Human factors that need to be addressed for a web-based appointment and scheduling management information system (ASMIS)

GDPR fines and the loss of reputation by loss of trust after a successful attack are strong motivators to strive for sufficient security for any organization, since attacks are likely to happen these days. An ASMIS does contain Personal health information (PHI), which is one of the most valuable assets and therefore often attacked (Yao 2017). To have a secure ASMIS is therefore essential. Since security of the ASMIS has a given budget, it is key to use it as wisely as possible. Human factors are a common root cause for most incidents and should because of this accordingly be considered. (Johnson 2021), (Cox 2012)

Many data breaches do occur, since employees of an organization do simply not fully know the value of the data, they are handling. Some might have an understanding that they are handling sensitive data, but most employees do not know the current threats to the data and due to this underestimate, the risk their behavior sometimes poses. An essential element to the tailored annual cyber awareness training thus should be the value of PHI and the current threat landscape a hospital faces. This element comes with little cost and is likely to prevent many social engineering attacks. (The CERT Insider Threat Team 2013)

Another human factor causing data breaches frequently, is the fact that hopsital staff is very focused on their goal to treat patients. Secondary tasks like dealing with an ASMIS are handled with lower priority. The fact, that employees are biased by their goal to treat patients leads to the fact that employees do not plan for sufficient time, read instructions in a rush, see security as hindering to their task etc. An hospital ASMIS providing a well thought out balance between security, functionality and usability can overcome most of those issues. (Johnson 2021), (Sasse & Rashid 2019).

Essential to a balanced ASMIS is to design it with the weaknesses and strength of the human in mind. The human eye for example only truly focuses on a small portion within the visual field. Any critical security message therefore should be emphasized appropriately. To do so one could blur out the background and display a pop up having intuitive or known pictograms. This will immediately catch the attention of the user. Combined with the pop-up box shaking no one will miss this alarm. This highlighting however should be done with care, since a user that gets those

messages nonetheless learns to ignore them forever, if their content is in fact seldomly critical. (Johnson 2021), (Waite 2010)
It is also very important to keep any security message short and understandable, that are shown to the user. Many people think that security messages should be lengthy and comprehensive. The opposite is in fact the case. If there is however lengthy information, that must be shown to the user a sound structure to support the reading is necessary. Vocabulary that is not common to the user but might be common to the developers should also be avoided. (Johnson 2021)

Another reason to engage in behaviors endangering the company, is the so called knowing doing gap of individuals. It is a known fact, that sometime people still choose to engage in risky behavior, although they are aware of the negative consequences a successful hack might pose. This has several reasons one being for example that in western culture you are trained that productivity is the primary goal in your work life and it is socially acceptable that you cut corners to achieve your goal. Another reason for some to act against corporate policy is because the have narcissitic tendencies. Knowing this is essential to successfully manage this human factor, since corporate training, will not fix this issue. It is however more effective that superiors montior the behaviour of employees and resolve personnel issues individually or forward it to the software developers in order to implement changes to the user interface (UI), that makes certain cutting of corners impossible. (Cox 2012)

Most data breaches occur due to human interaction, where either the behavior is the reason, or the UI is not designed well. Simply measures such as designing the UI properly, regular training and continuous monitoring of employees, will however significantly strengthen security and are thus recommended. When designing or adapting the UI it is essential to find the right balance between usability, functioanlity and security, which is very case indivdual and cannot be transported from e.g., a sales company to a hospital. Finally it also needs to be stated, that fitting the task to the human is in the long run proven to be more cost effective than vice versa. (Sasse & Rashid 2019), (Cox 2012), (Waite 2010)

References:

Cox, J. (2012) Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior* 28: 1849-1858:

https://www.researchgate.net/publication/257252888_Information_systems_user_security_A_structured_model_of_the_knowing-doing_gap

Johnson, J. (2021) *Designing with the Mind in Mind*. Third Edition. Cambridge: Elsevier Inc.

Sasse, A. Rashid, A. (2019) *Human Factors Knowledge Area.* First Edition. Bristol: CyBOK

The CERT Insider Threat Team (2013) Unintentional Insider Threats: A Foundational Study. Social Engineering Institute. Available from: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

Yao, M. (2017) *Your Electronic Medical Records Could Be Worth $1000 To Hackers*. Forbes. Available from: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/?sh=1c8f72f450cf [Accessed on 08.10.2021]

Waite, A. (2010) InfoSec Triads: Security/Functionality/Ease-of-Use Available from: https://blog.infosanity.co.uk/?p=676

Bibliography:

Kokolakis, S. (2015) Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Computers & Security DOI: https://doi.org/10.1016/j.cose.2015.07.002

Sasse, M.A & Rashid A (2019) Human Factors Issue. The Cyber Security Body Of Knowledge (1). Available from: https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf