Unit 10 Reflection

In this unit, I considered the reading material to be quite laborious to wade through because the topics, namely Computer Emergency Response Teams (CERT) and regulation-based pressures on Information Security Management, I found difficult to associate with. Despite that, it was interesting to read that several organisations are trying to tackle cyber security, and despite the mish-mash amalgamation of ideas and policies, there is still much room for consolidated international norms to guide states in their public-private collaboration to establish defence networks to counter emerging cyber threats. Choucri et al. (2014) identified several institutional domains in the cyber security ecosystem, and they note that the organisations "often have unclear mandates". I considered the organisations listed, such as Council of Europe, North Atlantic Treaty Organisation (NATO), OECD, National Security Agency (NSA), Central Intelligence Agency (CIA), Federal Bureau of Investigations (FBI), Government Communications Headquarters (GCHQ) and MacAfee. My initial thoughts are that it is obvious for each organisation to seemingly overlap or have unclear cyber security mandates because each entity focuses on a unique set of local and international challenges, and not solely on cyber threats. For instance, NATO focuses on military attacks while GCHQ focuses on information assurance and cryptography.

I picked up a GDPR data breach case study that dealt with the leakage of over one terabyte of data related to American voters by Deep Root Analytics. This case study was very interesting because, for me, it raised a few questions, namely, why a security data analyst was able to download the vast amount of data over two days, and secondly, who gives moral right to the Republican National Committee to model *intended racial and religious* preferences of roughly 180 million American voters? The last question I find particularly heinous because it makes mockery of a person's sovereign right to declare their religious affiliation; instead, some AI-based models were used to make a computer-based decision on what each individual *likely* would choose. The fact that a data analyst downloaded the data, caused me to stop and ponder why they were permitted to do so—yes, they did alert the authorities—yet, if actors from outside America had downloaded the data, they likely would be tried in a court of law. Therefore, both questions highlight that knowledge is power, and the power of our information is given out onto public spaces and websites, the worse off society will become because they willingly give up information that will be used for manipulation, control, and assertion.

I responded to four students' discussion posts and tried to home in on the aspect of consent as it relates to GDPR. This is because a post by a fellow student, Shan (2021) raised the use of signage to enforce GDPR compliance. This is interesting because, if erecting signs to alert

customers and staff that their actions are recorded, and people then enter a building to conduct their business, it implies automatic consent. And the issue with automatic consent because a sign happens to say this or that, is that the wording may be obscure, illegible, unreasonable, or designed to protect the owners of the building or workspace. Therefore, it seems that GDPR policies are not fool proof and do still exhibit a grey area for abuse.

I continued to work with the team to contribute and prepare our final executive summary document. In this activity we trimmed down content that was irrelevant and ensured we used alternate words or phrases useful in trimming down long sentences.

References

Choucri, N., Madnick, S. & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. Information Technology for Development, 20(2):96-121.

Swanlow, S. (2021). Collaborative Learning Discussion 3: Initial Post. Available from https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=292900 [Accessed 15 Feb. 2021]