ASMIS Cyber Security

SOCIO-TECHNICAL ASSESSMENT

Securing Information: Human Context

- "Human Factors", an evolving area of research, 100+ year back story
- Secure Communication System:
  - "… the system be easy to use, requiring neither tension of mind, nor knowledge of a long series of rules to be observed" (Kerckhoffs, 1883)

Securing Information: Human Context

- "Human Factors", an evolving area of research, 100+ year back story
- Secure Communication System:
  - "… the system be easy to use, requiring neither tension of mind, nor knowledge of a long series of rules to be observed" (Kerckhoffs, 1883)
- Design Principles:
  - Psychologically acceptable, fewest security mechanisms possible, attacker's effort must exceed reward (Saltzer & Schroeder, 1975)
- "Useable Security:
  - "security measures cannot be effective if humans are neither willing nor able to use them" (Sasse & Rashid, 2019)

Website vs. Web Based Application

- Existing Business functions abstracted into computer code

Website vs. Web Based Application

- Existing Business functions abstracted into computer code
- Benefits:
  - 7X24 patient access
  - Reduced staff effort on potentially rote booking tasks (Relatient, n.d.)
  - Reduced no-show rates (Marhefka, 2020; Zhao et al., 2017).

Website vs. Web Based Application

- Existing Business functions abstracted into computer code
- Benefits:
  - 7X24 patient access
  - Reduced staff effort on potentially rote booking tasks (Relatient, n.d.)
  - Reduced no-show rates (Marhefka, 2020; Zhao et al., 2017).
- Limitations:
  - Two-dimensional interface, (web browser on computer or mobile)

Website vs. Web Based Application

- Existing Business functions abstracted into computer code
- Benefits:
  - 7X24 patient access
  - Reduced staff effort on potentially rote booking tasks (Relatient, n.d.)
  - Reduced no-show rates (Marhefka, 2020; Zhao et al., 2017).
- Limitations:
  - Two-dimensional interface, (web browser on computer or mobile)
  - Predefined responses to data input

Website vs. Web Based Application

- Existing Business functions abstracted into computer code
- Benefits:
  - 7X24 patient access
  - Reduced staff effort on potentially rote booking tasks (Relatient, n.d.)
  - Reduced no-show rates (Marhefka, 2020; Zhao et al., 2017).
- Limitations:
  - Two-dimensional interface (web browser on computer or mobile)
  - Predefined responses to data input
  - Minimal user recourse when required steps not understood

Socio-Technical Considerations

- *"Organisational change programmes often fail because they are too focused on one aspect of the system, commonly technology, and fail to analyse and understand the complex interdependencies that exist."* (Leeds University Business School, 2021)

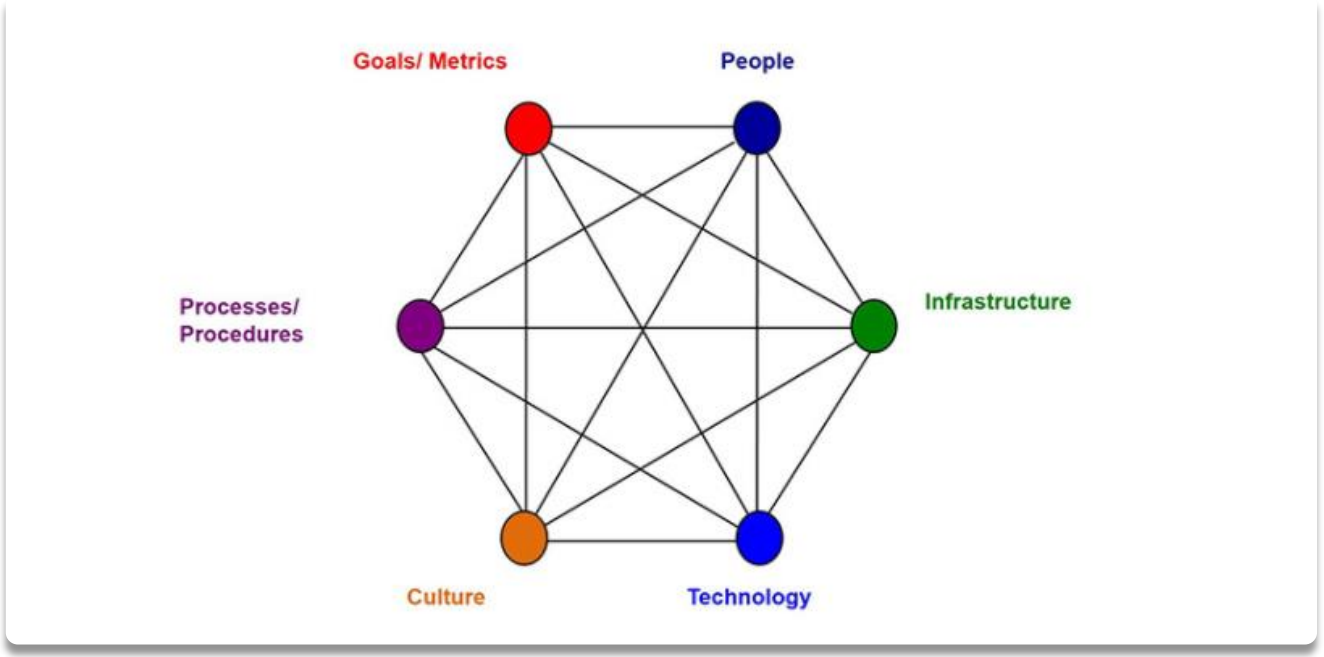

Fig 1 Interdependency elements (Leeds University Business School, 2021)

High Impact Human Factors

- Cognitive Load/Overload
  - Social engineering implications (Siadati et al, 2017; Sasse & Rashid, 2019)
  - Productivity implications (Johnson, 2021; Hartson & Pyla, 2012)

High Impact Human Factors

- Cognitive Load/Overload
  - Social engineering implications (Siadati et al, 2017; Sasse & Rashid, 2019)
  - Productivity implications (Johnson, 2021; Hartson & Pyla, 2012)
- Organizational Changes:
  - User support
  - Knowledge management (Kang et al, 2015)
- Organizational Security Culture:
  - Assumptions & misconceptions (McEvoy & Kowalski, 2019)

Social Engineering

- Mobile usage ~50% (Petrov, 2021)
- Usage 4 hours daily (Petrov 2021)

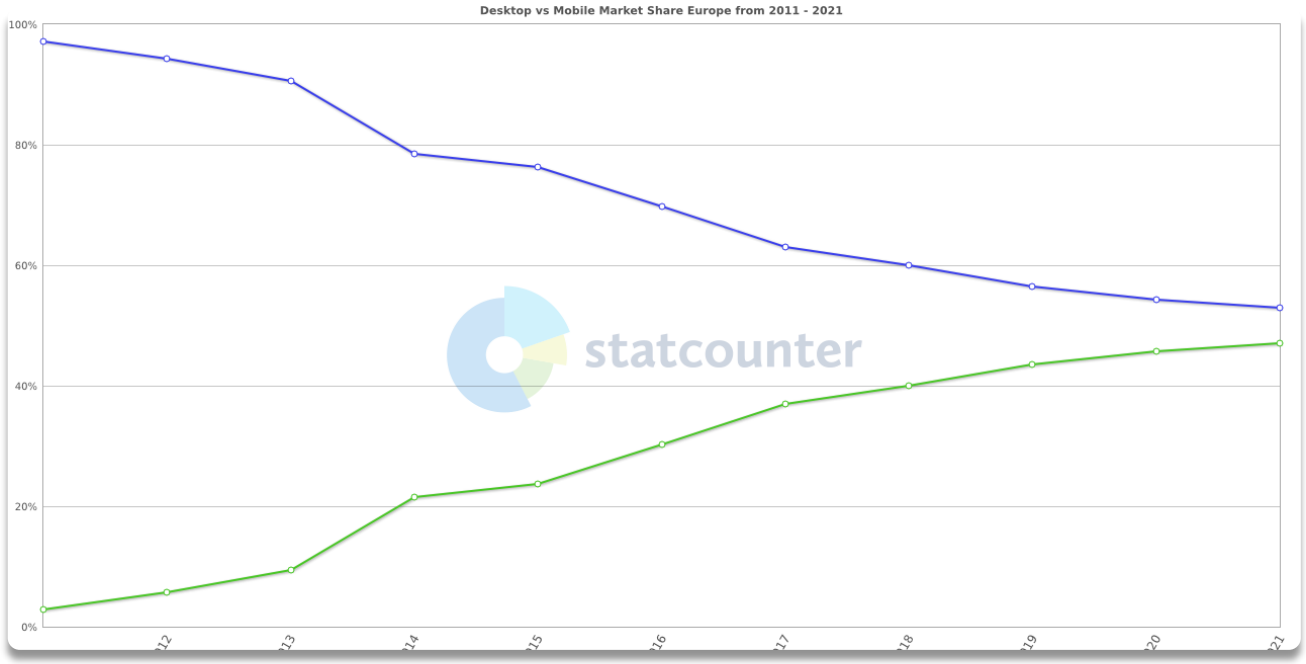

Fig 2 Mobile vs Desktop Usage (Statcounter, 2021)

Social Engineering

- Mobile usage ~50% (Petrov, 2021)
- Usage 4 hours daily (Petrov 2021)
- Segment should not be ignored
- Form factor & medium present additional human factor challenges

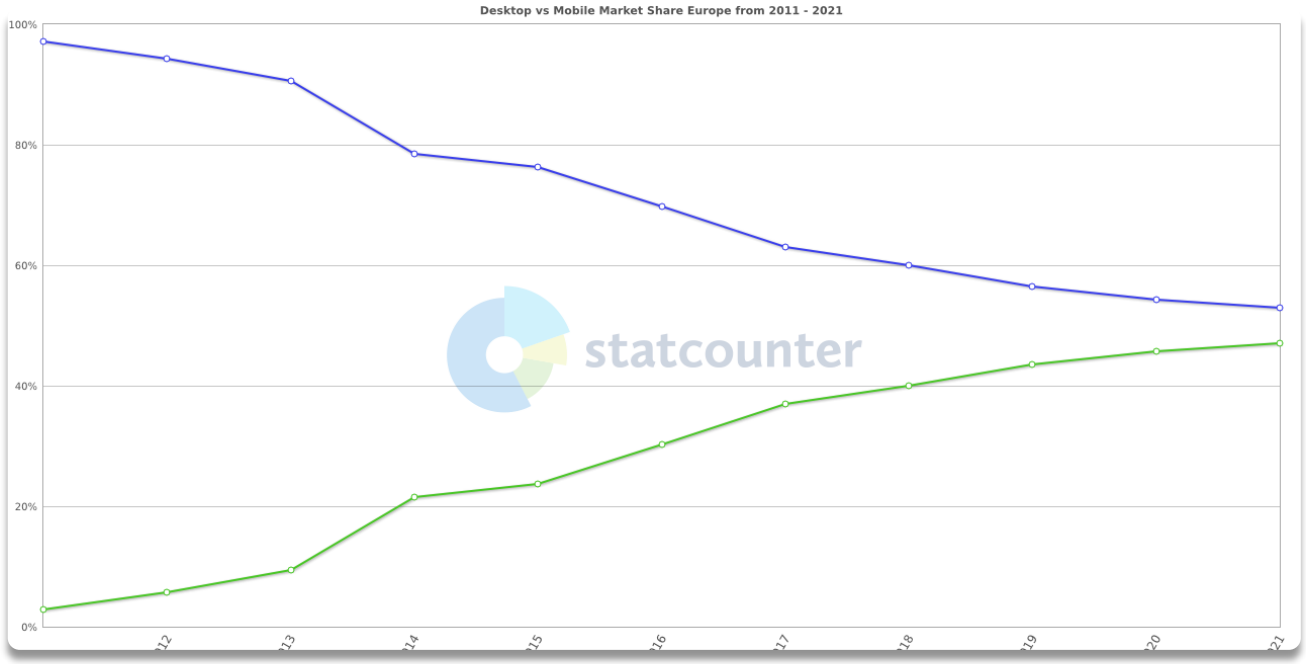

Fig 2 Mobile vs Desktop Usage (Statcounter, 2021)

Social Engineering

- SMishing
  - Text messages leading to cloned sites (Social Engineer, 2020)
  - SMS attack identification potentially difficult (Siadati et al, 2017)

Social Engineering

- SMishing
  - Text messages leading to cloned sites (Social Engineer, 2020)
  - SMS attack identification potentially difficult (Siadati et al, 2017)
- Queens can create short public awareness information video
  - Contact Criteria, and methods
  - Clarify safe to ignore (E.G., “account security alert”)

Social Engineering

- SMishing
  - Text messages leading to cloned sites (Social Engineer, 2020)
  - SMS attack identification potentially difficult (Siadati et al, 2017)
- Queens can create short public awareness information video
  - Contact Criteria, and methods
  - Clarify safe to ignore (E.G., “account security alert”)
- Verification guidance
  - Include 10-digit NHS number with middle six digits masked

Productivity Implications

- Ideally addressed in design
  - Missed warnings due focus (Johnson, 2021)
  - Human error due to task complexity (Hartson & Pyla, 2012)

Fig 3 Status alert outside field of view (Johnson, 2021)

Productivity Implications

- Ideally addressed in design
  - Missed warnings due focus (Johnson, 2021)
  - Human error due to task complexity (Hartson & Pyla, 2012)
- Uneven skills distribution (Nielsen, 2016)

Fig 3 Status alert outside field of view (Johnson, 2021)

Productivity Implications

- Ideally addressed in design
  - Missed warnings due focus (Johnson, 2021)
  - Human error due to task complexity (Hartson & Pyla, 2012)
- Uneven skills distribution (Nielsen, 2016)
  - Potential stressor
  - Executive brain function impact (Wu et al, 2019)
    - Working memory & attention
    - Quick decisions & task completion

Fig 3 Status alert outside field of view (Johnson, 2021)

Computer Skills Distribution

- Extensive global study (Nielsen, 2016)
- Internal staff, clinicians level 1 or 2
  - 35% change level 2 or higher

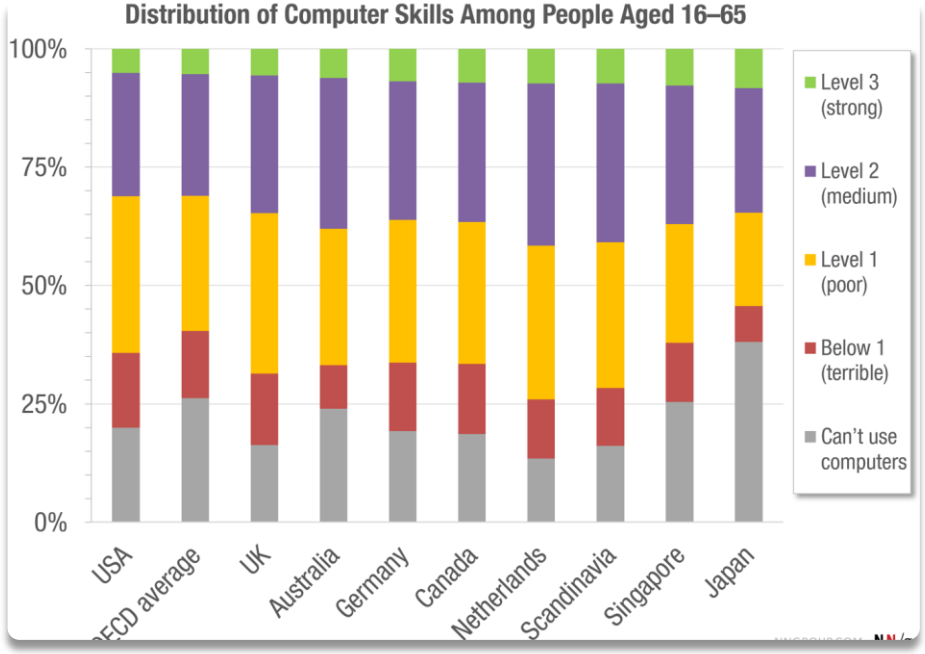

Fig 4 Computer skills distribution (Nielsen, 2016)

Computer Skills Distribution

- Extensive global study (Nielsen, 2016)
- Internal staff, clinicians level 1 or 2
  - 35% change level 2 or higher
- Patients: 50% basic task only
  - Limit navigation & steps
  - Explicit choices and criteria
  - Simplified tasks (Hartson & Pyla, 2012)

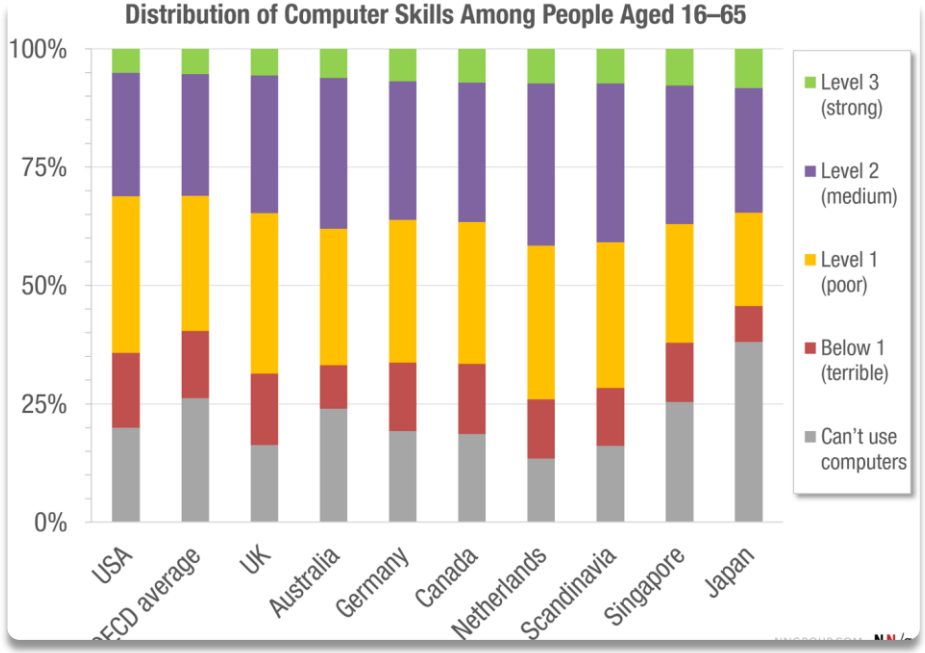

Fig 4 Computer skills distribution (Nielsen, 2016)

Behavioural Modification Strategy

- "***People are generally resistant to teaching and training because it requires effort***" (Fogg 2009)
  - Reduce time & thought needed (Fig. 5)

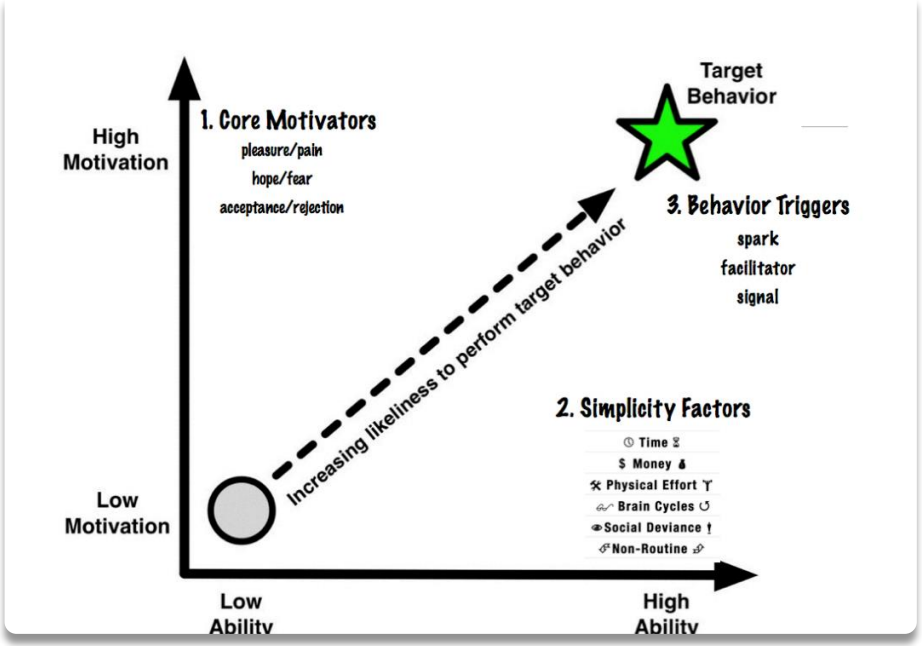

Fig 5 FBM model & factor framework(Fogg 2009)

Behavioural Modification Strategy

- "***People are generally resistant to teaching and training because it requires effort***" (Fogg 2009)
  - Reduce time & thought needed (Fig. 5)
- User centered design (Hartson & Pyla 2019)
  - Prefilled/retained data,
  - Clickable choices vs data entry
  - Prompts for infrequent tasks
- Quick reference guides (QRG)
  - Single page per task
  - Visual cues, few words

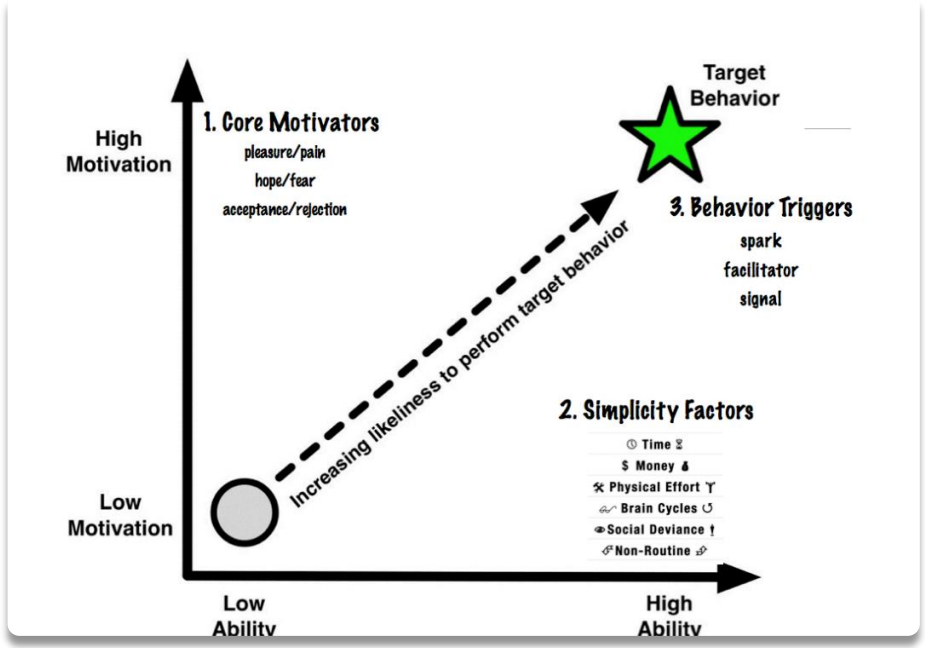

Fig 5 FBM model & factor framework(Fogg 2009)

Organizational Changes

- 2015 study shows wide technical understanding variation (Kang et al, 2015)
- Admin staff inherit user support role

	Description of the models
Simple and service-oriented models: 13 lay participants; 1 technical participant	Represent the Internet as a vague concept or a service; Only show awareness of organizations or services they directly interact with; Lack awareness of underlying layers, structures and connections; Use inconsistent or made-up terminologies.
Articulated technical models: 4 lay participants; 10 technical participants	Represent the Internet as a complex, multi-level system; Show broader awareness of components and organizations in the network; Express awareness of layers, structures and connections; Use accurate, detailed, consistent terms.

Table 1 Internet mental models among test subjects (Kang et al, 2015)

Organizational Changes

- 2015 study shows wide technical understanding variation (Kang et al, 2015)
- Admin staff inherit user support role
  - Inconsistent guidance (Kang et al, 2015)
  - Patients & clinicians typically rely on admin staff "expertise"

	Description of the models
Simple and service-oriented models: 13 lay participants; 1 technical participant	Represent the Internet as a vague concept or a service; Only show awareness of organizations or services they directly interact with; Lack awareness of underlying layers, structures and connections; Use inconsistent or made-up terminologies.
Articulated technical models: 4 lay participants; 10 technical participants	Represent the Internet as a complex, multi-level system; Show broader awareness of components and organizations in the network; Express awareness of layers, structures and connections; Use accurate, detailed, consistent terms.

Table 1 Internet mental models among test subjects (Kang et al, 2015)

Organizational Changes

- 2015 study shows wide technical understanding variation (Kang et al, 2015)
- Admin staff inherit user support role
  - Inconsistent guidance (Kang et al, 2015)
  - Patients & clinicians typically rely on admin staff "expertise"
- Tech teams build user support QRGs
- Test effectiveness with lay focus group (Wong-Parodi & Bruine de Bruin, 2017)

	Description of the models
Simple and service-oriented models: 13 lay participants; 1 technical participant	Represent the Internet as a vague concept or a service; Only show awareness of organizations or services they directly interact with; Lack awareness of underlying layers, structures and connections; Use inconsistent or made-up terminologies.
Articulated technical models: 4 lay participants; 10 technical participants	Represent the Internet as a complex, multi-level system; Show broader awareness of components and organizations in the network; Express awareness of layers, structures and connections; Use accurate, detailed, consistent terms.

Table 1 Internet mental models among test subjects (Kang et al, 2015)

Organizational Priorities

- Security controls typically viewed as “tax on production” (McEvoy & Kowalski, 2019)

Organizational Priorities

- Security controls typically viewed as "tax on production" (McEvoy & Kowalski, 2019)
- Bypass attempts and mistakes not necessarily an indicator of a cybersecurity resistant culture (Wu et al, 2019)
- Patient care and safety priority understood across the industry (Erickson & Millar, 2005; Veloski et al, 2005)

Organizational Priorities

- Security controls typically viewed as "tax on production" (McEvoy & Kowalski, 2019)
- Bypass attempts and mistakes not necessarily an indicator of a cybersecurity resistant culture (Wu et al, 2019)
- Patient care and safety priority understood across the industry (Erickson & Millar, 2005; Veloski et al, 2005)
- Recommended resolution: Management communication & action plan
  - Articulate cyber security is just another aspect of patient care (Fix et al, 2018)
  - Acknowledge transition efforts and assure livelihoods not in jeopardy
  - Promote a security culture (Walsh, 2017) and QRG support development

Conclusions

- Cyber Security extends beyond technological controls (Sasse & Rashid 2019)
- Human factors were involved in 85% of data breaches (Verizon, 2021)
- Human error is often the result of design mistakes (Johnson, 2021)
- A strong security culture starts with management leadership (Walsh, 2017)
- Security champion can nurture culture day to day (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

References

- 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]

References

- 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

References

- 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]

References

- 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