An outline of the human factors and socio-technical problems of acquiring an appointment and scheduling management information system (ASMIS).

When acquiring an ASMIS, human behaviour plays a crucial role in maintaining the CIA Triad (Ham, 2021). We will discuss three human factors of social engineering, malicious insider threat and human error, considering the socio-technical issues faced with ASMIS implementation in Queen's Medical Centre.

We can analyse the significance of various actors using the ASMIS, such as patients, receptionists, managers, doctors, IT administration staff and external cyber criminals and their implications.

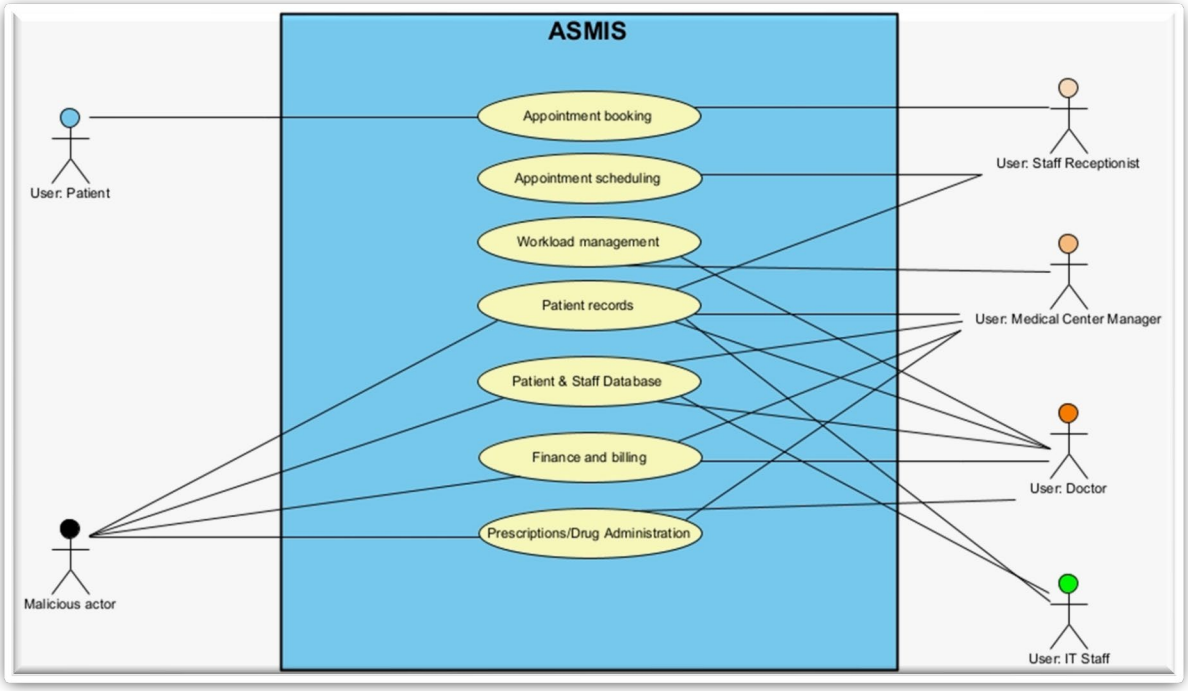

Figure 1: Use case diagram indicating actors to the ASMIS.

External threat actors using social engineering methods such as pretexting and phishing pose a high-risk factor. In this scenario, the malicious actor may pose falsely

as an authoritative figure and attempt to gain levels of trust from an employee. This is commonly used on the telephone, and victims may divulge sensitive information or grant access to the intruder. The actor preys on the vulnerability of the employee's character; it must be noted that grumpy or socially awkward employees can be less susceptible to falling for pretexting attempts (Steinmetz, 2021). Phishing is more common, whereby employees are sent believable emails that can provide fraudulent links and give access to malicious actors (UK Department for Digital Culture Media and Sport, 2019).

The malicious insider threat considers the dated view from Colwill (2009) that 90% of security controls are focused on the external threat. However, due to the nature of the risk posed to medical centres, more recent studies suggest organisations focus on insider threats. Compared to studies by Gheyas & Abdallah (2016), we find that most insider threats are based upon opportunities presented rather than capabilities. The users of any privilege level generally target file repositories and databases due to the value of sensitive data available (Gheyas and Abdallah, 2016).

These users could be disgruntled employees or take advantage of an opportunity. These findings are further supported by McIlwraith (2021), who identified up to 85% of security incidents by the company's employees. The perception of risk and workplace culture directly affects human behaviour, whereby education and training to vital to minimise insider threats. (McIlwraith, 2021).

Human error can stem from social engineering techniques or negligence from an employee; accidental insiders pose a significant risk. No planning of malicious intent,

security protocols and system usability can be confusing (Hadlington, 2021). Lack of understanding regarding the importance of the health data they manage and unrealised responsibility of how their behaviour could put the assets at risk. All users should not be ignorant of potential risks (Kearney and Kruger, 2016).

Security protocols of access control so health records are secure by privilege level help prevent data leaks. In severe cases, malicious users who gain access to wider area networks accidentally provide access to malicious networks. Healthcare can be restricted, such as in the NHS Wannacry attack (Dwyer, 2018). Health reports can be shared across departments and authorities to maintain confidentiality and not have restricted medical treatment, which could cause fatalities (Sharma, 2021).

Incidents will arise from inadequate training or latent failures combined with active failures from the individual. This supports McIllwraith's (2021) view that workplace culture is crucial not to have a latent environment whereby employees are stressed or fatigued.

Furthermore, complex usability increases risk, and incidents are not due to single actions alone. The Swiss-Cheese Model (Sasse and Rashid, 2019) identifies barriers in place from technology, process, and people to bridge the knowing-doing gap (Cox, 2012) and create a more transparent workplace where anyone can report incidents of senior employees to support bridging and change attitudes (Vilander et al., 2021).

Adapting security to humans is difficult as humans have limited capabilities (Sasse and Rashid, 2019). This limitation presents difficulties in meeting the intended goals

of the ASMIS. Humans can have short/long-term memory challenges and visualising a perceived threat. The user experience (Hartson and Pyla, 2019) is perhaps one of the crucial components of usability. The medical centre will see high volumes of patients, which challenges health data security, as doctors and staff may change roles or departments.

Therefore the user interface should be designed so that users' workload and flow require minimal comprehension with measures such as security by default (Gorski et al., 2018) which is built-in to the ASMIS. Understanding in design should consider human disabilities (Scholz et al., 2017) and privacy implications (Kang et al., 2015). Medical centre staff need to know where data is accessible for GDPR regulations and controls following a framework such as ISO/IEC 27002. If the ASMIS considers using a third-party vendor service, a SOC2 report could be generated to identify risk.

Training and awareness of human risks for improved staff education are necessary. Therefore we can consider that insiders of staff members, doctors, and IT Administrators of the medical centre play a crucial role in security practice. They are deemed a potential vulnerability, and mechanisms should be in place from a technological view to provide security triggers for potential security breaches. Other frameworks such as HEART (Harte et al., 2017) could be implemented to improve the user experience and usability of the ASMIS.

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

Dwyer, A. 2018. The NHS cyber-attack: A look at the complex environmental conditions of WannaCry. *RAD Magazine,* 44**,** 25-26.

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.

Hadlington, L. 2021. The “Human Factor” in Cybersecurity: Exploring the Accidental Insider. *In:* MANAGEMENT ASSOCIATION, I. R. (ed.) *Research Anthology on Artificial Intelligence Applications in Security.* Hershey, PA, USA: IGI Global.

Ham, J. V. D. 2021. Toward a Better Understanding of “Cybersecurity”. *Digital Threats,* 2**,** Article 18.

Harte, R., Glynn, L., Rodríguez-Molinero, A., Baker, P. M. A., Scharf, T., Quinlan, L. R. & Ólaighin, G. 2017. A Human-Centered Design Methodology to Enhance the Usability, Human Factors, and User Experience of Connected Health Systems: A Three-Phase Methodology. *JMIR Hum Factors,* 4**,** e8.

Hartson, R. & Pyla, P. 2019. Chapter 12 - The Nature of UX Design. *In:* HARTSON, R. & PYLA, P. (eds.) *The UX Book (Second Edition).* Boston: Morgan Kaufmann.

Kang, R., Dabbish, L., Fruchter, N. & Kiesler, S. 2015. "My data just goes everywhere": user mental models of the internet and implications for privacy and security. *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security.* Ottawa, Canada: USENIX Association.

Kearney, W. & Kruger, H. 2016. Theorising on risk homeostasis in the context of information security behaviour. *Information and Computer Security,* 24**,** 496-513.

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

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].

Scholz, F., Yalcin, B. & Priestley, M. 2017. Internet access for disabled people: Understanding socio-relational factors in Europe. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 11**,** Article 4.

Sharma, A. 2021. Online Doctor Appointment System.

Steinmetz, K. F. 2021. The Identification of a Model Victim for Social Engineering: A Qualitative Analysis. *Victims & Offenders,* 16**,** 540-564.

Uk Department for Digital Culture Media and Sport. 2019. *Cyber Security Breaches Survey 2019: Statistical Release* [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf [Accessed 21 June 2022].

Vilander, J., Tiedekunta, I., Technology, F. O. I., Informaatioteknologia, Technology, I., Yliopisto, J., Jyväskylä, U. O., Tietotekniikka, Technology, M. I. & 602. 2021. *Bridging the knowing-doing gap: the role of attitude in information security awareness.*