Section 1: Research Proposal

Introduction

Despite the fact that security technology keeps evolving, human error is still the primary source of cybersecurity vulnerabilities and data breaches prevalent in organizations (Sawyer & Hancock, 2018). Recent research suggests that inadvertent insider actions constitute up to 90% of the reported cases, overcoming even enterprise-grade defenses (Grobler, Gaire & Nepal, 2021). Since the technical controls and safeguards become more robust, the attackers are mainly using human weakness, or better said, the human factor, as the easiest path for the system's entry. This accentuates an urgent requirement for the intensification of attention on the part of human-centric efforts founded in accessibility and user experience (UX) aptitudes to reinforce behavioral cybersecurity defenses. This proposal presents a systematic literature review to explore extant literature that examines the effectiveness of purposeful user-centered design within security awareness programs and training in increasing employees' security knowledge, attitudes, and compliance behavior to reduce insider threats.

Justification

The resilience of security breaches stemming from employee errors and neglect as opposed to purely technical ones illustrates a worrying loophole in organizational defenses (Maalem et al., 2020). This calls for going beyond passive technological controls and looking for proactive measures that will enhance staff cyber hygiene. Most of the data breaches (70%) result from deceived employees, such as phishing or machine-authorization mishaps (Hadlington, 2021). Such incidents can cause painful wounds for companies in terms of economic costs, reputational damage, and lost customer trust. Instead of overly strict compliance monitoring or limitations that degrade usability, it is constructive enabling and consciousness-raising programs developed organically according to users' needs and limitations, which is the ideal solution (Zimmermann & Renaud, 2019). This stresses the importance of studying human-focused security frameworks.

Research Question

How can organizations leverage user experience (UX))-centered design principles in crafting security awareness programs and protocols to improve employee cyber hygiene and reduce insider threat vulnerabilities?

Scope and Limitations

The review concentrates exclusively on the English language publications of scholarly articles, conference proceedings, and industry reports related to organizational security awareness initiatives between 2012 and 2022. It utilizes database searches across platforms like IEEE Xplore, ScienceDirect, ACM Digital Library, and Google Scholar using combinations of the terms "usable security," "cybersecurity," "awareness," "training," and "user experience." The scope of the research is also restricted to publications available on academic databases or open-access journals and excludes public domain media reports or analyses.

Key Literature

An initial search in the database for papers on "usable security," "security awareness," and "user-centered design" returned more than 600 results published since 2013. Having a preliminary review exercise enables the search parameters to be refined by isolating relevant sub-topics such as training evaluation, stage model of behavior, and design frameworks. Filtering of these outputs was performed to focus on the empirical studies or the systematic reviews with clear, meaningful findings. The short-listed papers in the final cluster of around 62 are majorly on organizational contexts.

Literature Synthesis Review

A thematic analysis of recent usable security literature conducted broadly reveals the importance of reconciling the inherent tensions of system security against usability in enterprise socio-technical systems primarily based on the user's capabilities and objectives (Münch et al., 2022). Experts favor regular awareness programs rooted in known instructional theories instead of independent training or scare methods (Jeong et al., 2019). Content customized to particular staff

roles, positive reinforcements for secure behaviors, and consistent assessments arise as critical design elements from evidence-based studies.

History and Background

Scholarly research on usable security emerged in the late 1990s due to the rapid mainstream penetration of personal computing and Internet access (Carroll, 2021). The initial studies considered prevention of the occurrence of incidents were centered on finding root causes and technical limitations aimed to stop possible users from exercises that would likely compromise the system's security. However, the recurrence of incidents related to human failures and unsafe practices has caused a fundamental philosophical change (AlGhamdi et al., 2020). There is better acceptance today of the fusion of psychological and ergonomic factors in the proactive design to promote security actions through user-experience-centered education, awareness, and guidance instruments mandatory to cognitive limitations and demands (Sawyer & Hancock, 2018).

New Research

In the last couple of years, innovative empirical investigations and case studies have confirmed that security education programs based on UX principles empower employees' cyber hygiene and have huge potential (Chalhoub et al., 2020). However, only a few of those detectable impacts are at the attitudinal or behavioral level, affecting different organizational environments. Moreover, applicable human-centered design pattern claims need to be included when it comes to systematically constructing awareness initiatives (Cuchta et al., 2019). Alternatively, so unfold the open issues around how programs factor various things such as skills gaps between user groups or sustainability in a constantly changing threat landscape.

Proposed Methodology

The study employs the Systematic Literature Review (SLR) methodology, which allows coverage of comprehensive repositories and databases such as IEEE Xplore, ScienceDirect, ACM Digital Library, and Google Scholar through combinations of "usable security," “cybersecurity,” “awareness,” “training,” and “user experience” (Paul et al., 2021).

The detailed search strategy ensures the retrieval of papers with data on security behavior or conceptual breadth, such as phishing resilience. The articles of interest are meticulously screened both for the relevance of the topic and also for the research quality based on the suggested metrics by Kitchenham et al. (2015). The filtered set of selected papers finally undergoes detailed scrutiny to single out frequently mentioned security awareness outcome behavioral antecedents and mediators. To consolidate the fragmented insights, textual analysis methods provide a means of finding repeated themes and constructs of interest (Morgan, 2022). These recurring elements are then systematically coded qualitatively to emerge with a User-Centered Security Awareness model.

Ethical Considerations

The current project adopts a content analysis of the existing literature that does not gather any primary data directly from the human participants. Consequently, it does not need formal ethical clearance, which is primarily obligatory for research studies involving human subjects. All cited references are previously published journal papers, conference outcomes, and reports. All the public domain sources are authentically cited and appropriately referenced in the APA style to avoid plagiarism and maintain academic honesty.

Artefact(s)

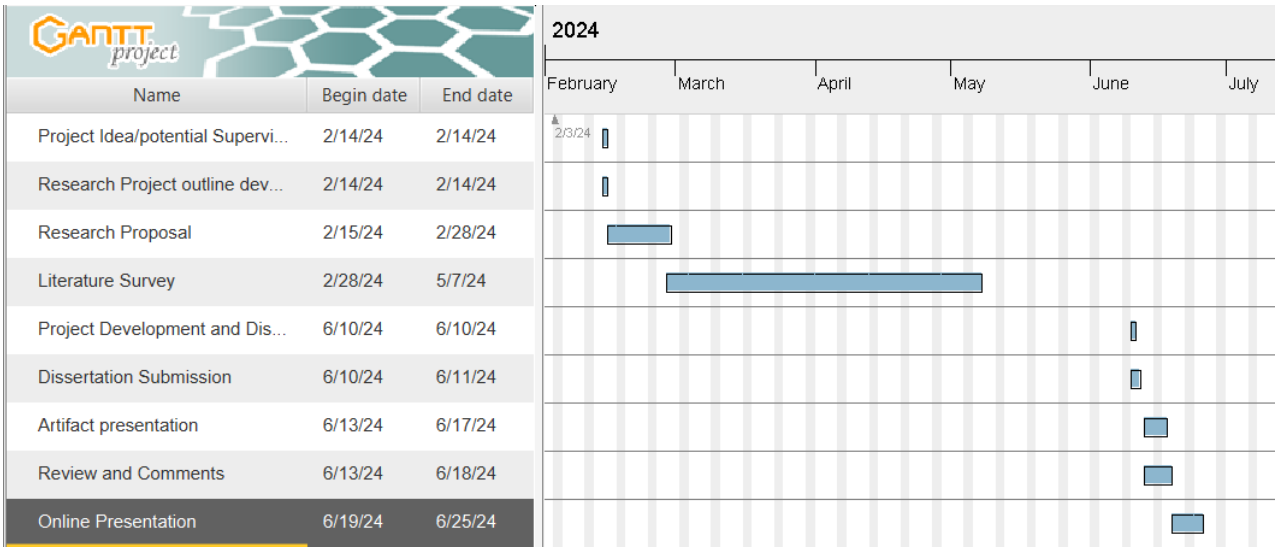
The artifact that will result from the systematic analysis is a conceptual model together with evidence-based guidelines for the development of user-focused security awareness campaigns based on behavioral change theories and instructional design principles intended for the cybersecurity field.

Timeline of Activities

Phase	**Tasks**	**Duration**
Preparation	Project Idea/potential Supervisor search	February 14, 2024

	Research Project outline development	
Research and Development	Research Proposal and Development	February 28, 2024
	Literature Survey	May 7, 2024
	Project Development and Dissertation Write-Up	June 9, 2024
Defense	Dissertation Submission	June 10, 2024
	Artifact presentation	June 13, 2024
	Review and Comments	June 17, 2024
	Online Presentation	June 24, 2024

Gannt Chart



Conclusion

This systematic review reveals from previous scholarly work that despite organizations spending large sums of money on enterprise security solutions, weaknesses persist because of human errors and unsafe cyber practices. The gaps between applicable security theories and formulated security interventions render such interventions not statistically nor practically verified as a means of long-term attitude or behavioral changes regarding security among employees. The proposed study is an effort to introduce a user-centric model of awareness for awareness-oriented initiatives toward closing the theory and practice gap for human-centered cybersecurity. Additional empirical tests could determine if principles from fields like

instructional design and a UX perspective could consolidate organizational cyber resilience.

References

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Almeida, F. (2018). Strategies to perform a mixed methods study. European Journal of Education Studies. http://dx.doi.org/10.5281/zenodo.1406214

Alohali, M. (2019). A Model for User-centric Information Security Risk Assessment and Response (Doctoral dissertation, University of Plymouth). https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/13698/2019alohali10479051phd.pdf?sequence=1

Alohali, M., Clarke, N., & Furnell, S. (2018). The design and evaluation of a user-centric information security risk assessment and response framework. https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/17952/Paper_18-The_Design_and_Evaluation_of_a_User_Centric_Information.pdf?sequence=1&isAllowed=y

Carroll, F. (2021, October). Usable Security and Aesthetics: Designing for engaging online security warnings and cautions to optimize user security while affording ease of use. In *Proceedings of the 2021 European Symposium on Usable Security* (pp. 23–28). https://doi.org/10.1145/3481357.3481376

Chalhoub, G. (2020, April). The UX of things: Exploring UX principles to inform security and privacy design in the smart home. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–6). https://doi.org/10.1145/3334480.3381436

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., ... & Stephenson, R. J. (2019, September). Human risk factors in cybersecurity. In Proceedings of the 20th annual SIG conference on information technology education (pp. 87–92). https://drive.google.com/file/d/1vHMG7RON5GcBvQdx7sYO0kCmdZomNvyS/view

CyBOK. (2019). *CyBOK* – The cyber security body of knowledge *v1.0*. CyBOK – The CyberSecurity Body of Knowledge. https://www.cybok.org/knowledgebase/

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage, and usability: Redefining human-centric cyber security. Frontiers in Big Data, 4, 583723. https://www.frontiersin.org/articles/10.3389/fdata.2021.583723/full

Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. In Research anthology on artificial intelligence applications in security (pp. 1960-1977). IGI Global. https://dora.dmu.ac.uk/bitstream/handle/2086/15621/Hadlington

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) (pp. 338–345). IEEE. https://easychair.org/publications/preprint_download/XRKm

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, *3*(1), 1–18. https://doi.org/10.1186/s42400-020-00050-w

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, *27*(1), 64–77. https://doi.org/10.46743/2160-3715/2022.5044

Münch, C., Marx, E., Benz, L., Hartmann, E., & Matzner, M. (2022). Capabilities of digital servitization: Evidence from the socio-technical systems theory. *Technological*

Forecasting and Social Change, *176*, 121361. https://doi.org/10.1016/j.techfore.2021.121361

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. HOLISTICA–Journal of Business and Public Administration, 9(3), 71-88. https://sciendo.com/pdf/10.2478/hjbpa-2018-0024

Paul, J., Lim, W. M., O'Cass, A., Hao, A. W., & Bresciani, S. (2021). Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies*, *45*(4), O1-O16. https://doi.org/10.1111/ijcs.12695

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24(2), 371-390. https://link.springer.com/article/10.1007/s10111-021-00683-y

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. Human factors, 60(5), 597–609. https://www.bendsawyer.com/wp-content/uploads/2017/10/Sawyer-et-al.-2018-Hacking-the-Human-The-Prevalence-Paradox.pdf

Young, H., van Vliet, T., van de Ven, J., Jol, S., & Broekman, C. (2018). It is understanding human factors in cyber security as a dynamic system. In Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17− 21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA 8 (pp. 244-254). Springer International Publishing. https://www.researchgate.net/profile/Heather-Young-7/publication/318131332_Understanding_Human_Factors_in_Cyber_Security_as_a_Dynamic_System/links/622f1c83a39db062db9c8b8a/Understanding-Human-Factors-in-

Cyber-Security-as-a-Dynamic-System.pdf

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. International Journal of Human-Computer Studies, *131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Section 2: Ethical approval

1. Consent

How do you intend to seek informed consent from participants?

N/A

2. Right to withdraw

How do you intend to inform participants of their right to withdraw? N/A

3. Confidentiality

How do you intend to maintain confidentiality?

N/A

4. Harm

How do you intend to protect participants from harm?

N/A

5. Data access, storage and security

Please confirm that all personal data will be stored and processed in compliance with the General Data Protection Regulation (GDPR). Describe the arrangements for storing and maintaining the security of any personal data collected as part of the project.

6. Other issues

N/A

Identify any specific ethical issues relating to this research, for example if your research involves vulnerable groups like young children, or pupils who have SEND (special educational needs/disability).

Section 3: Risk Assessment

If your research does not involve human participants, you are able to enter "N/A" in the comment box.

N/A

1. Are there any potential risks, for example physical, psychological, social, legal or economic, to participants or subjects associated with the proposed research?

YES / NO

Please provide full details of the potential risks and explain what risk management procedures will be put in place to minimise the risks:

N/A

2. Are there any potential risks to researchers as a consequence of undertaking this proposal?
YES / NO
Please provide details and explain what risk management procedures will be put in place to minimise this.

3. Are there any potential reputational risks to the University as a consequence of undertaking this

N/A

proposal?
YES / NO
Please provide full details and explain what risk management procedures will be put in place to minimise this.

N/A

4. Will the research involve individuals below the age of 18 or individuals of 18 years and over with a limited capacity to give informed consent?
YES / NO

(If yes, a Disclosure and Barring Service disclosure (DBS check) may be required. Please attach as part of your application). Give further details of participants below.

N/A

5. Are there any other ethical issues that have not been addressed, which you would wish to bring to our attention?
YES / NO
Give details below:

N/A

Section 4: Confirmation Statements

The results of research should benefit society directly or by generally improving knowledge and understanding. I confirm that my research project has a potential benefit. (If you cannot identify a benefit, you must discuss your project with your supervisors to help identify one or adapt your proposal so the study will have an identifiable benefit.)

I confirm that I have read the Research Ethics Policy and the relevant sections of the Research Ethics Procedures and will adhere to these in the conduct of this project.

(These statements must be ticked in the form.)

Signature

N/A

Attachments

You are required to attach the following documents to this form:

1. An example of your participant information sheet and consent form, if applicable.

   N/A

2. Consent document from the organisation your research is taking place, if applicable.

   N/A