Unit 2

UML Modelling to Support Secure System Planning

Seminar 1 – Scrum Security Review

Blog Post – People and Cyber Security

Managing cybersecurity in today's organisations is vital to an organisation's systems and information. Using security technologies prevents cyber attacks if employees fail to adhere to cybersecurity policies. (Anwar et al., 2017). For this reason, organisations must realise the importance of human behaviour when considering cybersecurity policies.

The need to monitor device usage is essential when users can plug in their own portable USB devices. Often, these devices are laden with malicious software allowing a social engineer remote access to a system after plugging in a device into a computer connected to the Internet. This process is often a prime means of infiltration used by social engineers who often leave such devices in available places to gain entry to highly protected systems (Tischer et al., 2016). The use of security monitoring tools also extends to an organisation's network infrastructure to identify possible security events before they occur.

Unsurprisingly, organisations must establish a cyber-security incidence prevention objective by improving security awareness among their software engineers (Pfleeger & Caputo, 2012). Greater understanding is required because software engineers are often trusted to select the correct security mechanism to balance security with performance and usability requirements. A sound information security policy ensures information protection, confidentiality, and integrity and goes hand-in-hand with monitoring tools. Though, human attitudes toward cybersecurity in a business environment can negatively affect the integrity and privacy of such information. Security is (often) considered subservient to a user's primary requirement, for example, locating information, processing transactions or making decisions (Hadlington, 2017). Therefore, such restrictions could interfere with their primary goal and cause users to bypass information security policy manually.

In today's world of information systems, the presence of risk or vulnerabilities in an information asset can cause harm to an organisation. For this reason, cybersecurity is concerned about the protection of information assets from threats posed by inherent vulnerabilities. Incorporated into information security governance, the establishment, selection and implementation of security controls, organisations can significantly reduce and manage risks posed by these vulnerabilities (Disterer, 2013).

References

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L. (2017) Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior 69*:437-443.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

Hadlington, L. (2017) Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), p.e00346. DOI: https://doi.org/10.1016/j.heliyon.2017.e00346

Pfleeger, S.L. & Caputo, D.D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. Computers & Security 31(4):597-611.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. & Bailey, M. (2016). Users really do plug in USB drives they find. *IEEE Symposium on Security and Privacy (SP)*: 306-319.

Bibliography

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review* 4(10).