**Turnitin submission ID: 1886355595**

4 hours ago

The Queens Medical Centre is a local community healthcare provider. It has recently installed an appointment and scheduling management information system (ASMIS) to help it better manage the patient appointments. Whilst the system is considered secure by the clinic’s IT team, the management team is aware of the human factor impact on the cyber security and would like this impact to be analysed and assessed.

To be able to determine the applicable human factors and assess its impact, it is assumed that ASMIS is used by the patients and the clinic’s employees: administrative staff, general practitioners, nurses, management, and IT teams. It is also assumed that the clinic’s staff has a higher system authorisation level than the patients, and thus poses a higher threat. Because of it, the staff will be used as the primary source in this human factor impact analysis.

When securing a system from cyber threats, the primary focus is often on the technology related countermeasures whilst the system users and their behaviour is often ignored (Bowen et al, 2011). A 2021 (Critical Insights) report indicates that there were 45 million individuals in the US alone impacted by the healthcare data breaches thus highlighting the need for a sociotechnical approach to cyber security rather than just the technical countermeasures (Malatji et al, 2019).

Three human factors have been identified as of interest in terms of its impact in the healthcare system setup, namely: the human limitations and biases, workplace related stress and pressure, and the varied risk perceptions.

Many cyber-attacks, such as phishing, exploit human bias (Lyn Paul et al, 2019), thus, the confirmation and availability biases should be considered when creating a security policy. A confirmation bias is a term that refers to the seeking of evidence which conforms to the existing beliefs (Nickerson, 1998). The availability bias, on the other hand, refers to the decision making based on the small sample of data (Ting, 2022). The two biases combined can have a great impact on the security related actions taken by the individuals as well as on those responsible for the Cyber Security policy design.

For example, the medical centre staff may not log out of ASMIS after finishing their tasks, leave their machines unlocked whilst away from their desks, write down their passwords or use weak passwords because of confirmation bias: the users tend to believe they are out of reach of a cyber-attacks just because they weren’t targeted previously (Ting, 2022).

When creating a new cyber security policy or user training, the management and IT teams may choose to emit what they deem to be less important security aspects and focus on the countermeasures required to address the threats they have seen on the news instead, for example (Smith, 2012). Whilst these prioritised threats may be less relevant to ASMIS, due to the availability bias, it can seem more important because of the person’s recent exposure to it.

Another human factor which plays an important role in the overall success of the cyber security is stress and pressure. Recent data published by the HSE UK (2021) has shown an increase in self-reported work-related stress and anxiety when compared to pre-coronavirus levels. A 2021 study (Gilleen) has further confirmed the high levels of poor mental wellbeing of the UK healthcare staff. Various studies have demonstrated the linkage between the poor decision making and the level of stress (Park, 2013; Michailidis & Banks, 2016; Tsiga et al, 2017) and provided clear evidence of the need to address this factor when designing a cyber security action plan.

The burnout at work can result in the riskier behaviours, such as: sharing patient data with un-authorised colleagues or discussing it on social media, not reporting cyber security breaches, absent-mindedly clicking on suspicious links in the emails (Fauzi et al, 2021), etc. Since the medical organisation capacity levels are reaching an all-time high (Royal College of Nursing, 2021), work induced stress and pressure has an even greater impact on the security related decision making.

The study by Fauzi et al (2021) has found a correlation between the stress and the changes in the risk perception, however, stress is not the only factor impacting our attitudes towards the risk taking: frequent technology users tend to be higher risk takers (Öğütçü, 2016) and so do those who have not experienced a data breach or have not received any education on the cyber security (Kostyuk & Wayne, 2019). In terms of ASMIS, the medical centre staff is likely to underestimate the threat of cyber security risks should they receive no training on this subject. Equally, more experienced IT staff may underestimate the threats, having more false confidence in the system.

Peoples’ biases, risk perceptions and work-related stress are all intertwined and can have a significant impact on the overall systems’ security. Since computer systems do not exist in a vacuum and interactions with people are unavoidable, it is of great importance to not only address the technical aspects of the cyber security, but also the social ones.

**References**

Bowen, B.M., Devarajan, R. and Stolfo, S. (2011) Measuring the human factor of cyber security. 2011 IEEE International Conference on Technologies for Homeland Security (HST).

Critical Insights (2021) Critical Insight Healthcare Data Breach Report Jan-Jun 2021 Key Findings. Available from: https://www.criticalinsight.com/resources/news/article/critical-insight-healthcare-data- breach-report-jan-jun-2021-key-findings [Accessed 20 August 2022].

Fauzi, M.A., Yeng, P., Yang, B. and Rachmayani, D. (2021) Examining the Link Between Stress Level and Cybersecurity Practices of Hospital Staff in Indonesia. The 16th International Conference on Availability, Reliability and Security.

Gilleen, J., Santaolalla, A., Valdearenas, L., Salice, C. and Fusté, M. (2021) Impact of the COVID-19 pandemic on the mental health and well-being of UK healthcare workers. BJPsych Open, 7(3).

HSE (2021) Work-related stress, anxiety or depression statistics in Great Britain, 2021. Available at: https://www.hse.gov.uk/statistics/causdis/stress.pdf [Accessed 23

August 2022].

Kostyuk, N., & Wayne, C. (2019) Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats.

Lyn Paul, C., Blaha, L.M., Fallon, C.K., Gonzalez, C. and Gutzwiller, R.S. (2019) Opportunities and Challenges for Human-Machine Teaming in Cybersecurity Operations. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), pp.442–446.

Malatji, M., Von Solms, S. and Marnewick, A. (2019) Socio-technical systems cybersecurity framework. Information and Computer Security, 27(2), pp.233–272.

Michailidis, E. and Banks, A.P. (2016) The relationship between burnout and risk- taking in workplace decision-making and decision-making style. Work & Stress, 30(3), pp.278–292.

Nickerson, R.S. (1998) Confirmation bias: A ubiquitous phenomenon in many guises. Review of General Psychology, 2(2), pp.175–220.

Öğütçü, G., Testik, Ö.M. and Chouseinoglou, O. (2016) Analysis of personal information security behavior and awareness. Computers & Security, 56, pp.83–93.

Park, Y.-M. and Kim, S.Y. (2013) Impacts of Job Stress and Cognitive Failure on Patient Safety Incidents among Hospital Nurses. Safety and Health at Work, 4(4), pp.210–215.

The Royal College of Nursing. (2021) Pressure on staff ‘unsustainable’ as nurse to patient ratios diluted to meet demand. Available at: https://www.rcn.org.uk/news-and- events/news/uk-pressure-on-staff-unsustainable-as-nurse-to-patient-ratios-diluted-to- meet-demand-150120 [Accessed 23 August 2022].

Smith, S.W. (2012) Security and Cognitive Bias: Exploring the Role of the Mind. IEEE Security & Privacy, 10(5), pp.75–78.

Ting, D. (2022) Why Cognitive Biases and Heuristics Lead to an Under-investment in Cybersecurity.

Tsiga, E., Panagopoulou, E. and Montgomery, A. (2017) Examining the link between burnout and medical error: A checklist approach. Burnout Research, 6, pp.1–8.

Response for 200 words