HUMAN-CENTRIC APPROACHES TO INFORMATION SECURITY: EMPOWERING FUTURES

Fidelis Obukohwo Aghware
Computer Science Department
University of Delta
Agbor, Nigeria.
http://orcid.org/0000-0001-7040-9387

Lucky Ogechukwu Okoh
ICT Department
University of Delta
Agbor, Nigeria.
http://orcid.org/0009-0001-2994-1889

Bridget Ogheneove Malasowe
Computer Science Department
University of Delta
Agbor, Nigeria.
http://orcid.org/0000-0002-6104-2314

***Abstract* — This article addresses the critical challenges of information security through human-centric approaches. Misalignment between work practices, business processes, and security support procedures often exacerbates security issues. By integrating human-computer interaction and socio-cognitive research, this book explores how organizations can achieve a human-centric alignment in developing and managing secure systems. This collaborative work highlights the importance of human factors in preventing and mitigating attacks, emphasizing that human-centric strategies are essential for robust information security frameworks.**

Keywords — ***human-centric approach, information security, organizational processes, human-computer interaction, socio-cognitive research***

I. INTRODUCTION

This section explores the importance of human-centered approaches to information security and their potential impact on future developments in the field.xplores the notion that the two most prevalent approaches to contemporary information security can be characterized as technology-centric or regulation-centric. In the technology-centric approach, sustainable information security is seen as securing the computational infrastructure, software applications, and services in which information is used and shared. This approach is supplemented with security-centric legislation and regulatory measures characteristic of the regulation-centric approach. These two umbrella approaches act as general filters for the wide and diverse range of knowledge and technique areas that contribute to information security at local, organizational levels and at national, international levels.

Information security is a necessary aspect of the information society and those participating in it. [1][2][3]

Some possible predictions could be:

- "It is essential to prioritize the protection of personal and sensitive data."
- "In today's digital age, the ever-evolving threat landscape requires innovative approaches to safeguarding information."
- "As technology continues to advance, the importance of implementing human-centric strategies becomes increasingly apparent. "Predicted next words:

"It is essential to consider human-centric approaches to ensure the protection of personal and sensitive data. This essay will explore the empowerment of individuals and organizations in information security and the potential impact on future advancements in the field." [4][5]

The nature of attackers, threats, and attacks is unfavorable to populations and individuals who interact with, create, and use information technology. Over thirty years of global information security initiatives have entrenched digital information security into organizational risk management concerns. Information security is in such a situation that it cannot be delegated to specific areas of an organization, nor can it be bolted on in the way that technical knowledge and skills can be placed into products and solutions. [6][7][8]

Recognition of the breadth of human issues in information security is reflected in calls for the development of preventative, deterrent, and contributory areas of knowledge, skills, and techniques.

A. Research Gaps

Looking at the topics discussed above, e.g., peer pressure, social identity, trust, privacy calculus etc., it is important to acknowledge the dearth of information on how to orchestrate change for these phenomena. To what extent are security norms evolving in organizations over time, what types of in/formal control mechanisms are organizations applying, which processes are modal for the evolution of security awareness or how stem? And, how and by which means may organizations monitor these processes so that they can make targeted decisions for improvement?

In understanding social and behavior change, there are a number of research gaps that invite further research. Researching social cognition is a relatively young research paradigm and yet it is widely accepted that it is pertinent to understand for successful social and behavior change at large. This also holds true for our research on social and behavior change in the area of information security.

This brings us to related gaps of knowledge in the areas of socio-cognitive research and the development of innovative uses of IS frameworks to facilitate security deployment inside organizational life.

II. LITERATURE REVIEWS

Literature surveys done in the fields of information security indicated that it is currently indistinct and diverse. It is usually guarded by technical security personnel relying heavily on technical controls designated to protect against unauthorized access, which are intended to protect digital data of an organization and base-wide with respect to information management. [1][9]

There is a glaring recognition regarding the individual person as an essential element in information security practice, particularly within information security discourse from a human science stand, which has started to gain more traction recently. However, this line of thought is often not passionately presented, desultory, and even occasionally

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

ignored entirely. In addition, it is often belittled by information security staff tasked with technical operational duties. [1][3]

Different intrinsic values of students who engage in postgraduate studies due to them already being the custodians of the main client of Vermooten's study (in a commercial audit firm or the public sector) were also reported. [10]

Various soft elements, such as time spent on experiences, professional status, self-confidence, having a broad perspective well-spring and big-company orientation, are used as predictive indicators of both loyalty and intention to explore new employment opportunities. With the increasing need for postgraduate studies in the discipline of internal audit influencing the well-being of future employees, the determinant factors and their accurate significance should be further researched and investigated. [11][12]

Introduction: This section described the literature reviews undertaken to inform the development of the framework and guidelines. A framework was proposed to describe factors that postgraduate students at the University of Pretoria, Internal Audit and Forensic Accounting students presently consider for securing their information. Guidelines based on the framework have also been discussed and a structure for such guidelines proposed. The intention and mandates of various existing bodies and committees worldwide, as well as informatics and other academic research exploring information security, were investigated. This included an examination of the 'soft' characteristics of students such as their management styles, risk behavior, leadership qualities, and social competencies. The latter should be considered by professional bodies and tertiary institutions involved in education and training.

III. METHOD

The two main issues that have been the focus of our recent research involve privacy capabilities and the requirement of benefits realization to prevent security incidents, especially due to underestimated privacy demands. Privacy capabilities empower information security architectures and related artifacts as their interaction to prevent or contain privacy incidents, including identity theft and impersonation issues explicitly. The public acceptance of surveillance during the present pandemic by nationwide tracing applications shows integrating privacy capabilities to understand privacy considerations better overall remains necessary. Despite varying substantial positive effects, for instance, to detect a COVID-19 infection promptly, tracking terminal illnesses of threatened domestic violence victims. [13]

In the social constructivist theory underpinning the Jansen et al. approach developed, that is summarized in the subsequent section "Value Situation of Information." Special care is devoted to how stakeholders use information and make decisions, respecting information technologies beneficial to prevent or contain, e.g., privacy incidents. [14]

A. Contributions to Knowledge

In adopting a people-centric approach, it is not anticipated that the technical and procedural measures traditionally identified and deployed in information security will be diluted, but simply that they will be supplemented with considerations that encompass a broader level of expertise. This level of expertise is richer in terms of quality and enables sustainable interactions and development between individuals and groups in their interactions with these technical and procedural solutions.

Of course, different occupational groups and people employ different ways of successfully coping with the system and the risks associated with it. In pinning down and discussing these worlds, one is taking a vital step in structuring a more realistic and a more comprehensive view of risk. Contributors have covered this area, with many of them highlighting the 'front-line' operators who must cope with the threats and the failures that others have not been able to address or reduce adequately. Ten proposal themes have been highlighted in this article as prime areas for improving the management of the threats of information security and technology. We believe that these areas must be addressed to move from the concept of information security to the practice.

The risk analysis, which is the backbone of safety science, is enhanced by looking at these constructs and extending them. Traditionally, safety experts have been trained to see the black-and-white formal outcomes of error as 'failures'. It is often the laypeople whom the safety and security culture of organizations consider to be at the root of exposure to danger. Very rarely have the perspectives and interpretations of these laypeople been systematically explored and understood. Such wider perspectives argue that human interpretation of safety critical systems needs to be understood to a wider depth than it is currently. We are not arguing that risk assessment is entirely subjective but, rather, it is a reflection of the system from the point of view of those who have to live within it. The system was, after all, built for them.

In this article, we described what human-centric approaches to information security are and what aims they have. These aims are not merely about user friendliness but about enabling futures. We argued that information security risks need to be managed in a multi-disciplinary way that better encompasses human values. We discussed the current state of play in information security and safety science, and its limitations. Subsequently, in this article, we addressed constructs across disciplines that need to be taken into account when considering human interpretations of the risks arising from information security technologies.

IV. DISCUSSIONS

Additionally, for corporate users' continuous user awareness education, currently, awareness programs' focus is mainly on the promotion of security policies, and they focus on general ICT rules. However, since hacks seem to be focusing on end users who are not familiar with these security policies, coverage of security issues through general user awareness programs is limited to encrypted hack information, security patches, password usage, management, tablet security, and social networking sites. The application of the program is also problematic because it is rare for general users to catch the proposed vulnerabilities and to make peace with the complex security countermeasures. The relationship of end-user behavior to security has not yet been established as a field of study.

Thus, the paper argues that there are important opportunities for researchers and practitioners to move toward a human-centric orientation when dealing with underlying core issues of information security. A couple of examples include how, currently, the focus of attribution studies is mainly on cybercriminals and rogue states for major cyber war threats and large-scale cyber attacks, etc. However, as some studies have pointed out, though there is no solid proof/confirmation, the percentage of crowdsourcing malicious codes has grown to the scale of 10%~25% recently. Such shifts invite us, the researchers, to reconsider the severity of the threats considered and to investigate both the technological and human perspective of the issues and to develop appropriate countermeasures. Furthermore, due to the importance of human behavior, it has become critical to consider psychological factors of the organizations' users and end users as well.

V. SUMMARY

The article introduced a pair of human-centric metaphors, leadership and a role of team manager, to discuss a new pedagogical tool of Forecast Deliverable Projects in the Information Sciences & Technology course as a mechanism testing students understanding of the material, application to the material and ideas for moving the stewardship of information forward after the completion of the course. Implemented during the spring 2010 semester, the Forecast Deliverable Projects were designed to address a series of traditional outcomes of a final project, while emphasizing a deliverables-based framework and development of soft skills. Accompanying the Forecast Deliverable Projects upon their completion were student preparations towards the mid-term, as both an opportunity for students to engage with material and for the instructor to assess the effectiveness of the Forecast Deliverable Project requirement.

This chapter responded to the challenge outlined at the Symposium, "Security Metaphors: Designing for E-Safety": how to infuse the conversation about information security at large, specifically in computer science education more generally, with the humanistic considerations needed to develop responsible and broadly educated computing practitioners and experts. It summarized a human-centered approach for developing - within the technical-security classroom - the capacity for secure and responsible stewardship of all of the various types of information we have developed and which we, as humankind, currently have access to, independent of its actual use in the class. It employed the metaphor of "shepherding" in framing information stewardship for students and incorporation as an information steward into the newly emerging areas of the Web community that are exploring more socially-conscious uses of the Web.

REFERENCES

[1] M. D. Okpor, F. O. Aghware, M. I. Akazue, A. A. Ojugo, F. U. Emordi, C. C. Odiakaose, R. E. Ako, V. O. Geteloma, A. P. Binitie, and P. O. Ejeh, "Comparative Data Resample to Predict Subscription Services Attrition Using Tree-based Ensembles," Journal of Fuzzy Systems and Control, vol. x, no. x, 2024. ISSN: 2986-6537, DOI: 10.59247/jfsc.vxix.xx.

[2] F. Aghware, W. Adigwe, M. Okpor, C. Odiakaose, A. Ojugo, A. Eboka, P. Ejeh, E. O. Taylor, R. Ako, and V. Geteloma, "BloFoPASS: A blockchain food palliatives tracer support system for resolving welfare distribution crisis in Nigeria," International Journal of Informatics and Communication Technology (IJ-ICT), vol. 13, no. 2, pp. 178-187, Aug. 2024. ISSN: 2252-8776, DOI: 10.11591/ijict.v13i2.pp178-187.

[3] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, et al., "Cyber security awareness, knowledge and behavior: A comparative study," Journal of Computer Information Systems, vol. 2022, Taylor & Francis, 2022. researchgate.net. https://doi.org/10.1080/08874417.2021.1876561

[4] S. Human and F. Cech, "A human-centric perspective on digital consenting: The case of gafam," in Human Centred Intelligent Systems: Proceedings of …, Springer, 2021. wu.ac.at., https://doi.org/10.1007/978-3-030-70512-4_15

[5] B. Wang, P. Zheng, Y. Yin, A. Shih, and L. Wang, "Toward human-centric smart manufacturing: A human-cyber-physical systems (HCPS) perspective," Journal of Manufacturing, vol. 2022, Elsevier, 2022. parkjonghyuk.net https://doi.org/10.1016/j.jmsy.2021.10.007

[6] S. Schinagl and A. Shahim, "What do we know about information security governance? “From the basement to the boardroom”: towards digital security governance," Information & Computer Security, 2020. emerald.com https://doi.org/10.1108/ICS-12-2019-0145

[7] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things," Heliyon, 2021. cell.com https://doi.org/10.1016/j.heliyon.2021.e06650

[8] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 14, no. 6, pp. 94-100, 2023. DOI: 10.14569/IJACSA.2023.0140610.

[9] E. Yoro, F. O. Aghware, M. I. Akazue, A. E. Ibor, and A. A. Ojugo, "Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian," International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 2, pp. 1943-1953, Apr. 2023. DOI: 10.11591/ijece.v13i2.pp1943-1953.

[10] A. Wigfield and J. S. Eccles, "35 years of research on students' subjective task values and motivation: A look back and a look forward," Advances in motivation science, 2020. [HTML] https://doi.org/10.1016/bs.adms.2020.01.002

[11] A. T. Verčič, "The impact of employee engagement, organisational support and employer branding on internal communication satisfaction," Public Relations

Review, 2021. [HTML] https://doi.org/10.1016/j.pubrev.2020.102011

[12] R. Manita, N. Elommal, P. Baudier, and L. Hikkerova, "The digital transformation of external audit and its impact on corporate governance," Technological Forecasting and Social Change, vol. 150, 2020, Elsevier. e-tarjome.com https://doi.org/10.1016/j.techfore.2019.119751

[13] E. Uzobo and A.D. Ayinmoro, "Trapped between two pandemics: domestic violence cases under COVID-19 pandemic lockdown: a scoping review," Community Health Equity Research & Policy, vol. 2023. journals.sagepub.com. sagepub.com https://doi.org/10.1177/0272684X231169798

[14] F. O. Aghware and B. O. Malasowe, "Empirical Evaluation of Hybrid Cultural Genetic Algorithm Trained Modular Neural Network Ensemble for Credit-Card Fraud Detection," International Journal of Advances in Engineering and Management (IJAEM), vol. 5, no. 3, pp. 1516-1524, 2023. DOI: 10.35629/5252-050315161524.