**Mitigations of an ASMIS (Human Factors)**

University of Essex Online

Master of Cyber Security

The Human Factor

July 2022

# Contents

[Contents 2](#_Toc109487235)

[Introduction 3](#_Toc109487236)

[Mitigations 3](#_Toc109487237)

[Legal, Social and Ethical Considerations 7](#_Toc109487238)

[Conclusion 8](#_Toc109487239)

[References 11](#_Toc109487240)

[Appendix 14](#_Toc109487241)

# Introduction

The following mitigating solutions have been recommended to Queens Medical Centre based on the human factors defined in the previous report. The solutions mapping to the previously found problems (Trust, Habituation, and Mental Models) can be found in the Appendix. All recommendations are designed to complement the existing technological controls and help the ASMIS become more secure.

# Mitigations

1. **IT Security Awareness Training**

An important tool when considering security from a human point of view, and in fact now is required by many laws and regulations, including GDPR. By educating staff, they become aware of threats at a high level and as a result, can adjust their mental models, meaning they are more likely to be hardened to attempts such as phishing and social engineering, and more likely to report incidents rather than fall victim to them. IT Security Awareness is not only about educating users, it should also be designed to open the communication channels with the IT security team and promote risk communication with their peers (ENISA, 2018). IT security teams should promote a positive message in dealing with security, as staff will be more likely to report security incidents and respond well to threats if they feel they are a positive contributor to the security effort rather than being seen as the weakest link (Cox, 2012). Training should not be a one off attempt, however it should be launched as a continuous improvement campaign, and targeting areas where problems have been found using previous findings. The COM-B and B=MAT behavioural models, as shown in Figures 2 and 3, can be useful in determining this (ENISA, 2018).

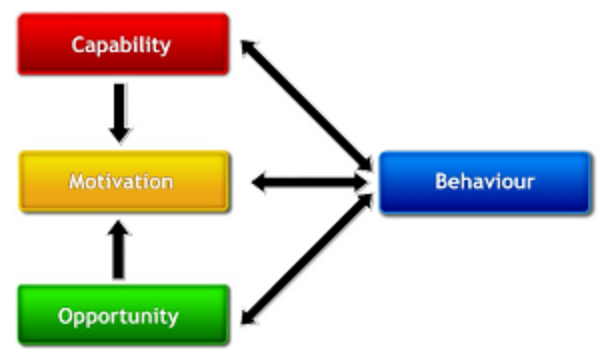


Figure 2: COM-B Model (Michie et al., 2011)

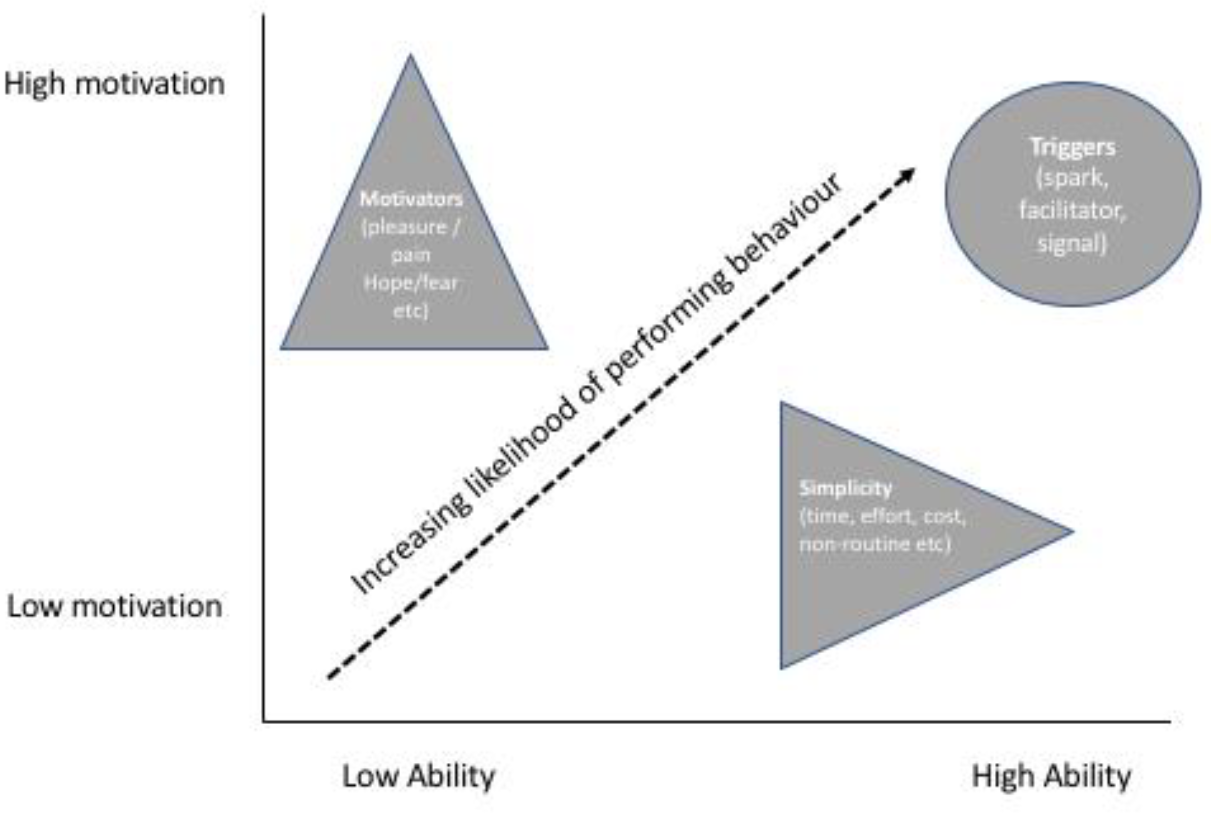


Figure 3: Adapted B=MAT Model (ENISA, 2018)

1. **Policies**

Policies are essential to any Governance, Risk Management and Compliance (GRC) effort at an organisation and help to keep everyone focused by enforcing ways of working. This makes processes easier to follow, controls workflows throughout the organisation, and also helps to address the Knowing-Doing Gap (Cox, 2012) by threatening disciplinary action if they are not followed. Policies have the additional benefit of changing culture, forming new subjective norms, and immediately allowing new employees to understand and conform to such a security culture at the organisation (Software Engineering Institute, 2013). It is imperative that these policies have the full backing and compliance of top management, or else there is potential for them to lose impact and credibility (NCSC, N.D.).

1. **Mock Phishing Campaigns**

It is suggested that humans are more willing to adopt a more secure behaviour once they have themselves experienced a negative experience (Kang et al, 2015). Of course, it should not be necessary to prove this with a real attack, however it is possible to simulate. Mock phishing campaigns can be conducted as a schedule of security incident “drills” designed to keep everyone aware of perennial threats. Such exercises send out entirely safe emails, mimicking real phishing attempts to encourage users to think more about emails, rather than blindly trusting them. Upon clicking on a containing link or attachment, the user is taken to a site showing that they clicked on a potentially malicious email, and explains the negative consequences of such actions. Through reporting, the IT Security department can then keep track of the number of victims and compare with previous campaigns to identify the overall state of awareness.

Although such campaigns should be conducted regularly to keep users constantly aware of threats, it is important not to overburden them as this can cause compliance fatigue, which may lead in turn to habituation (Sasse, 2019).

1. **User Experience (UX) Design**

Considering users’ mental models by incorporating attributes into the design of the system can make it more usable, and therefore more secure, as users are less likely to make errors and omissions. In order to do this, developers must view the ASMIS system from a member of staff, and patient’s point of view when designing. This includes designing the system consistent with cultural understandings such as using meaningful colours (e.g., red for alerts, green for success), recognisable symbols, common task execution paths, and consistent button labels (such as “Cancel”, “Save”, or “Finish”). This is important as patients and staff want to be able to concentrate on their work tasks rather than what the system does and how it works (Hartson & Pyla, 2019). If they are distracted with other things, they are distracted from their main goal, causing them to exhibit omissive behaviour or enter erroneous information. Thus, a more usable system is a more secure system.

Usage research can help when carried out in the context of the users’ work domain early in the design in order to better understand their needs (Hartson & Pyla, 2019). By designing a system which matches users’ work goals, it is possible to create a more usable system, which in turn should decrease the risk of habituation.

It should be also considered to keep the level of alerts to a minimum. Johnson (2021) refers to this as “Heavy Artillery”. Constant error messages may have good intentions but they can quickly become annoying, leading to users dismissing them and ultimately having the reverse effect. False positives and irrelevant information can have a similar effect, and so testing should be incorporated at every stage of the design.

# Legal, Social and Ethical Considerations

**Menlo Report**

The Menlo Report was written as a framework for ethical information computer and security research in information and communications technologies. Any usage research or user testing related to human behaviour used to improve the design of the ASMIS should abide by the framework. Such research, as listed in the report, should continue with the following principles in mind:

* Respect for Persons
* Beneficence
* Justice
* Respect for Law and Public Interest

U.S. Department of Homeland Security (2012).

**Other Considerations**

As the ASMIS has a public facing website, it is also obligated by law to provide affordances for people with disabilities and impairments. For example, in the UK, software vendors and website providers must comply with the Equality Act (2010). It is also recommended in order to comply with the applicable accessibility laws, that websites are designed and coded according to the Web Content Accessibility Guidelines (WCAG), which many international accessibility laws are created from (Siteimprove, N.D.). As the clinic contains private patient data, the ASMIS would also have to comply with data protection laws such as the Data Protection Act (2018) and UK GDPR (2022).

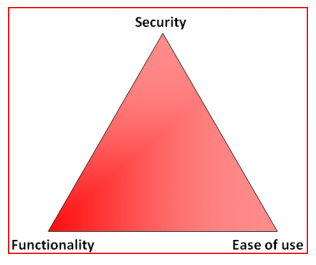
# Conclusion

The aforementioned tools will help provide a more secure ASMIS by considering the human factors involved.

The specialists and general staff using the system will be bound by policies and subjected to regular mock phishing campaigns. IT Security Awareness Training will ensure an improvement in education, awareness and communication with the IT Security team and their peers. These methods are designed to address users’ trust, and their mental models. As a result, reporting incidents should become more common, insider threats should pose less of a problem due to the positive security culture, and social engineering and phishing attempts are more likely to be thwarted. This of course reduces the chances of a successful attack made by bad actors as users will be less likely to trust unsolicited phone calls, emails and even face to face encounters, furthermore they will feel empowered to challenge them rather than blindly trusting them and handing over sensitive information. These human factor mitigations help to combat two major problems: Social engineering, which is a common precursor to real attacks, where attackers can learn more about a system by asking probing questions of the staff in a method called pretexting. They can also include directly asking or demanding a user’s login credentials. Additionally, phishing remains the UK’s most reported security incident.

Habituation in terms of the ASMIS is more of a fault in poor UX design. By introducing the recommended design features and considerations, the system will become more usable, and therefore more secure from a human factors point of view. By minimising the amount of beeps, alerts, errors, and dialogue boxes, the users are less likely to dismiss them. Additionally, by considering users’ existing mental models as part of the design, performing usage research, and by including intuitive defaults and task execution paths, they will be less likely to enter errors or omit data.

Of course, the introduction of any security measures will likely reduce the functionality and usability of the ASMIS, as Waite (2010) describes by using the Security / Functionality / Ease-of-use Triad as shown in Figure 9. However, by baking in the aforementioned design features, the reduction in usability and functionality of the ASMIS should be minimised, while still maximising security potential.

Figure 9: Security/Functionality/Ease-of-use Triad (Waite, 2010)

# References

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior* 28(5): 1849-1858. DOI: http://dx.doi.org/10.1016/j.chb.2012.05.003

Data Protection Act 2018, United Kingdom. Available from: <https://www.legislation.gov.uk/ukpga/2018/12/enacted> [Accessed 14 July 2022].

ENISA. (2018) Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Available from: <https://securitydelta.nl/media/com_hsd/report/228/document/WP2018-O-3-3-2-Review-of-Behavioural-Sciences-Research-in-the-Field-of-Cybersecurity.pdf> [Accessed 14 July 2022].

Equality Act 2010, United Kingdom. Available from: <https://www.legislation.gov.uk/ukpga/2010/15/contents> [Accessed 14 July 2022].

Hartson, R. & Pyla, P. (2019) *The UX Book.* 2nd Ed. Cambridge: Morgan Kaufmann. Available from: [https://0-www-sciencedirect-com.serlib0.essex.ac.uk/book/9780128053423/the-ux-book?via=ihub=](https://0-www-sciencedirect-com.serlib0.essex.ac.uk/book/9780128053423/the-ux-book?via=ihub=%20) [Accessed 14 July 2022].

Johnson, J. (2021) *Designing with the Mind in Mind* *Simple Guide to Understanding User Interface Design Guidelines.* 3rd Ed. Cambridge: Morgan Kaufmann. Available via the Vitalsource Bookshelf. [Accessed 18 July 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. *Symposium On Usable Privacy and Security.* 39-52. Available from: <https://www.usenix.org/conference/soups2015/proceedings/presentation/kang> [Accessed 18 July 2022].

Michie, S., van Stralan, M. M., & West, R. (2011) The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*. 6(1): 42 DOI: https://doi.org/10.1186/1748-5908-6-42

NCSC (N.D.) Board Toolkit. Available from: <https://www.ncsc.gov.uk/collection/board-toolkit> [Accessed 14 July 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 15 July 2022].

Siteimprove (N.D.) Overview of UK website accessibility laws. Available from: <https://www.siteimprove.com/glossary/uk-accessibility-laws> [Accessed 14 July 2022].

Software Engineering Institute. (2013) Unintentional Insider Threats: A Foundational Study. Available from: <https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf> [Accessed 14 July 2022].

UK GDPR 2022, United Kingdom. Available from: [https://www.legislation.gov.uk/eur/2016/679/contents](https://www.legislation.gov.uk/eur/2016/679/contents%20) [Accessed 17 July 2022].

U.S. Department of Homeland Security. (2012) The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. Available from: <https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf> [Accessed 14 July 2022].

Waite, A. (2010) InfoSec Triads: Security/Functionality/Ease-of-use. 12 June 2010. *Offensive and Defensive IT Security*. Available from: https://blog.infosanity.co.uk/?p=676 [Accessed 18 July 2022].

# Appendix

**Mitigation Mapping**

* MENTAL MODELS
  + Policies
  + IT Security Awareness
  + UX Design
* TRUST
  + Mock Phishing Campaigns
  + IT Security Awareness Training (E.g. anti-Social Engineering)
* HABITUATION
  + UX Design