Network and Information Security Management – Units 10 - 12

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 10 - 12, including the following outcomes:

- Utilise the breach checklist to analyse a breach.
- Recommend a number of actions and tools based on the analysis.
- Critically assess published responses.
- Describe emerging trends and technologies.
- Explain the impact of emerging changes.
- Describe some challenges encountered with both current and new solutions.
- Describe several potential future Internet architectures.
- Argue for and against several architectures.
- Reflect on the role of Information Security Management in modern computing solutions.
- Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them.
- Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues.
- Gather and synthesise information from multiple sources (including Internet security alerts and warning sites) to aid in the systematic analysis of security breaches and issues.
- Articulate the legal, social, ethical and professional issues faced by information security professionals.

Progressive Learning Experience

Producing an executive summary report was a particular focus area of these units. The executive summary report was the final part of the project assignment. Our team focused on the imaginative e-health themed website of pink e-health services organisation' target assets, assessment approach, methodologies, tools, standards, and threat risk analysis methodologies to produce the final report. Employing various active and passive information gathering techniques, debating the rationale of identified vulnerabilities, incorporating a STRIDE-based threat classification scheme, and performing DREAD-based risk assessment/scoring provided invaluable hands-on experience. Moreover, performing several scans and utilising different scanning tools supported a distilled view on vulnerabilities, including the elimination of false positives.

Personal Take-Away for Units 10 - 12

Personally involved in creation of risk rating matrix, incorporation of DREAD-based risk assessment/scoring method and documentation of limitations around various approaches. These were noticeable contributions in producing an executive summary and well received within the team. Working in a team promoted creativity. Additionally, it has maximised the shared knowledge within the team. There could have stale viewpoints if we were working as individuals; thus, the teamwork helped us avoid that potential concern.

Required Reading

The following reading assignments were available during these units:

- Swinhoe, D. (2020) The 15 Biggest Data Breaches Of The 21St Century. CSO Online.
- Rawat, D. & Reddy, S. (2017) Software Defined Networking Architecture, Security and Energy Efficiency: A Survey. *IEEE Communications Surveys & Tutorials* 19(1): 325-346.
- Ding, W., Yan, Z. & Deng, R. (2016) A Survey on Future Internet Security Architectures. *IEEE Access.*
- Clarke, I., Miller, S., Hong, T., Sandberg, O. & Wiley, B. (2002) Protecting free expression online with Freenet. *IEEE Internet Computing* 6(1): 40-49.
- Soomro, Z., Shah, M. & Ahmed, J. (2016) Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36(2): 215-225.

Additional Reading

The following reading assignments were available during these units:

- Hou, Y., Gao, P. & Nicholson, B. (2018) Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital. *Technological Forecasting and Social Change* 1(126): 64-75.
- Choucri, N., Madnick, S. & Ferwerda, J., 2013. Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development 20(2): 96-121.
- Grispos, G., Glisson, W.B., Bourrie, D., Storer, T., & Miller, S. (2017). Security Incident Recognition and Reporting (SIRR): An Industrial Perspective. Americas Conference on Information Systems (AMCIS 2017)
- Chiosi, M., Clarke, D. & Willis, P. (2012) Network Functions Virtualisation - Introductory White Paper.
- Shaotong Z. (2016) A Clean-Slate ID/Locator Split Architecture for Future Network. *Journal of Network Computing and Applications* 1(1):1-6.
- Huang, Y. (2019) Decentralized Public Key Infrastructure (DPKI): What Is It And Why Does It Matter?
- Horne, C., Maynard, S. & Ahmad, A. (2017) Organisational Information Security Strategy: Review, Discussion and Future Research. Australasian *Journal of Information Systems* 21(1): 1-17.
- Azmi, R., Tibben, W. & Win, K. (2016) 'Motives Behind Cyber Security Strategy Development: A Literature Review Of National Cyber Security

Strategy' Australasian Conference on Information Systems. Wollongong. 1-12

- Urdaneta, G., Pierre, G. & Steen, M. (2011) A Survey of DHT Security Techniques. *ACM Computing Surveys* 43(2): 1-49.
- Shafqat, N. & Masood, A. (2016) Comparative Analysis of Various National Cyber Security Strategies. *IJCSIS* 14(1): 129 - 136.