Review You Must Read Before You Start Using It. It's FOSS
- Alhazmi, O. & Malaiya, Y. (2013) Evaluating Disaster Recovery Plans using the Cloud. 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS) 1(1): 1-6.
- Fraser, J. & Simkins, B. (2016) The Challenges of and Solutions for Implementing Enterprise Risk Management. *Business Horizons* 59(6): 689-698.
- Ross, R., McEvilley, M. & Oren, J. (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in The Engineering of Trustworthy Secure Systems, Volume 1
- Hertzog, R., O'Gorman, J. and Aharoni, M. (2017) *Kali Linux Revealed.* 1st ed. Cornelius: Offset Press.
    - Comprehensive guide to using Kali Linux for pen testing and vulnerability assessments.
- Vielberth, M. & Pernul, G. (2018) 'A Security Information and Event Management Pattern' 12th Latin American Conference on Pattern Languages of Programs (SLPLoP). Valparaiso, Chile. 20-23 November. 1 - 12.
- SolarWinds.com (2020) Windows Logging Basics - The Ultimate Guide To Logging.

- Eaton, I. (2003) The Ins and Outs of System Logging Using Syslog.