Introduction

Li and Liu (2021) claim that people can unintentionally harm systems, making them unpredictable when managing cyber security. Liu et al. (2022) cite many arguments supporting this statement, as seen in Figure 1:

Reasons why people are the biggest risk of cybersecurity as cited in Liu et al. (2022)
In both the US and UK, their contribution to risking cyber systems is deemed notable (Dysktra, 2017).
Compared to computers, there is a bigger possibility of individual blunders (Metalidou et al., 2014).
People cause 80% of breaches in cyber defence (Saeed et al., 2013).
Agencies find it difficult to defend against security risks during computer-human interaction (Nobles, 2015).
Stakeholders are considered to be vulnerable points in security management as more companies embrace technology in order to advance their performance (Alavi et al., 2016).
There is a need to choose which up-to-date security systems to utilise in order to fight cyber threats that are growing daily (Neely, 2017).
Stakeholders should be given appropriate training on the information systems of firms alongside the adaptation of recent cyber security technologies. (Metalidou et al., 2014)
Companies allot insufficient budget in employing cyber security experts (Alavi et al., 2016)

Figure 1: Liu et al. (2022) provide us sources that support the statement that people are the biggest cybersecurity risks.

In addition, Cains et al. (2022) posit that we, as “users, defenders, and attackers” are ineludible cyber security threats. Therefore, there is a need to deal with internal cyber security attacks through people management.

ISO/IEC Standard 27000:2018 Section 3 Terms and Definitions

It is important to equip the workforce of a company with the necessary knowledge and skills to master the precautions and steps placed when faced with cyber security threats, through online and face-to-face training. (Dash & Ansari, 2022). Five terms from ISO/IEC Standard 27000:2018 Section 3 are highlighted to help manage individuals in cyber security. These are: **‘Top Management (3.50)’, ‘Management System (3.41)’, ‘Governance of Information Security (3.23)’, ‘Risk Criteria (3.66)’,** and **‘Documented Information (3.19)’** (ISO, N.D.). Figure 2 presents why these terms were selected. It also shows that the OWASP Top 10 Proactive

Protocols 2018 **‘C1: Define Security Requirements’, ‘C8: Protect Data Everywhere’,** and **‘C9: Implement Logging and Monitoring**’ (OWASP, N.D.) were considered in the selection of the aforementioned standards to strengthen people management in cyber security within organisations.

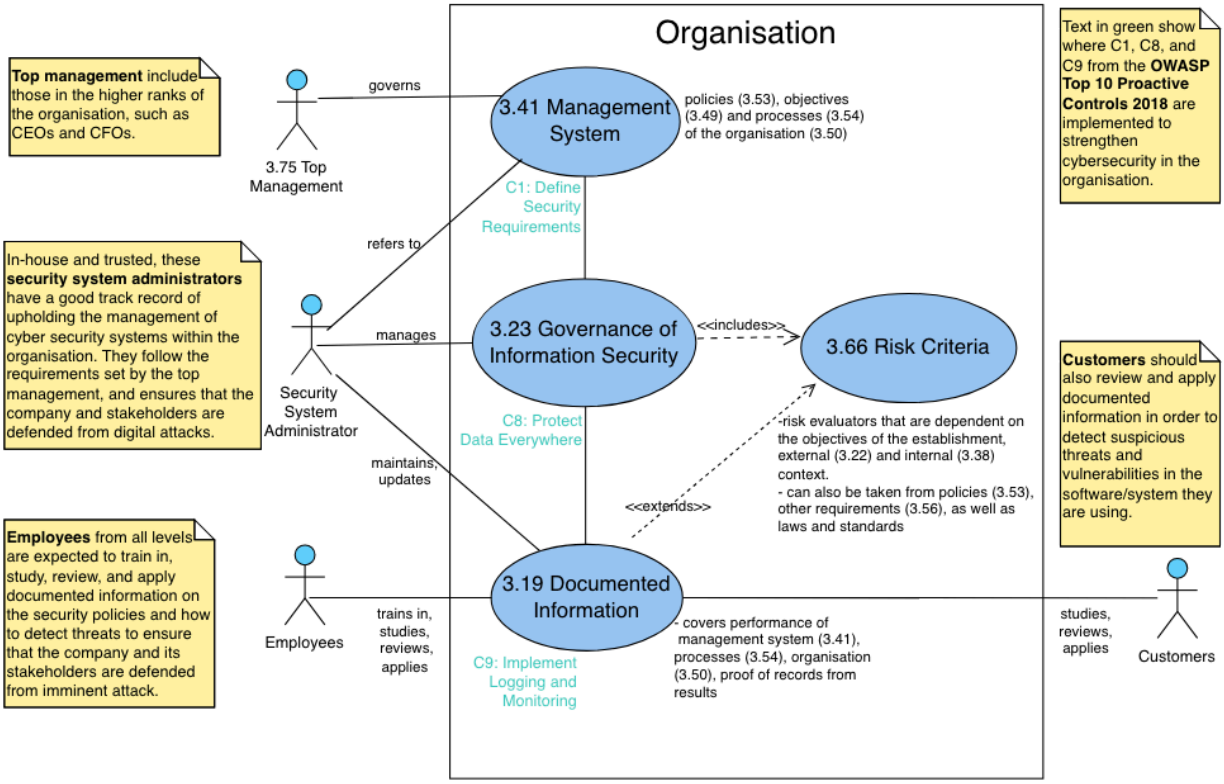

Figure 2: UML use case diagram explaining how an organisation has to set clear guidelines and criteria in assessing cyber security risks.

Conclusion

Cyber security training develops awareness on detecting weaknesses, as well as skills in preventing attacks and implementing defensive protocols inside companies. However, Chowdhury and Gkioulos (2021) argue that there is still insufficient research regarding critical infrastructure cyber security, and that a consensus has not been reached as to what the most ideal practices are in gaining expertise in the field. Therefore, it is crucial for software engineers to be knowledgeable in international standards, such as those from the **ISO** and **OWASP**. They can then ascertain that the cyber security policies and requirements they are upholding and implementing within their organisations correlate with these internationally accepted standards.

References:

Cains, M.G., Flora, L., Taber, D., King, Z. & Henshel, D.S. (2022) Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis* 42(8): 1643-1669. DOI: https://doi.org/10.1111/risa.13687.

Chowdhury, N. & Gkioulos, V. (2021) Cyber security training for critical infrastrucutre protection: A literature review. *Computer Science Review* 40(100361): 1-20. DOI: https://doi.org/10.1016/j.cosrev.2021.100361.

Dash, B. & Ansari, M.F. (2022) An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology* 9(4): 1-6. Available from: https://www.researchgate.net/publication/359772764_An_Effective_Cybersecurity_Awareness_Training_Model_First_Defense_of_an_Organizational_Security_Strategy [Accessed 20 March 2024].

ISO (N.D.) ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.56 [Accessed 20 March 2024].

Li, Y. & Liu, Q. (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports* 7: 8176-8186. DOI: https://doi.org/10.1016/j.egyr.2021.08.126.

Liu, X., Ahmad, S.F., Anser M.K., Ke, J., Irshad, M., Ul-Haq, J. & Abbas, S. (2022) Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology.* 13(927398): 1-15. DOI: https://doi.org/10.3389/fpsyg.2022.927398.

OWASP (N.D) OWASP Top Ten Proactive Controls 2018 | Introduction. Available from: https://owasp.org/www-project-proactive-controls/v3/en/0x04-introduction [Accessed 15 March 2024].