Individual Presentation Transcript

This presentation aims to unravel and explain the solutions to the issues identified from my Individual Essay. Before proceeding to the solutions, first we will look at the most significant information to note from my Individual Essay. These include:

1. Benefits of the web-based appointment and scheduling management information system (ASMIS) at the Queens Medical Centre: The Queens Medical Centre is a community clinic that made a decision to adopt a web-based appointment and scheduling management information system (ASMIS). This particular system facilitates the booking of appointments online, by gathering important patient information which is then used to determine the most suitable specialist to attend to their specific case. Therefore, the implementation of ASMIS offers a range of advantages, including timely access to care for residents, the ability to accommodate the increasing population growth of the community, and a secure platform that is protected against cyberattacks.
2. The concerns that the management of Queens Medical Centre have raised despite ASMIS been secure and compliant with government's policy on patient data protection, and also providing the above-mentioned benefits to the clinic. The management specifically raised concerns about the lack of attention to human factors in ensuring optimal security.
3. The Human factors and their effects on cybersecurity. To achieve optimal security, usability and functionality of ASMIS, human factors need to be prioritised because human errors is the leading contributor to data breaches and cyberattacks (Nobles, 2018).

Based on the information noted above (as from the individual essay), this presentation will henceforth concentrate on the strategies that can be employed to mitigate the human factors that have been previously identified.

1. **Mitigating Lack of Cybersecurity Awareness**

   (Nifakos , et al., 2021) highlights that users with inadequate cybersecurity knowledge are more prone to human errors thus becoming victims to cyber-attacks like phishing, data breaches, etc.

   Furthermore, some users are ignorant or lack motivation to learn and follow cybersecurity practices. Ways of mitigating this include:

   a) Patients and staff members should follow a cybersecurity and social engineering training and awareness programs that equips the users with knowledge on how to identify, prevent, mitigate and report any risks, vulnerabilities or malicious activities (Aldawood & Skinner, 2019).

   b) The use of interactive or fun way of learning or training users about cybersecurity. This will motivate users to engage in the program. Such training can be administered using questionnaires, videos, interactive simulations, fun games, seminars, etc.

   c) The clinic to integrate and practice security culture by targeting the users (their attitude, behaviour, competency) and the organisation (its assets, operations, technological infrastructure, policies) (Georgiadou, et al., 2022).

   d) Staff and patients should be encouraged to report any suspicious activities and to be shown who to report it to, for example, to a designated hotline or email, IT technical support, police etc.

e) The clinic should prioritize training budgets and regularly perform assessments and penetration tests to identify areas of weaknesses and vulnerabilities. This will help eliminate the know-doing gap and enable the clinic to assess users' response to potential security threats, thereby allowing them to develop suitable countermeasures that effectively mitigate cybersecurity risks. (Aldawood & Skinner, 2019)

f) The clinic should advocate for institutions to teach on human factors that impact information security (Nobles, 2018).

g) The clinic should establish a cybersecurity incident response plan that outlines how to handle and respond to cybersecurity incidents and the users must be aware of it too.

2. Mitigating Fatigue/Tiredness

Because users are humans, they may experience fatigue from mental and physical work overload, or from being overwhelmed by numerous security features like complex passwords or nested Multi-Factor Authentication. This fatigue can reduce attentiveness and increase the likelihood to human errors (The CERT Insider Threat Team, 2013).

There is a couple of ways this could be mitigated, and these are:

a) Better management practices that promote more selfcare and stress-free work environments.

b) The clinic should consider integrating more shift rotations, work breaks, vacation leaves or employ more employees or automate work etc, so that employees will not be burnt-out from over working (Nobles, 2018).

c) Implement features and automation tools that are clearer, simpler and more user friendly to all users including users with disabilities or short-term memories (The CERT Insider Threat Team, 2013).

d) Implementing automation security techniques such as implicit authentication that identifies authorized users without the need for repetitive password re-entry.

e) Security mechanisms like authentication can be designed to be triggered only when needed, therefore optimizing their use (Sasse & Rashid, 2019).

f) Implement simplified security features to reduce user frustration, such as, longer password reset periods, considerate session time-limits, non-nested MFAs, and streamlined processes.

g) Implementing Captchas that are accessible to all users, including users with disabilities (Sasse & Rashid, 2019).

h) Ensuring ASMIS follows a secure software development process and undergoes regular testing for it to maintain efficiency and prevent system downtime and errors.

i) Adopting to password-less authentication, such as, software authentication tokens, token hardware authentication, One-Time-Pin (OTP) authentication, etc. (Parmar, et al., 2022).

3. Mitigating Stress

Stress been a response, both physical and emotional, to particular situations or circumstances, can result to increase of human errors and decreased performance (Nobles, 2022). Ways to mitigate this and ensure cybersecurity include:

a) Clear, easy and simplified user interface that is adaptable and stress-free to all users including disabled users, etc.

b) Implement user feedback and technical support and all reports and feedbacks should be addressed promptly.

c) Ensure that ASMIS has fewer complex processes, errors and bugs by testing, patching and upgrading it regularly.

d) Encourage users to participate in stress management training, such as mindfulness and yoga, mental health care, etc., - so as to promote a positive and stress-free work environment.

e) Creating a supportive and positive environment that does not induce stress to the end users, for instance encouraging breaks, shifts, vacations, etc.

Social and Ethical considerations

a) Data transparency should be ensured by communicating it to everyone involved with ASMIS i.e., the staff, patients, etc.

b) The best data privacy and protection policies and regulations should be implemented and practiced. For instance: compliance to European Data Protection Regulation (GDPR), among others (Georgiadou, et al., 2022).

c) Technologies such as blockchain, Artificial Intelligence, etc, can be used to combat human factor problems by detecting and flagging human errors, ensuring transaction integrity, analysing human behaviours, and more.
d) To consult human factors specialists and behavioural analysis, and to create an executive-led committee that addresses the impact of human factors on information security (Nobles, 2018).

In conclusion, human factors play a critical role as end-users constitute the weakest link in the security chain due to their vulnerability to attacks and potential for errors that could result in security breaches (Sultan, 2022). To ensure optimal effectiveness, efficiency and safety of ASMIS, the clinic must prioritize and manage the human factors.

References

Aldawood, H. & Skinner, G., 2019. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet,* 11(3), p. 73.

Georgiadou, A., Mouzakitis, S., Bounas, K. & Askounis, D., 2022. A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems,* 62(3), pp. 452-462.

Nifakos , S. et al., 2021. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors,* 21(15), p. 5119.

Nobles, C., 2018. Botching Human Factors in Cybersecurity in Business Organizations. *Holistica Journal of Business and Public Administration,* 9(3), pp. 71-88.

Nobles, C., 2022. Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *Holistica Journal of Business and Public Administration,* 13(1), pp. 49-72.

Parmar, V., Sanghvi, H. A., Patel, R. H. & Pandya, A. S., 2022. *A Comprehensive Study on Passwordless Authentication.* Erode, IEEE.

Sasse, A. & Rashid, A., 2019. *Human Factors Knowledge Area.* [Online]
Available at: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf
[Accessed 04 February 2023].

Sultan, O., 2022. *The human factor in cybersecurity.* [Online]
Available at: https://www.hackread.com/the-human-factor-in-cybersecurity/
[Accessed 28 February 2023].

The CERT Insider Threat Team, 2013. *Unintentional Insider Threats: A Foundational Study.* [Online]
Available at: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf
[Accessed 04 February 2023].