Unit 8 Reflection

This week, focus was around data standards including Health Insurance Portability Accountability Act (HIPAA), General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS). I considered these standards in the context of the website assigned for scanning activity and found that GDPR and PCI DSS (to a lesser degree) are applicable to Human Resource Management systems. GDPR is a completely relevant given that any personal data must be governed for privacy and security concerns. In this respect, I engaged in a GDPR study case relating to photographs published onto a social media website—refer to the separate document showing the discussion post. I was thoroughly surprised to learn that Google Cloud Platform supports HIPAA, PCI DSS, ISO 27000, ISO 27001, ISO 27017 and ISO 27018 and they also present several best practices

Paying consideration to above data standards, I researched that ISO 27000 has several supporting standards which I believe are relevant today. For example, ISO 27017 that deals with guidance and recommendations for implementing security controls in cloud environments and ISO 27701 that extends ISO 27001 to include privacy topics and defines basic requirements for Privacy Information Management Systems (PIMS). Overall, the ISO 27000 set of standards provide clear guidance for guidance to customers' and requirements for information and data protection. I believe that GDPR and ISO 27001 both attempts to achieve similar outcomes, however they have different focuses. In a blog post by Data Privacy Manager (2021), they state ISO 27000 is an *international framework* and cover 75-80% of GDPR compliance, GDPR is a European Union *regulation* but has wider impact since it encompasses data privacy and security and prescribes how such data is to be protected and dealt with (Office for Civil Rights, 2020).

I continued to work with the Nmap scanning tool to uncover vulnerabilities. To continue scanning for vulnerabilities, I had to sign up for a Virtual Private Network (VPN) subscription because the firewall protecting the website is working correctly; however, Nmap sends many port scans that my home ISP address is often blocked. I find the penetration testing to be unengaging because there is no indication that what I am doing is correct when using Nmap to perform some scans.

Though, I found interesting an article by Paganini (2021) that noted that Nmap scripts are used—to be released on GitHub—by the UK's National Cyber Security Centre (NCSC). The NCSC will approve scripts submitted by ensuring they meet mandatory requirements. Though my initial thoughts considering this is that governments do not ever seem to act in the interest of the wider society, but rather to establish dominion over citizens and their data. In my view, I would have preferred release of such security-related scripts to be undertaken by other well-known security organisations who have no connection to an government institution.

References

Data Privacy Manager (2021). What is the Difference Between GDPR and ISO 27001. Available from https://dataprivacymanager.net/what-is-the-difference-between-gdpr-and-iso-27001/ [Accessed 29 Jan. 2021]

Office for Civil Rights (2020). https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

Paganini, P. (2021). UK NCSC is going to release Nmap scripts to find unpatched vulnerabilities. Available from https://malwaredefinition.com/index.php/2022/01/25/uk-ncsc-is-going-to-release-nmap-scripts-to-find-unpatched-vulnerabilities/news/admin/ [Accessed on 29 Jan. 2021]

HIPAA (2018). Health Insurance Portability Accountability Act of 1996 (HIPAA). Available from https://www.cdc.gov/phlp/publications/topic/hipaa.html [Accessed 29 Jan. 2021]

Lopes, I.M., Guarda, T. & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. Journal of Information Systems Engineering & Management, 4(2):1-8.