**Human Factors of an ASMIS**

University of Essex Online

Master of Cyber Security

The Human Factor

July 2022

# Contents

[Contents 2](#_Toc107610171)

[Introduction 3](#_Toc107610172)

[Human Factor Considerations 3](#_Toc107610173)

[Implications 5](#_Toc107610174)

[References 7](#_Toc107610175)

# Introduction

To further enhance the security posture at Queens Medical Centre, it is imperative that the system is designed with humans in mind. Humans are hard wired to behave in particular ways, they have the ability to introduce errors and omissions (intended or unintended), and have the ability to be tricked (by the use of social engineering, for example). These flaws are not considerations for the technology of the ASMIS itself, and as such, the following human related factors have been highlighted for special consideration.

# Human Factor Considerations

**Habituation**

Habituation is not the same as “habit”. Habituation is the brain’s desensitisation to repeated stimuli over time.

Habituation is described by Sasse (2019) as one of four types of latent failures that are more likely to cause people to make errors, along with limitations of human memory.

It is part of what forms our “experience”, a subcategory of our perception bias in our minds based on past events (Johnson, 2021) and may be one explanation for the Privacy Paradox, where even though users are aware of risks, they continue to act irresponsibly (Kokolakis, 2015).

**Mental Models**

Mental models is a term used to describe how users perceive a given system or service and how it works. Although it was found having a superior knowledge of technology and security is not sufficient to improve one’s security habits, users with a limited understanding of technology, generally have a more simplified mental model, and therefore may be unaware of the risks involved in using the ASMIS (Kang et al., 2015). Those that have a more articulated mental model of how technology works may be more aware of vulnerabilities and threats (such as hackers) and therefore may also have a more positive approach to security due to their awareness of (perceived) vulnerabilities (Cox, 2012).

**Trust**

Humans are inherently trusting (Kosfield, 2008), and this is unfortunately something which can be detrimental to security.

Humans who trust in their organisation’s ability to maintain a security environment are less likely to carry out additional security checks of their own (Kearney & Kruger, 2016). This also affects the state of perceived vulnerability, as stated earlier.

Humans also consistently trust people in certain situations, which may leave them open to social engineering exploitation. For example, users are more likely to trust an impersonator if they:

* Pretend to be someone in a position of power, such as a CEO or a manager (authority)
* Offer something in return, such as a voucher or prize (Reciprocity)
* Tell the user everyone else is already doing something (Consensus)

These are some examples of ways in which users may be coerced into giving up sensitive information (Kelley, 2020).

Finally, users may put their trust in irrelevant information such as a familiar company logo on a website (University of Essex Online, 2022), a laptop on a tidy desk, or a particularly friendly colour (Camp 2009). All of which have absolutely no effect on the level of security, nor the threat that is posed.

# Implications

All of the above human factors can weaken the organisation’s security. Users, who experience continuous, similar error messages, may decide to ignore them as after time as they become annoying. This is known as alarm fatigue, and can become a huge problem for both staff and patients as important alarms and notifications may be subsequently dismissed or ignored (Sasse, 2019).

Mental Models are not only about how simplistic a user perceives the system. They can also be formed to simulate a particular scenario, such as a battle between the organisation and the enemy (warfare). This model is relatable in cybersecurity, however it can also be problematic due to the perception that the organisation’s security experts (military) are responsible for keeping staff protected (civilians), while relieving general staff of their duties (Camp, 2009).

Trust makes social engineering particularly problematic and a potentially worse threat to an organisation than any hacker as it offers a way for a user to simply allow the attacker to “log in”, rather than require any skillset to circumvent security technology. Additionally, they can manipulate them into running malware on a system, which may run at a level of privilege higher than the hacker could otherwise, causing devastation, data exfiltration or open possible backdoors into the system. Phishing is another security threat caused by the trust a user puts in particular emails. Users may receive scores of emails each day and 99% of them they see will be legitimate, however it is because of this habituation and trust combination that causes them to click on malicious links, designed to look like their bank account, logo and all. Phishing is a particularly problematic subject as in 2022, once again, it was the most common incident reported by UK businesses and charities (HM Government, 2022).

Finally, unless the system is usable, existing user mental models may cause users to enter erroneous information or make slips and mistakes (Johnson, 2021). Unfamiliar terminology, functions, and layouts may cause frustration and make the system difficult to use, negating the initial purpose of the ASMIS, or cause them to reduce their desire for security, such as by entering a simple password while still meeting minimum requirements.

# References

Camp, L.J. (2009) Mental Models of Privacy and Security. Available from: <https://0-ieeexplore-ieee-org.serlib0.essex.ac.uk/document/5247001> [Accessed 30 June 2022].

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. Available from: <https://www.sciencedirect.com/science/article/abs/pii/S0747563212001318> [Accessed 30 June 2022].

HM Government. (2022) Cyber Security Breaches Survey 2022. Available from <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022> [Accessed 29 June 2022].

Johnson, J. (2021) *Designing with the Mind in Mind*. Waltham: Morgan Kaufmann. Available from: <https://essexonline.vitalsource.com/reader/books/9780128182031/pageid/18> [Accessed 30 June 2022].

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. Available from: <https://www.usenix.org/conference/soups2015/proceedings/presentation/kang> [Accessed 30 June 2022].

Kearney, W.D. & Kruger, H. A. (2016) Theorising on risk homeostasis in the context of information security behaviour. Available from: <https://0-www-emerald-com.serlib0.essex.ac.uk/insight/content/doi/10.1108/ICS-04-2016-0029/full/html> [Accessed 30 June 2022].

Kelley, D. (2020) The psychology of social engineering—the “soft” side of cybercrime. Available from: <https://www.microsoft.com/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime> [Accessed 30 June 2022].

Kokolakis, S. (2015) Privacy attitudes and privacy behaviour:

A review of current research on the privacy paradox phenomenon. Available from: <https://0-www-sciencedirect-com.serlib0.essex.ac.uk/science/article/pii/S0167404815001017?via%3Dihub> [Accessed 30 June 2022].

Kosfield, M. (2008) Brain Trust. Available from: <https://greatergood.berkeley.edu/article/item/brain_trust> [Accessed 30 June 2022].

Sasse, M. A. (2019) Human Factors Knowledge Area Issue 1.0. Available from: <https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf> [Accessed 30 June 2022].

University of Essex Online. (2022) Mental Models and Their Impact on Security. Available from: <https://www.my-course.co.uk/Computing/Cyber%20Security/THF/THF%20Lecturecast%202/content/index.html#/lessons/f3lsdplAb3pHYIBUx__uSqbIxcwPrNdN> [Accessed 30 June 2022].