Review 1 - 1866549312

The response provides a holistic view of human factors when implementing an ASMIS. Three apparent human factors are identified with good examples of how they pose a risk to the system. Each factor is clearly defined and linked to socio-technical risks. Furthermore, in some places, there are helpful contemporary case studies to support the referenced findings.

The piece suggests that inside actors pose the greatest threat, and this is supported as they usually base risks due to opportunities rather than capabilities (Gheyas and Abdallah, 2016). Situational awareness is highlighted as a crucial factor which supports the view that education and training are vital for users to gain a deeper understanding of the risks presented (McIlwraith, 2021).

In each human factor, there are mitigations to support the ASMIS; however, perhaps considering limited privileged access and a security policy by default in the ASMIS software development process. (Gorski et al., 2018).

The scope of actors was limited to patients and administrators, which could have been expanded. Some sources are deemed sightly older and could have been more recent publications to give a contemporary outlook. Social engineering was discussed as a severe risk where humans are susceptible to health impairments or cognitive loads; considering Hartson & Pyla (2019), greater emphasis should be placed on usability and user experience in the ASMIS development stages.

Gheyas, I. A. & Abdallah, A. E. 2016. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics,* 1**,** 6.

Gorski, P. L., Iacono, L. L., Wiefling, S. & Möller, S. Warn if Secure or How to Deal with Security by Default in Software Development? HAISA, 2018. 170-190.

Hartson, R. & Pyla, P. 2019. Chapter 15 - Mental Models and Conceptual Design. *In:* HARTSON, R. & PYLA, P. (eds.) *The UX Book (Second Edition).* Boston: Morgan Kaufmann.

McIlwraith, A. 2021. *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*, Routledge.

Review 2 – 1866678234

The response provides sound analysis, which is well referenced. A good view of human factors' importance in ASMIS implementation is identified implicitly, and precise details on socio-technical risks. Furthermore, there is a good use of source material used to support and extends the analysis by offering more contemporary references to support some older source material.

A beneficial discussion on the design for user experience was well received and led the pathway to elaborate on the management's role in business strategy. The discussion surrounding a human-centred approach is supported by the view that adapting security to humans is challenging due to limited capabilities (Sasse and Rashid, 2019), and the critical focus should be on the usability of the user experience (Hartson and Pyla, 2019).

To consider further, perhaps identifying the human factors more explicitly and considering a broader scope of actors involved as the management would be concerned for all users, not just the patients.

Also, the view that management should have a top-down approach could cause conflict. Other perspectives suggest a bottom-up solution is helpful so that a security-aware culture environment is developed and the responsibility is for all (Pollini et al., 2022), not just a CISO or high-level manager. Therefore, a more inclusive, educated and multidisciplinary approach is needed for a knowledgeable, human-focused workplace (McIlwraith, 2021).

Hartson, R. & Pyla, P. 2019. Chapter 15 - Mental Models and Conceptual Design. *In:* HARTSON, R. & PYLA, P. (eds.) *The UX Book (Second Edition).* Boston: Morgan Kaufmann.

McIlwraith, A. 2021. *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*, Routledge.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. & Guerri, D. 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work,* 24**,** 371-390.

Sasse, M. A. & Rashid, A. 2019. *Human Factors Issue. The Cyber Security Body Of Knowledge (1)* [Online]. Available: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf [Accessed 21 June 2022].