# Addressing Human Factors for Secure & Usable ASMIS. *Human Factor Module*

According to the Ponemon Institute's (an independent research organisation conducting studies on data protection and emerging information technologies) 2020 global insider threat study, 62% of security breaches are found to be stem from human error and negligence of employees (non-malicious) (Ponemon Institute, 2020). While the overall cost of insider threats has risen 31% from 2018 to 2020, the number of incidents rose by 47%, highlighting that insider threats are still lingering and often an under-addressed cyber security threat within organisations. Though negligent insiders represent most incidents, incidents involving criminal or malicious insiders is the costliest per incident.

Following the definition guidance of Insider Threat Team, CERT (2013), an employee, a contractor, or a patient who have or had authorised access to ASMIS/data could become an unintentional insider threat through action or inaction without malicious intent. Such an action substantially increases harm to the confidentiality, integrity, or availability of Queens Medical Centre's ASMIS and data.

Failure in human performance leads to non-malicious insider threats, focusing on conditions that contributed to or even made unavoidable adverse outcomes can dramatically reduce human errors. However, they can never be eliminated entirely. The study by Insider Threat Team, CERT (2013), grouped these conditions into broad categories, which can be related directly to Queens Medical Centre operational environment.

### *Business processes and environment settings impacting the readiness of ASMIS users*

Any operational factors at the Queens Medical Centre that increase work pressures for its employees could result in work stress-based cognitive impacts such as attention deficits, poor situational awareness, and reduced working memory capacity (Greitzer et al., 2014). As stated in the assignment topic, a high volume of calls due to the growth of the community populations highlights work pressure in serving patients at different contact points.

Employees being direct users of the ASMIS with privileged access to patient's health information; a periodic short worker survey or a thorough investigation of the business processes and the operational environment identifying adverse impacts on employee behaviour would help clarify any unintended effects on employee morel or employee performance. The outcomes from the surveys are beneficial for risk management of avoiding the likelihood of employees lowering the acceptable performance thresholds and shedding some or even critical security-related responsibilities (Vishwanath et al., 2011).

Any exposure to confidential personal and health information accidentally due to work stress-based cognitive effects (Greitzer et al., 2014) or due to a situation like responding to

a phishing message when attending to too many emails (Jalali et al., 2020) must be prevented to avoid any strict legal action for privacy laws violations such as GDPR (European Commission, 2012). Therefore, well-managed employees' workload leads to increase information security.

### *Psychosocial, Sociocultural factors leading to variable risk perceptions and various personality predispositions*

Demographic factors (age, gender, and cultures) may influence risk tolerance/behaviour. According to Insider Threat Team, CERT (2013), males have lower risk perceptions, and females have higher risk perceptions. A study by Sheng et al. (2010) on demographic analysis of phishing susceptibility further revealed the same by concluding that females tend to attend phishing emails more often than men. The study also concluded that education could bridge this gap by providing anti-phishing education, reducing the inclination to provide information to phishing web pages by 40%.

Moreover, personality predispositions play an essential role in comprehending behaviours in cyber security. A study by Shappie et al. (2019) provides evidence that individuals high in conscientiousness and openness are more likely to engage in cybersecurity-related behaviours.

Deloitte's GDPR Benchmark Survey (2018) based on 1,650 consumers revealed that 70% would trust an organisation less if its data were compromised or if there is a history of data breaches - highlighting the importance of data security.

Therefore, it is vital to improving employees' sense of cyber security self-efficacy by evaluating Queens Medical Centre's socio/cultural work environment. Investing in and enhancing cyber security practices by employing emotion- and logic-based influencers, utilising effective user-system interface designs, conducting training, and awareness on individuals' biases and tendencies would help improve a sense of cyber security self-efficacy among employees (Greitzer et al., 2014; Shappie et al. 2019).

### *Security and compliance fatigue ruling cognitive biases*

Mental processes affecting our capability to perceive a specific situation based on inputs that we have met in the past are addressed as cognitive biases. They can play a crucial role in shaping one’s decision-making process in reasoning, evaluating, or remembering a situation.

The first step to overcome cognitive bias is to understand and acknowledge its impact. Security is a combination of process and technology, which depends heavily on human behaviour; therefore, focusing on procedures, tools, guidance, and training to identify, analyse, and monitor advanced cyber threats is essential in managing security threats.

The National Institute of Standards and Technology study (2016) found that many users have reached their saturation point and become desensitized to cyber security when they are bombarded with demands for compliance that they cannot take anymore. At that point, they become less likely to comply. When people are fatigued, they are prone to fall back on cognitive biases when making decisions.

Bear in mind Cormac Herley's (2014) quote, 'More is not the answer', crafting effective security awareness messages is vital to avoid any security and compliance fatigue. Shadowing General MacArthur's famous phrase 'never give an order that cannot be obeyed', never issue security guidance that is impossible to follow or are not effective.

# Reference


Cormac H. (2014) *More is not the answer*. Available from: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/MoreIsNotTheAnswer.pdf [Accessed 25 August 2021].

Deloitte (2018) *A new era for privacy GDPR six months on*. Available from: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf [Accessed 25 August 2021].

European Commission. (2012) Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Available from: https://ec.europa.eu/transparency/regdoc/rep/2/2012/EN/SEC-2012-72-2-EN-MAIN-PART-1.PDF [Accessed 27 August 2021].

Greitzer, F. et al. (2014) 'Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies', *Proceedings of the 2014 47th Hawaii International Conference on System Sciences.* Waikoloa, HI, USA, 6-9 January. IEEE. DOI: 10.1109/HICSS.2014.256

Insider Threat Team, CERT (2013) *Unintentional Insider Threats: A Foundational Study* Available from: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf [Accessed 25 August 2021].

Jalali, M., Maike, B., Daniel, W. & Gerhard, S. (2020) Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research*. 22(1). DOI:10.2196/16775

Kingsbury, D. (2017) Mapping cognitive biases in risk assessment. Available from: https://cybersecpsych.com/2017/07/11/mapping-cognitive-biases-in-risk-assessment/ [Accessed 25 August 2021].

NIST (2016) *'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests*. Available from: https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly [Accessed 28 August 2021].

Ponemon Institute (2020) *2020 Cost of Insider Threats*. Available from: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf [Accessed 25 August 2021].

Shappie, A., Dawson, C. & Debb, S. (2019). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media Culture*. 9 (4). DOI: 10.1037/ppm0000247.

Sheng, S., Holbrook, M, Kumaraguru, P., Cranor, L. & Downs, J. (2010) Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions, *28th ACM Conference on Human Factors in Computing Systems*, Atlanta, GA, USA, 10-15 April. DOI: DOI:10.1145/1753326.1753383

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*. 51: 576-586. DOI: 10.1016/j.dss.2011.03.002