ASMIS Cyber Security Socio-technical assessment (transcript)

Securing Information: Human Context

The technical software security requirements for the *appointment scheduling management information system* project, hereafter referred to as (ASMIS) have been implemented. The purpose of this assessment was identifying potential cyber security impacts related to people interacting with the ASMIS application and recommend solutions to the human factor issues identified.

(Kerckhoffs, 1883) published a cryptographic principle to deal with human tendencies and limitations that can impact the security of information processed by a technical system.

Restated as design principles in the 1970s, (Saltzer & Schroeder, 1975), (Sasse & Rashid, 2019) have summarized this concept as useable security, I.E., 'security measures cannot be effective if humans are neither willing nor able to use them"

Website vs. Web Based Application

(ASMIS is not a general-purpose website it is an extension of Queens medical clinic operations. Patients, staff and clinicians must interact with the application using a two-dimensional web browser instead of telephone conversations and existing internal proceedures.

Internet self-service can reduce costs and provide benefits like appointment booking for patients at times that best suit them, reduce staff performing rote appointment data entry work (Relatient, n.d.) and reducing the number of missed appointments (Marhefka, 2020, Zhao et al, 2017).

A significant limitation of web applications is the replacement of human-to-human interaction with a two-dimensional interface into a computer program.

Essentially the ASMIS application accepts input from users, interprets the data and provides a response, within the limits of its programing.

Unlike booking an appointment directly with a clinic staff member, a patient has little recourse if they did not understand something in the computer program response. In a human-to-human conversation this clarification activity is typically seamless.

Socio-Technical Considerations

Figure 1 and the following quotation, (Leeds University Business School, 2021), summarize the multiple points of interaction that take place between a computerized device, applications or systems and the people involved.

High Impact Human Factors

The assessment identified the following items as most likely to potential impact cyber security.

The term cognitive load or overload refers to the limitations of human working memory and attention capacity (Johnson 2021, Hartson and Pyla 2012)

In addition to dealing with human limitations and application information flow, there are social engineering implications related to ASMIS, some of which are exacerbated with mobile device usage. (Siadati et al, 2017; Sasse & Rashid, 2019)

There are also mental model considerations pertaining to the organization that will also need to be addressed.

Social Engineering

Online services tracking technology is used to access applications are reporting mobile device usage is now roughly equal to desktop usage at close to 50%, (Petrov, 2021), and the average adult spends 3 to 4 hours a day with their phone.

This segment size and demographic is too large to ignore yet the mobile device small form factor and use of short messaging service, AKA SMS presents additional cyber security challenges.

SMS based phishing attacks continue to be prevalent because of massive daily internet access using mobile devices and the ease with which attackers can create look-alike websites and send fake SMS messages (Social Engineer, 2020)

Users also struggle to distinguish spoofed SMS phishing messages from legitimate communication (Siadata et al, 2017)

Therefore, it is recommended Queens create user awareness training for their patients, ideally something like an online video or screencast rather than a lengthy statement on a website.

Ensure patients understand when Queens would contact them electronically, how that would be done and messages they can safely ignore.

Finally, ensure patients have a way to determine Queens messages are authentic such as including a masked version of the patient's National Health Services number since this data would not be known to attackers but easily identified by the user.

Productivity Implications

ASMIS application design and installation are complete, so it is too late to address any design related issues (example figure 3) without rewriting portions of the program (Johnson, 2021). Therefore, these human factors will need to be monitored and addressed through alternative means until design improvements are justified and completed.

It is understood that Queens staff and clinicians will be required to perform additional tasks within ASMIS instead of Queens' existing systems. It should also be recognized that internal users will have varying computer skill levels, (Nielsen, 2016).

Those that struggle with the new system are likely to experience stress until they become more proficient. Unfortunately, percieved stress quickly affects the brain's executive function abilities such as amount of working memory, ability to pay attention and make correct decisions (Wu et al, 2019)

Computer Skills Distribution

The Nielsen Norman group 2016 global study confirms Queens can expect only a portion of their internal staff to have medium to strong computer skills (Nielsen 2016; Figure4).

Additionally, only 50% of patients will have basic computer skills. The only recommended resolution is to limit the number of steps a person must perform before they can close a task (Hartson & Pyla, 2012) which may be a design limitation in some cases.

Behavioural Modification Strategy

Over a hundred years after Kerckhoffs stated "security should not put undue tension on the user's mind", BJ Fogg articulates the reality that most people are generally resistant to extensive training requirements. (Fogg, 2009)

Within the ASMIS context, the Fogg simplicity factors that will best assist users are:

- reducing the time it takes to complete a task and
- how much they have to think about while performing the task (figure 5).

(Hartson & Pyla 2018) provide user interface design recommendations to reduce the amount of training required. While Queens may not be able to make extensive design updates for some time to come, the recommended mitigation monitoring for user errors or failing to comply to security requirements and create quick reference guides or (QRGS).

A lengthy user manual is unlikely to be read beyond the first few pages but a QRG enabling the user to recognize the problem and solution in a single page visual document is much more aligned with how humans learn.

Organizational changes:

People often make decisions based their mental model of how a system works. (Kang et al, 2015) identified a very wide range of mental models associated with the internet and online applications. (Table 1).

Currently, patients encountering difficulties using ASMIS are likely to contact Queens via telephone with questions since they are already in the habit of calling for appointment services.

Front-line clinic staff may be providing technical support to help patients and other staff, potentially without the proper understanding of the problem (Kang et al, 2015), and disseminating misinformation to patients and clinicians who are used to engaging staff for administrative support.

As a solution, the ASMIS technical team can develop quick reference guides for common problems. The front-line admin staff could use the QRGs to answer inquiries once they have been reviewed by less technical internal staff and tested for effectiveness. (Wong-Parodi & Bruine du Bruin, 2017)

Organizational Priorities:

Medical practices are often extremely busy and prioritize patient care. One plausible outcome of a production focus is the willingness to bypass time consuming controls because workers perceive, correctly or incorrectly, that management prioritizes task completion over security (McEvoy & Kowalski, 2019).

Revisiting cognitive load and executive function concepts, procedural steps or warnings are also more likely to be ignored when a staff member or clinician is feeling stressed due to immediate workload. (Wu et al, 2019).

It should be acknowledged that the need for patient information confidentiality is typically well understood within the medical community (Erickson & Millar, 2005; Veloski et al, 2005). Consequently, ASMIS control errors may not be a security awareness issue but the result of forgetting, making a mistake, incorrect mental models or lack of training.

Queens management can support their staff and clinicians through this transition period using communication and observable actions.

Clarify the importance of cyber security within the clinic, how it is now just another aspect of patient centered care (Fix et al, 2018).

Remove a source of high stress, assure people that sharing their struggles learning the new system will not result in job termination.

Security culture, when properly approached, can benefit the entire organization. (Walsh, 2017). Queens management can encourage reporting system interaction issues, identification of solutions and prioritize development of support for internal staff. Essentially sending the message that support is available and complying with ASMIS security controls is also expected.

Conclusions:

In summary the key points of this assessment and presentation are:

Human factors can affect an organization’s cyber security as much as technology choices, (Sasse & Rashid, 2019).

85% of the data breachs reported in 2020 include some human factor or involvement, this is an area that should not be ignored (Verizon, 2021)

Design flaws that fail to account for human limitations appear to be at least partially responsible (Johnson, 2021)

Finally. a strong security culture starts as a top management initiative (Walsh 2017) and fostering security champions in the organization sustains it (Huisman & Horvath 2017)

References

Erickson, J. & Millar, s. (2005) Caring for Patients While Respecting Their Privacy: Renewing Our Commitment. *The Online Journal of Issues in Nursing* 10(2): Man1. DOI: 10.3912/OJIN.Vol10No02Man01 Available from: http://ojin.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Volume102005/No2May05/tpc27_116017.aspx [Accessed 30 October 2021]

Fix, G. M. et al. (2018) Patient-centred care is a way of doing things: How healthcare employees conceptualize patient-centred care. *Health expectations : an international journal of public participation in health care and health policy* 21(1): 300-307. DOI:https://doi.org/10.1111/hex.12615

Fogg, BJ. (2009) A Behavior Model for Persuasive Design, *Persuasive '09: Proceedings of the 4th International Conference on Persuasive Technology.* Claremont California, USA 26-29 April 2009. Claremont. 1-7 DOI: https://doi.org/10.1145/1541948.1541999

Huisman, Joanna. & Horvath, M. (2017) Designing a Security Champion Program. Available from: https://www.gartner.com/en/documents/3746118/designing-a-security-champion-program [Accessed 30 October 2021]

Hartson, R. & Pyla, P. (2012) The UX Book Process and Guidelines for Ensuring a Quality User Experience 1st Edition, Waltham MA Morgan Kaufmann

Hartson, R. & Pyla, P. (2019) The UX Book Agile UX Design for a Quality User Experience 2nd Edition, Cambridge MA Morgan Kaufmann

Johnson, J. (2021) *Desiging with the Mind in Mind.* 3rd ed. Cambridge: Morgan Kaufmann.

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 (SOUPS)* . Ottawa, Canada 22-24 July 2015. Ottawa. 39-52.

Kerckhoffs, A. (1873) La cryptograpie militaire. Journal des sciences militaires, 9:5-38. Available from: https://www.petitcolas.net/kerckhoffs/la_cryptographie_militaire_i.htm [Accessed 30 October 2021]

Leeds University Business School. (2021) Socio-technical systems theory. Available from: https://business.leeds.ac.uk/research-stc/doc/socio-technical-systems-theory [Accessed 2 October 2021].

Marhefka, K. M. (2020) The Impact of Digital Self-Scheduling on No-Show Event Rates in Outpatient Clinics. Doctoral thesis, Walden University.

McEvoy, T. R. & Kowalski, S. J. (2019) Deriving Cyber Security Risks from Human and Organizational Factors - A Socio-tecchnical Approach. *Complex Systems Informatics and Modeling Quartely,* 3(18): 47-64. Avaliable from: https://scholar.google.ca/scholar?q=complex+systems+informatics+and+modeling+quarterly+mcevoy+pdf&hl=en&as_sdt=0&as_vis=1&oi=scholart [Accessed 29 September 2021]

Nielsen, J. (2016) The Distribution of User's Computer Skills: Worse Than You Think. Available from: https://www.nngroup.com/articles/computer-skill-levels/ [Accessed 24 October 2021]

Petrov, C. (2021) 51 Mobile vs. Desktop usage Statistics for 2021. Available from: https://techjury.net/blog/mobile-vs-desktop-usage [Accessed 29 October 2021]

Relatient. (n.d.) Why Patient Self-Scheduling: Healthcare Trends & Getting Started. Available from: https://www2.relatient.net/resources/why-patient-self-scheduling-healthcare-trends-getting-started/ [Accessed 30 June 2021]

Saltzer, J. & Schroeder, M (1975) The Protection of Information in Computer Systems, *Proceedings of the IEEE 63-9.* September 1975

Sasse, M. A. & Rashid, A. (2019) Human Factors Issue. The Cyber Security Body Of Knowledge (1) Available from: https://www.cybox.org/media/downloads/Human_Factors_issue_1.0.pdf

Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M. & Memon, N. (2017) Mind your SMSes: Mitigating social engineering in second factor authentication, *Computers & Security* 65: 14-28. DOI: https://doi.org/10.1016/j.cose.2016.09.009

Social Engineer. (2020) SMishing – Is It Really A Threat? Avaliable from: https://www.social-engineer.com/smishing-is-it-really-a-threat/ [Accessed 28 Oct 2021]

Statcounter. (2021) StatCounter Gobal Stats Available from: https://gs.statcounter.com/platform-market-share/desktop-mobile/europe#yearly-2011-2021 [Accessed 29 Oct 2021]

Verizon. (2021) DBIR 2021 Databreach Invetigations Report. Available from: https://www.verizon.com/business/resources/reports/dbir [Accessed 12 June 2021].

Veloski, J., Fields, S., Boex, J. & Blank, L. (2005) Measuring Professionalism: A Review of Studies with Instruments Reported in the Literature between 1982 and 2002, *Academic Medicine* 80(4): 366-370. Available from: https://journals.lww.com/academicmedicine/Fulltext/2005/04000/Measuring_Professionalism__A_Review_of_Studies.14.aspx [Accessed 30 October 2021]

Walsh, E. (2017) How to Develop a Security Culture. Available from: https://georgian.io/develop-a-security-culture/ [Accessed 30 October 2021]

Wong-Parodi, G. & Bruine de Bruin, W. (2017) Informing public perceptions about climate change: A ‘mental models’ approach. *Science and Engineering Ethics* 23(5): 1369-1386.

Wu, J., Feng, M., Liu, Y., Fang, H. & Duan, H. (2019) The Relationship between chronic percieved stress and error processing: evidence from event-related potentials. *Scientific Reports Nature Research* 9: 11605 DOI: https://dx.doi.org/10.1038%2Fs41598-019-48179-0

Zhao, P., Yoo, I., Lavoie, J., Lavoie, B. J. & Simoes, E. (2017) Web-Based Medical Appointment Systems: A Systematic Review. *Journal of Medical Internet Research* 19(4): e134. DOI: https://doi.org/10.2196/jmir.6747