e-portfolio: https://sam-tselapedi.github.io/CyberSecurity/irm.html

Information Risk Management: Reflective Essay

From the perspective of a system and security engineer, my focus on risk management has been intensely on mitigation through the understanding and knowledge I possess without a formal process of identifying and assessing risk. I have always focused on high availability, site resiliency, recoverability, and security systems protection information technology controls. Systems' functionality has been the motivating factor instead of focusing on the actual business impact.

After reading through (Barki, 2010) research paper (User Participation in Information Systems Security Risk Management), I realised that my organisation's lack of holistic risk management, including information technology and other business stakeholders, might have led to a poor recovery strategy. Without identifying and prioritising data based on its criticality to business, information technology may continue to have successful backups of little value to business continuity. Business stakeholders' input is essential in identifying and prioritising critical data for business continuity.

Developing a security program may be complicated and challenging without holistic and comprehensive information risk management. Identifying and valuing assets' relative criticality to the business provides a piece of knowledge to determine the cost and the extent required to protect the concerned assets. Understanding critical assets and their vulnerabilities are essential to measuring business impact when threats exploit such assets' vulnerabilities. Security controls and an adequate security program depends on comprehensive risk identification, assessment and review.

The integration of risk management within the system development life cycle(SDLC) is essential to establish effective risk management that will enable organisations to minimise risks. Incorporating risk management throughout SDLC nurtures and increases efficiency and transparency while empowering stakeholders at every level to identify and consider potential risks. Through the SDLCstages, organisations can evaluate and ensure that no new vulnerabilities are unintentionally introduced as the organisation's technology portfolio broadens and other processes are introduced.

After reading through all the information about mapping risk management strategies and frameworks to the systems/software development cycle, I was interested in understanding the software development team's formal or informal risk management structure during the developments projects. I learned that essential processes such a reviewing one developer's code by a senior developer to ensure the secure development frameworks have been followed were not present. After learning about the lack of risk management framework in our organisation, I realised that we might be so vulnerable that, as an authoritative organisation for all communicable diseases within our country, the quality of the data we produce may be questionable. I have since asked my line manager to propose and discuss risk management within the management committee. Having completed the IRM module does not make me an

expert in risk management; however, it has changed how I view risk management, and it made me realise its significance in the organisation.

In conclusion, the pervasiveness of information technology systems in organisations and considering the potential and actual existing threats and vulnerabilities in these systems, a management plan and program to mitigate these risks are essential. As a success factor, establishing a risk management program and identifying key stakeholders to ensure its success can enable organisations to reach their missions securely. It is something fundamental. To achieve this goal also depends on broad support and participation of managers, members and officials of the organisation.

My contribution to group work can be found on my e-portfolio.

References :

Barki, H. (2010) ‘Qa ’ rteny’, 34(3), pp. 503–522.

Dey, P. K., Clegg, B. and Cheffi, W. (2013) ‘Risk management in enterprise resource planning implementation: A new risk assessment framework’, *Production Planning and Control*, 24(1), pp. 1–14. doi: 10.1080/09537287.2011.597038.

Ramona, S. E. (2011) ‘Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches’, *Chinese Business Review*, 10(12), pp. 1106–1110. doi: 10.17265/1537-1506/2011.12.002.

Zio, E. (2018) ‘The future of risk assessment’, *Reliability Engineering and System Safety*, 177, pp. 176–190. doi: 10.1016/j.ress.2018.04.020.