I. INTRODUCTION

A. Background

1. Queens medical centre acquiring ASMIS.
2. Install a web-based system for appointment and scheduling with cybercrime and patient data protection concerns.
3. Cyber Security Officer advises on human factors for ASMIS to be usable and secure.

B. Scope

1. Human factors (3): Discuss Management's requirements and expectations
   i) Insider malicious threat
   ii) Social engineering
   iii) Human error
2. Socio-technical problems.
3. Discuss implications and analysis of various actors in the ASMIS system.

II. BODY

C. Human factors with Management requirements and expectations.

1. **Insider malicious threat:**
   Fraud- 70% inside employee
   90% of security controls focused on the external threat (Colwill, 2009)
   Malicious intent
2. **Social Engineering:**
   Pretexting
   Phishing (UK Department for Digital Culture Media and Sport, 2019)
3. **Human error:**
   Access control: Patient records can be secured by only the staff that need access.
   GDPR -conforms the system to regulations. Data confidentiality is established with access control.
   Reports can be shared easily with patients and privileged users who require access (linked departments, health authorities) (Sharma, 2021)
   Swiss cheese model (Sasse and Rashid, 2019)
   Latent failure + active failure = incident
   Knowing-doing gap (Cox, 2012)
   Ignorance of risk (Waite, 2010) (Kearney and Kruger, 2016)
   Accidental insider (The CERT Insider Threat Team, 2013)

D. Risk in socio-technical problems

1. **Adapting security to humans:**
   Human capabilities and limitations (Sasse and Rashid, 2019) / Goals / Usability
   e.g STM / LTM / Passwords (Johnson, 2010)
   ASMIS limitations with security
   Captchas (Reynaga et al., 2015)
   e.g. Patient records can be challenging to secure as doctors/nurses can move roles or departments. Personnel can have access for safety, privacy or both. (Anderson, 2008)
2. **System process and design (UI) (Johnson, 2010):**
   Workload and flow (Sasse and Rashid, 2019)

Security mechanism triggers
Default security

3. **Environment:**
   Light/Noise/Temperature/Pollution (Sasse and Rashid, 2019)
4. **User Experience (UX) (Hartson and Pyla, 2019)**
   Disability (Dobransky and Hargittai, 2006) (Scholz et al., 2017) / Rehabilitation Act (McLawhorn, 2001)
   Mental Models (Camp, 2009)
   Privacy implications (Kang et al., 2015)

III. CONCLUSION

E. Well-reasoned judgement concludes the implications of the most significant human factor from the three discussed.
F. Possibly outline assumed recommendation/strategy for solutions?

IV. REFERENCES

Anderson, R. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems,* Indianapolis, USA., Wiley.

Camp, L. J. 2009. Mental models of privacy and security. *IEEE Technology and Society Magazine,* 28**,** 37-46.

Colwill, C. 2009. Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report,* 14**,** 186-196.

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

Dobransky, K. & Hargittai, E. 2006. The disability divide in internet access and use. *Information, Communication & Society,* 9**,** 313-334.

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.

Johnson, J. 2010. *Designing with the Mind in Mind: Simple Guide to Understanding User Interface Design Rules*, Morgan Kaufmann Publishers Inc.

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.

Mclawhorn, L. 2001. Recent Development: Leveling the Accessibility Playing Field: Section 508 of the Rehabilitation Act. *North Carolina Journal of Law and Technology,* 3.

Reynaga, G., Chiasson, S. & Oorschot, P. 2015. *Exploring the Usability of CAPTCHAS on Smartphones: Comparisons and Recommendations*.

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.

The Cert Insider Threat Team. 2013. *Unintentional Insider Threats: A Foundational Study* [Online]. Social Engineering Institute. Available:

https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf [Accessed 21 June 2022].
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].
Waite, A. 2010. *InfoSec Triads: Security/Functionality/Ease-of-Use* [Online]. Available: https://blog.infosanity.co.uk/?p=676 [Accessed 21 June 2022].

V. APPENDICES