I. SLIDES 1-3 INTRODUCTION

A. Key priorities from Unit 3

1. Human factors (3):
   - i) Social engineering – Pretexting / Phishing
   - ii) Insider threat – Opportunities / Disgruntled employees
   - iii) Human error – Accidental / Limited human capabilities / Ignorance / Usability

B. Scope of solutions

2. Education and training
3. Organisational culture / Workplace environment
4. Usability in ASMIS software development

II. SLIDES 4-9 BODY

Examination identifying the strengths of each strategic solution and identifying the challenges/limitations of the potential solution.

A. Education and training

Solutions:	Challenges:
1. Social Engineering: Phishing simulations/ Game tools Targeted approach increases security compliance (Alotaibi et al., 2016) 2. Insider malicious threat: Artificial Intelligence (Nebeker et al., 2019) Motivation, social bonds and opportunity reduction strategies (Safa et al., 2018) 3. Human error: Improve skills and training (McIlwraith, 2021) Training improves intellectual capacity (He et al., 2020) Risk management models (Chua et al., 2019) Blockchain technology to flag errors (Tahir et al., 2020) COM-B model (Mayne, 2018) / B-MAT Model (Fogg, 2019)	Gamification has potential but limitations to formal context (Le Compte A. et al., 2015) Training scenarios must be incorporated to be effective (Adams and Makramalla, 2015) More vetting is needed on digital health technologies (Nebeker et al., 2019) ENISA report (ENISA, 2018) suggests training is not essential, but the work environment Behaviours are challenging to change, so other persuasive methods are needed (Zhang-Kennedy et al., 2014)

B. Organisation culture / Workplace environment

Solutions:	Challenges:
1. Security culture evaluation for organisational readiness (Georgiadou et al., 2020) 2. Security is everyone's responsibility (link to Mental Model Metaphors (Chen, 2020) - Public Health, Crime etc.) / Security culture programme / Employ mental models for risk communication (Boase et al., 2017) 3. A bottom-up approach to security policy could be more inclusive (McIlwraith, 2021) or	Top-down management can be more effective (Neumann et al., 2021)

hybrid to find security champions (Becker et al., 2017) 4. Less stress environments / Workload management / Employee benefits (Private healthcare/holidays/CPD/Scheduled breaks/Focus groups/Surveys/Awards/Linked to KPIs (Parsons et al., 2015) 5. ENISA (ENISA, 2018) Framework - not in awareness and training but in supporting domains that strongly influence the work environment of the individuals. 6. COM-B model (Mayne, 2018) / Organisation transparency to errors/breaches	Rewards or punishments in line with the company's security goals are only effective with suitable leadership styles (transactional leadership) (Guhr et al., 2019)

C. Usability in ASMIS development

Solutions:	Challenges:
1. Secure by default (National Cyber Security Centre, 2018) 2. Incorporating stakeholders with developers in the design process 3. Agile frameworks and roadmaps (Rosenzweig, 2015)	Resources and knowledge available. Experience in security incidents. Stakeholder pressure and company cultures (Assal and Chiasson, 2018) Limited research in usability and user experience at present (Bitkina et al., 2020)

D. Social and ethical considerations of developing and applying usable security

Solutions:	Challenges:
1. GDPR (Intersoft Consulting, N.D.) 2. User experience with disabilities (Hartson and Pyla, 2018) 3. Users needed for testing – Menlo report (Bailey et al., 2012) (Respect, Benefits and no harm, Justice, Respect for law and public interest)	Developers do not have enough formal ethics education in training (Nebeker et al., 2019) Patients over-reliance on technology rather than seeing healthcare providers (Nebeker et al., 2019)

III. SLIDE 10 CONCLUSION

A. Well-reasoned judgement concluding the suggested most effective solution from the discussion.

IV. SLIDE 11 REFERENCES

Adams, M. & Makramalla, M. 2015. Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review,* 5.

Alotaibi, M., Furnell, S. & Clarke, N. Information security policies: A review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 5-7 Dec. 2016 2016. 352-358.

Assal, H. & Chiasson, S. Security in the software development lifecycle. Fourteenth symposium on usable privacy and security (SOUPS 2018), 2018. 281-296.

Bailey, M., Dittrich, D., Kenneally, E. & Maughan, D. 2012. The Menlo Report. *IEEE Security & Privacy,* 10**,** 71-75.

Becker, I., Parkin, S. & Sasse, M. A. 2017. Finding security champions in blends of organisational culture. *Proc. USEC,* 11.

Bitkina, O. V., Kim, H. K. & Park, J. 2020. Usability and user experience of medical devices: An overview of the current state, analysis methodologies, and future challenges. *International Journal of Industrial Ergonomics,* 76**,** 102932.

Boase, N., White, M., Gaze, W. & Redshaw, C. 2017. Evaluating the Mental Models Approach to Developing a Risk Communication: A Scoping Review of the Evidence: Evaluating the Mental Models Approach. *Risk Analysis,* 37.

Chen, J. 2020. Risk communication in cyberspace: a brief review of the information-processing and mental models approaches. *Current Opinion in Psychology,* 36**,** 135-140.

Chua, Y. T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G. & Hutchings, A. Identifying Unintended Harms of Cybersecurity Countermeasures. 2019 APWG Symposium on Electronic Crime Research (eCrime), 13-15 Nov. 2019 2019. 1-15.

Enisa. 2018. *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity* [Online]. Available: 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 13 July 2022].

Fogg, B. 2019. Fogg behavior model. *Behav. Des. Lab., Stanford Univ., Stanford, CA, USA, Tech. Rep*.

Georgiadou, A., Mouzakitis, S., Bounas, K. & Askounis, D. 2020. A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems***,** 1-11.

Guhr, N., Lebek, B. & Breitner, M. H. 2019. The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal,* 29**,** 340-362.

Hartson, R. & Pyla, P. S. 2018. *The UX book: Agile UX design for a quality user experience*, Morgan Kaufmann.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L. & Tian, X. 2020. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital,* 21**,** 203-213.

Intersoft Consulting. N.D. . *GDPR* [Online]. Available: https://gdpr-info.eu/ [Accessed 22 January 2022].

Le Compte A., Elizondo D. & T., W. A renewed approach to serious games for cyber security. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 26-29 May 2015 2015. 203-216.

Mayne, J. 2018. The COM-B theory of change model. *unpublished www.researchgate. net/publication/314086441_The_COM-B_Theory_of_Change_Model_V3 (accessed July 22, 2019)*.

Mcilwraith, A. 2021. *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*, Routledge.

National Cyber Security Centre. 2018. *Secure by Default* [Online]. Available: https://www.ncsc.gov.uk/information/secure-default [Accessed 13 July 2022].

Nebeker, C., Torous, J. & Bartlett Ellis, R. 2019. Building the case for actionable ethics in digital health research supported by artificial intelligence. *BMC Medicine,* 17.

Neumann, W. P., Winkelhaus, S., Grosse, E. H. & Glock, C. H. 2021. Industry 4.0 and the human factor–A systems framework and analysis methodology for successful development. *International journal of production economics,* 233**,** 107992.

Parsons, K. M., Young, E., Butavicius, M. A., Mccormac, A., Pattinson, M. R. & Jerram, C. 2015. The influence of organisational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making,* 9**,** 117-129.

Rosenzweig, E. 2015. *Successful user experience: Strategies and roadmaps*, Morgan Kaufmann.

Safa, N. S., Maple, C., Watson, T. & Von Solms, R. 2018. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications,* 40**,** 247-257.

Tahir, M., Habaebi, M. H., Dabbagh, M., Mughees, A., Ahad, A. & Ahmed, K. I. 2020. A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities. *IEEE Access,* 8**,** 115876-115904.

Zhang-Kennedy, L., Chiasson, S. & Biddle, R. 2014. *Stop Clicking on "Update Later": Persuading Users They Need Up-to-Date Antivirus Protection*.

V. APPENDICES

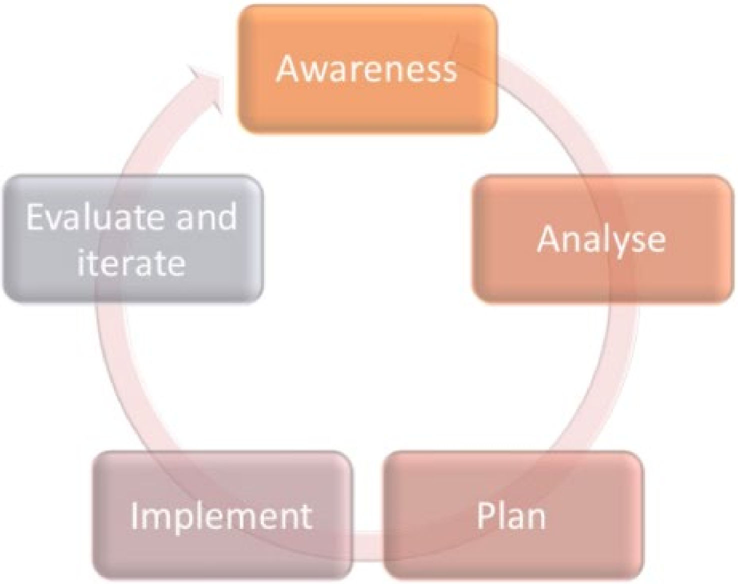

Figure 1: Framework for designing interventions for human aspects of cyber-security (ENISA, 2018)