**The Human Factor – Individual Presentation April 2022**

**Introduction**

This presentation will consider human factors and social technical problems encountered by Queens Medical Centre in ensuring optimal cyber security through an appointment and scheduling management information system (ASMIS). It will encompass a critical examination of effective strategies to promote and manage the human factor in cyber security. As well as an evaluation of the social and ethical considerations in developing and applying usable security.

The clinic offers various specialisations, traditionally appointments were scheduled via telephone then added manually to a scheduling system. High call volumes and population growth, combined with the human interaction required can result in patients not being attended to in a timely manner, meaning decreased customer satisfaction (Zhao, et al. 2017).

To ensure a high level of customer service and accurate scheduling, the management of Queens Medical Centre implemented ASMIS, allowing appointments to be booked online. Naturally, management is concerned with the high rate of cybercrime within the healthcare sector. Since 2010, data breaches in this sector have increased exponentially and it is now one of the most targeted industries by cyber criminals (Argaw, et al. 2020). Nifakos et al (2021) state that healthcare professionals have at times experienced the greatest volume of cyberattacks with most significant impact relating to social engineering.

This presentation considers three human factors and social technical problems associated with ASMIS, human interaction and how to mitigate them. These being training and awareness, Cyber Culture and Stake holder and leadership engagement.

Arguably, there are broad ethical considerations to be made by any medical institution given the sensitivity of data they store. Cybersecurity ethics must be applied to cultivate ethical sensitivity of patients, doctors, and board members (Formosa et al, 2021). GDPR is a new requirement for Queens as the clinic will now be storing personal patient information.

**Training and awareness**

Employees can be the weakest link in cyber defence however, with the right training employees can be your biggest allay (Pollini et al, 2021). A study was conducted in 2010 to determine the impact of cyber threat education and awareness intervention. This involved numerous groups of people from many different companies presented with hi-level (low detail) and low-level (high detail) cyber training. The high detail training made the most significant impact, compared to the low detail training, users in the high detail training changed their personal and work passwords to be more complex and set a schedule for future changes. The study found that when users are educated and trained about proper security practices, their behavior can be changed to enhance online security for themselves and the firms where they are employed (Kevin et al 2010).

Training is ethically essential. NIST (2017) reported that 35% of all data breaches are attributed to negligence or human error. Interestingly Kaspersky Lab and B2B International undertook a study on the role that employees play in the fight against cybercrime. The result revealed that 52% of all businesses believed that they are at risk from within (Kaspersky, 2017).

Importantly, traditional cyber training does not work for everyone, motivation is the key ingredient to successful learning. Employee motivation for cyber training and awareness can be difficult to achieve as people have different motivators. Many forms of security training fail as the users are not required to think and apply security concepts.

One interesting avenue for learning and motivation is game-based learning, computer and video games which are specialised in motivation. A highly interactive video game used by the US military (CyberCIEGE) could be used as an organizational training tool and has proved to be an effective addition for basic cyber awareness training programs (Benjamin et all 2007). 80% of all breaches in 2021 occurred from phishing attacks. Therefore, a game such as Anti Phishing Phil which is based on learning science principles could be used as an effect training awareness tool. Another study suggests that playing the game for 15 minutes dramatically increases knowledge of identifying three types of phishing URL’s: IP based URLs, sub domain, and deceptive. The results conclude that interactive games can be a promising way of teaching awareness of phishing attacks (Sheng et al, 2007).

**Cyber Culture**

Cyber security has been researched for decades and still many businesses fall short of creating a successfully secure culture. Betsy et al (2021) analyzed 58 research articles over ten years from 2010, using the PRISMA systematic literature review technique. The research indicated that there had been a significant increase in creating sturdy security cultures by implementing top down, consistently managed frameworks. It highlighted that creation of organizational culture played a substantial role in cyber models.

Kasperky (2017) reports that 40% employees of businesses globally hide an incident when it happens. Embedding security into the corporate culture means that staff will be less overwhelmed whensecurity incidents occur, having standard operations procedures in place increases the probability of being reported efficiently (Tourinsky, 2021).

Three similar large organizations in Australia implemented five key initiatives to improve their cyber culture.

Table

Description automatically generated

The study showed that five initiatives dramatically influenced a positive culture change in businesses. It was highlighted that building a cybersecurity culture takes continual investment and effort, follow up assessments are needed to evaluate the culture and to achieve sustainable behavioral change (Moneer, 2020).

**Stakeholder and leadership engagement**

Today, more than ever cyber security and cyber risk encompasses not only risk of network breach but also loss of data, financial loss or irreparable reputational damage. (Rothrock et al, 2018). Stakeholders play a vital role in the implementation and continual improvement of the cyber security lifecycle.

Executives can no longer simply delegate cyber security to the information technology department. It is the responsibility of every employee at every level. (Rothrock et al, 2018).

Business executives, while familiar with the business and risk management, often view cybersecurity as solely a technical problem. This mindset needs to shift into incorporation and awareness of the human elements of risk as a core component of leadership (Hasib 2014).

Achievable through:

* Setting the tone of importance in security, leading by example. Employees notice and respect senior management when they fully take on the cyber security space (Tourinsky, 2021).
* Empowering staff by making it easy to raise security concerns at any level within the organisation.
* Speaking positively and freely to staff about the importance of cyber security within the organisation.
* Taking responsibility for the potential security risk they pose as likely targets(whales) for attackers to exploit and should take appropriate measures to act accordingly.

**ASMIS**

ASMIS has been proven to dramatically improve efficiency and quality of service within the healthcare sector. However, digital transformation and the COVID-19 global pandemic expedited the adoption rate of health information systems at the loss of the human factor (Nifakos et al, 2021). The Human factor is a scientific field that is underutilized and undervalued in information security and cybersecurity (NSTC, 2016). To quote Auguste Kerckhoffs, “It must be easy to use and must neither require stress of mind, nor the knowledge of a long series of events”. Understanding the human factor is the key to success in developing a security aware culture.

**Conclusion**

It's essential for Queens Medical Centre to create a genuine cyber culture with adequate motivational cyber security training, alongside stakeholder and management buy in. In doing this they must also incorporate the human factor, which is key in mitigating the security risks associated with human characteristics (Kadena and Gupi, 2021).

**References:**

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B.J. and Simoes, E. (2017). Web-Based Medical Appointment Systems: A Systematic Review. Journal of Medical Internet Research, 19(4), p.e134.

NIST (2017), 30th FISSEA Annual Conference, Available from: https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017\_Witkowski\_Benczik\_Jarrin\_Walker\_Materials\_Final.pdf [Accessed 22 March 2022]

Kaspersky (2017), The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Available from: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ [Accessed 22 March 2022]

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O’Leary, C., Eshaya-Chauvin, B. and Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1).

Kevin F. McCrohan, Kathryn Engel & James W. Harvey (2010) Influence of Awareness and Training on Cyber Security, Journal of Internet Commerce, 9:1, 23-41, DOI: 10.1080/15332861.2010.487415

Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen, (2007), A video game for cyber security training and awareness, Computers & Security, Volume 26, Issue 1, 2007, Pages 63-72, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2006.10.005.

Beyer, R.E. and Brummel, B., 2015. Implementing effective cyber security training for end users of computer networks. *Society for Human Resource Management and Society for Industrial and Organizational Psychology*.

Sheng, Steve & Magnien, Bryant & Kumaraguru, Ponnurangam & Acquisti, Alessandro & Cranor, Lorrie & Hong, Jason & Nunge, Elizabeth. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. ACM International Conference Proceeding Series. 229. 88-99. 10.1145/1280680.1280692.

Betsy Uchendu, Jason R.C. Nurse, Maria Bada, Steven Furnell, Developing a cyber security culture: Current practices and future needs, Computers & Security, Volume 109, 2021, 102387, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102387.

Moneer Alshaikh (2020), Developing cybersecurity culture to influence employee behavior: A practice perspective, Computers & Security, Volume 98, 102003, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102003.

Hasib, M., 2014. *Cybersecurity leadership: powering the modern organization*. Tomorrow's Strategy Today, LLC.

Rothrock, Ray A; Kaplan, James; Van Der Oord, Friso (2018), The Board's Role in Managing Cybersecurity Risks, MIT Sloan Management Review; Cambridge Vol. 59, Iss. 2: 12-15.

Nifakos, Sokratis & Chandramouli, Krishna & Nikolaou, Charoula & Papachristou, Panagiotis & Koch, Sabine & Panaousis, Emmanouil & Bonacina, Stefano. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors. 21. 10.3390/s21155119.

Kadena, E. and Gupi, M., 2021. Human Factors in Cybersecurity. *Security science journal*, 2(2), pp.51-64.

Tuorinsky, Edward (2021), The human factor in cybersecurity, Overcome human nature with a “lock the door” mentality. Available from: https://www.securitymagazine.com/articles/96009-the-human-factor-in-cybersecurity [Accessed 23 March 2022]

Paul Formosa, Michael Wilson, Deborah Richards (2021), A principlist framework for cybersecurity ethics, Computers & Security, Volume 109, 102382, ISSN 0167-4048,

https://doi.org/10.1016/j.cose.2021.102382.

ISACA.org (2019), Figure 2 NIST Cybersecurity Lifecycle, Start with the Why: A Strategic Lifecycle for Information Security, Available from: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/start-with-the-why-a-strategic-lifecycle-for-information-security [Accessed 15 April 2022]

National Science and Technology Council, (2016). Networking and Information Technology Research and Development Program. Ensuring Prosperity and National Security. Available from: https://www.nitrd.gov/cybersecurity/publications/2016\_Federal\_Cybersecurity\_Research\_and\_Development\_Strategic\_Plan.pdf [Accessed 21 March 2022]

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., et al. (2021) Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work. [Online] Available from: doi:10.1007/s10111-021-00683-y.