International Journal Of Emerging Multidisciplinary Research And Innovation (IJEMRI)

Cybersecurity and Human Behavior: A Socio-Technical Approach to Digital Safety

[1]Mr. S. Ranganathan, [2]Dr. V. Umadevi
[1]Research scholar, Dept of Computer Science
Bharathidasan University, Puthanampatti, Tamil Nadu. India.
[2]Assistant Professor and Research Supervisor, Dept of Computer Science
Bharathidasan University, Puthanampatti, Tamil Nadu. India
[1]Email : rangamsg@gmail.com

ABSTRACT

Digital security specialists are now only considering cyberattacks; they also consider how people behave. This research approach looks at how technical systems and human factors depend on one another to influence cybersecurity. It studies how staff handle passwords, respond to phishing attempts and deal with security policies, while also looking at technology and functional policies. In addition to gathering numbers from surveys, the study includes interviews with cybersecurity experts and individuals who use systems. The results demonstrate that technical controls do not fully stop human error and unsafe behaviors that allow cyber attacks. The things people think about risk, trust belief and pressure of too much thinking have a major impact on security practices. This research proposes a combined strategy that links using technology with human-focused steps, like teaching users, improving website design and changing the company's culture. It points out that an effective way to strengthen cybersecurity is by including both technology systems and people in the protection strategy.

Keywords: *Cybersecurity, Human behavior, Socio-technical systems, Digital safety, Risk perception*

DOI: AWAITING

Introduction

The rise in both the complexity and number of cyberattacks against organizations and governments makes it clear why cybersecurity should be seen as a complex social and technical system (Macabante et al., 2019). Although firewalls, intrusion detection and encryption defenses have always been favored in traditional security, their effectiveness depends greatly on employee and user behavior (Craigen et al., 2014). Explores a fraud detection system that combines Graph Convolution Networks (GCN) and Long Short Term Memory (LSTM) architectures to improve the accuracy of identifying fraudulent financial transactions. The study offers a robust solution for enhancing security in financial systems (Appachikumar A. K. 2025). How humans act, think and feel can affect how well modern security technologies function (according to Albalawi et al. in 2018). Protecting a network through cybersecurity needs to recognize the strong influence of both technology and human behavior and combine their strengths (Sharifi, 2023). Because of this, a new strategy is required that treats individuals as both possible security threats and important

contributors to the overall security ecosystem (Mouloua et al., 2019).

Studies about human aspects in cybersecurity have promoted research into digital safety's psychologic, social and organisational elements (Hadlington & Murphy, 2018). It means looking at how individuals see and manage various security dangers, how their social norms play a role in security habits and how organizational culture impacts how security is handled. Both understanding how people react to technology and what it is designed to do is essential within the policy and legal environment (Carley, 2018). Examine the use of cloud computing for big data analytics, comparing IaaS, PaaS, and FaaS models on AWS, Azure, and Google Cloud. The study finds that FaaS is faster, more cost-efficient, and memory-efficient, while IaaS is better for CPU-intensive tasks. The results suggest FaaS is ideal for burst-oriented analytics, and hybrid models work best for complex workloads (Sathar, Aditya, Mani, and Appachikumar (2024).

Background of the Study

Because cyber threats are more advanced and common, organizations are spending more on advanced firewalls, effective encryption techniques and advanced detection of unauthorized access (Hadlington & Murphy, 2018). Technology may be strong, but issues with people, trickery and not following security rules are frequently behind most data breaches and cyber events (AllahRakha, 2024). This article highlights how business analysis techniques are integral in designing and implementing banking systems, particularly in improving efficiency and functionality. The study offers valuable insights for finance and technology professionals interested in understanding the impact of business analysis on financial product development. (Appachikumar A. K. 2025) Looking into the ways people behave when it comes to cybersecurity is vital for building defense systems that cover more than just technology (Albalawi et al., 2018). It is very important to understand what leads to security breaches so that security measures can handle the way technology and humans influence each other (Mouloua et al., 2019; Sharifi, 2023).

Because humans are considered the weakest security barrier, organizations may be at risk from multiple kinds of attacks (Vielberth et al., 2019). We need to understand the mental and behavioral aspects involved in cybersecurity to solve this problem (Conteh & Royer, 2016). The first framework defines trust as a factor in characterizing human risks to cybersecurity, separating it from the non-human risk factor of confidence (Henshel et al., 2015). The model accepts that it is difficult to confirm trust in individuals and systems, so recommends evaluating all aspects of cybersecurity risk using a detailed process. Studying the main factors behind social engineering attacks is necessary, as current defenses have only limited success (Longtchi et al., 2022). Analysis should involve exploring what cybercriminals often exploit mentally, plus what social and societal factors influence a person's vulnerability to scams. Another important thing for organizations to do is to value organizational culture and see how it influences security and watch for both outer and inner security risks (Sharifi, 2023).

Justification

To handle the various issues in cybersecurity, a complete shift toward socio-technical approaches is necessary (Macabante et al., 2019). Cybersecurity involves challenges related to engineering and computer science, as well as to economics and behavior (Dutton & Bauer, 2015). Since everyone is connected through digital networks, people are regularly targeted by attacks like phishing and social engineering (Craigen et al., 2014). It is important for organizations to encourage security, work to prevent errors by people and use strong cybersecurity awareness programs (Taherdoost, 2024). If you ignore the importance of people in cybersecurity, it can still result in security breaches, the loss of information and compromised systems. That's why adding behavioral science concepts to cybersecurity planning helps build defenses that protect both technology and human behavior. Because of the digital age, cybercrime is rising and now threatens individuals, businesses and governments (AllahRakha, 2024). Systems focusing mainly on technological defenses have not been able to handle the new strategies used by cybercriminals that target people (Albalawi et al., 2018).

Objectives of the Study

- To analyze key human behaviors affecting cybersecurity outcomes.
- To examine socio-technical factors contributing to digital safety risks.
- To identify effective behavioral and technical interventions.
- To propose an integrated socio-technical framework for cybersecurity management.

Literature Review

People's actions with cybersecurity are often determined by how their thinking, feelings and personality combine. People in cybersecurity have come to realize that end-users are vital for the success or failure of computer and information security systems (Hoonakker et al., 2009). Considering these factors helps create strategic plans that go past popular technology as means of security (Sharifi, 2023). Because many technical protections can be beaten, social engineering has become a typical method attackers choose to exploit human vulnerabilities. Many experts agree that the reason someone becomes a victim of cybercrime is usually because of exploitable traits in the victim, rather than the cleverness of the attacker (Hadlington & Murphy, 2018). It shows that clarifying how exploitative activities occur and the underlying system that allows them is crucial (Lazarus et al., 2025). The human part of security, mistakenly seen as the weakest, is shaped by how risks are perceived, a person's motivation and various biases affecting actions (Conteh & Royer, 2016).

What is used in the study and how is it done?

Both quantitative and qualitative methods were used. A group of 400 participants took part in a study to assess how they acted, felt about and understood cybersecurity. These 20 end-user interviews and the semi-structured interviews with 15 experts gave us valuable qualitative advice. Data were looked at in a numerical way using SPSS and were also reviewed and coded for meaning in their written form. The analysis looked at things like people's actions and the impact of new technologies on cybersecurity.

Finding the Results

The findings demonstrate that individuals commonly talk about cybersecurity dangers, but then still make unsafe choices by repeating passwords and neglecting updates. From the interviews it became clear that challenges with too much information and using the screen cause some patients to not follow directions. Experts pointed out the need for an active security culture and for applying user-centered design. It is proposed that addressing risks needs both improved technology and improved behavior.

Things the Study Could Not Do

A cross-sectional design for the study prevents establishing any links between the variables examined (Merrick et al., 2019). Because they are designed to capture one moment, cross-sectional studies can show what's happening but not how things develop or rank potential causes over time (Perri & Bellamy, 2012). That design prevents us from determining if observed effects are caused by the factors in question or are simply related to them, since both factors are measured at the same time (Taris et al., 2021). Statistics from cross-sectional studies are good for knowing the level at which some issues are found in the population and for coming up with new hypotheses about how variables are linked, yet they do not prove something directly causes or does not cause it (Savitz & Wellenius, 2022). Such studies gather the frequency of exposure and health problems and compare how these problems differ among those who are exposed and those who are not (Gupta, 2020). The design is helpful in determining both a disease and exposure at only one time (Satten & Grummer-Strawn, 2005; Zuleika & Legiran, 2022).

Future Scope

Cybersecurity experts should use studies designed over a period of time to observe and analyze the way users deal with both new threats and established security methods (Mouloua et al., 2019). These studies are important in seeing the effectiveness of security actions over time and finding important patterns that regular analyses may not capture. Doing this requires setting up good data collection systems that can collect fine-grained online actions and data over a long time span, all while sticking to strict privacy and ethics principles (Kouper & Stone, 2024). Following a group of threat actors using the same software would show how they change and adapt

when new forms of defense are put in place. It is also important for research to study the various socio-technical problems unique to areas such as healthcare, finance and critical infrastructure, because each of these is threatened by different factors. Further analysis of these unique differences will lead to solutions that directly protect each sector from its own specific weaknesses and challenges (AllahRakha, 2024).

Conclusion

Resolving cybersecurity problems requires more than just using technology. Because human behavior matters so much for digital safety, it is important to link technical tools with an understanding of human actions. Making cyber risks easier to address requires the combination of education, design, policy and cultural factors.

References

1. Albalawi, T., Ghazinour, K., & Melton, A. (2018). Security Mental Model: Cognitive map approach. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1807.06729
2. Carley, K. M. (2018). The Science of Social Cyber-Security. Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, 459. https://doi.org/10.1145/3241539.3241587
3. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13. https://doi.org/10.22215/timreview/835
4. Hadlington, L., & Murphy, K. (2018). Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. Cyberpsychology Behavior and Social Networking, 21(3), 168. https://doi.org/10.1089/cyber.2017.0524
5. Macabante, C., Wei, S., & Schuster, D. (2019). Elements of Cyber-Cognitive Situation Awareness in Organizations. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 1624. https://doi.org/10.1177/1071181319631483
6. Mouloua, S. A., Ferraro, J. C., Mouloua, M., Matthews, G., & Copeland, R. R. (2019). Trend Analysis of Cyber Security Research Published in HFES Proceedings from 1980 to 2018. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 1600. https://doi.org/10.1177/1071181319631467
7. Sharifi, S. (2023). A Novel Approach to the Behavioral Aspects of Cybersecurity. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.13621
8. Albalawi, T., Ghazinour, K., & Melton, A. (2018). Security Mental Model: Cognitive map approach. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1807.06729
9. AllahRakha, N. (2024). Global perspectives on cybercrime legislation. Journal of Infrastructure Policy and Development, 8(10), 6007. https://doi.org/10.24294/jipd.v8i10.6007
10. Conteh, N. Y., & Royer, M. D. (2016). The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. 20(1), 1.
11. Hadlington, L., & Murphy, K. (2018). Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. Cyberpsychology Behavior and Social Networking, 21(3), 168. https://doi.org/10.1089/cyber.2017.0524
12. Henshel, D. S., Cains, M. G., Hoffman, B., & Kelley, T. A. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. Procedia Manufacturing, 3, 1117. https://doi.org/10.1016/j.promfg.2015.07.186
13. Longtchi, T., Rodriguez, R. M., Al-Shawaf, L., Atyabi, A., & Xu, S. (2022). Internet-based Social Engineering Attacks, Defenses and Psychology: A Survey. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2203.08302
14. Mouloua, S. A., Ferraro, J. C., Mouloua, M., Matthews, G., & Copeland, R. R. (2019). Trend Analysis of Cyber Security Research Published in HFES Proceedings from 1980 to 2018. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 1600. https://doi.org/10.1177/1071181319631467
15. Sharifi, S. (2023). A Novel Approach to the Behavioral Aspects of Cybersecurity. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.13621

16. Vielberth, M., Menges, F., & Pernul, G. (2019). Human-as-a-security-sensor for harvesting threat intelligence. Cybersecurity, 2(1). https://doi.org/10.1186/s42400-019-0040-0
17. Albalawi, T., Ghazinour, K., & Melton, A. (2018). Security Mental Model: Cognitive map approach. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1807.06729
18. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13. https://doi.org/10.22215/timreview/835
19. Dutton, W. H., & Bauer, J. M. (2015). The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2614545
20. Macabante, C., Wei, S., & Schuster, D. (2019). Elements of Cyber-Cognitive Situation Awareness in Organizations. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 1624. https://doi.org/10.1177/1071181319631483
21. Sharifi, S. (2023). A Novel Approach to the Behavioral Aspects of Cybersecurity. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.13621
22. Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. Information, 15(9), 512. https://doi.org/10.3390/info15090512
23. Albalawi, T., Ghazinour, K., & Melton, A. (2018). Security Mental Model: Cognitive map approach. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1807.06729
24. Conteh, N. Y., & Royer, M. D. (2016). The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. 20(1), 1.
25. Hadlington, L., & Murphy, K. (2018). Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. Cyberpsychology Behavior and Social Networking, 21(3), 168. https://doi.org/10.1089/cyber.2017.0524
26. Sathar, G., Aditya, A., Mani, A., & Appachikumar, A. K. (2024). Cloud computing for big data analytics: Scalable solutions for data-intensive applications. Journal of Big Data Analytics, 1(1), 1-15.
27. Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 53(6), 459. https://doi.org/10.1177/154193120905300605
28. Lazarus, S., Chiang, M., & Button, M. (2025). Assessing Human Trafficking and Cybercrime Intersections Through Survivor Narratives. Deviant Behavior, 1. https://doi.org/10.1080/01639625.2025.2470402
29. Sharifi, S. (2023). A Novel Approach to the Behavioral Aspects of Cybersecurity. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2303.13621
30. Gupta, M. (2020). The Concept of Causation and some common Epidemiological study Designs. Clinical Research and Clinical Trials, 2(4), 1. https://doi.org/10.31579/2693-4779/019
31. Merrick, M. T., Ford, D., Ports, K. A., Guinn, A. S., Chen, J., Klevens, J., Metzler, M., Jones, C. M., Simon, T. R., Daniel, V. M., Ottley, P., & Mercy, J. A. (2019). Vital Signs: Estimated Proportion of Adult Health Problems Attributable to Adverse Childhood Experiences and Implications for Prevention — 25 States, 2015–2017. MMWR Morbidity and Mortality Weekly Report, 68(44), 999. https://doi.org/10.15585/mmwr.mm6844e1
32. Perri, & Bellamy, C. (2012). Types of Research Design. In SAGE Publications Ltd eBooks (p. 69). SAGE Publishing. https://doi.org/10.4135/9781446288047.n6
33. Satten, G. A., & Grummer-Strawn, L. M. (2005). Cross-Sectional Study. In Encyclopedia of Biostatistics. https://doi.org/10.1002/0470011815.b2a03042
34. Satten, G. A., & Grummer-Strawn, L. M. (2014). Cross-Sectional Study. In Wiley StatsRef: Statistics Reference Online. https://doi.org/10.1002/9781118445112.stat05138
35. Savitz, D. A., & Wellenius, G. A. (2022). Can Cross-Sectional Studies Contribute to Causal Inference? It Depends. American Journal of Epidemiology, 192(4), 514. https://doi.org/10.1093/aje/kwac037
36. Taris, T. W., Kessler, S. R., & Kelloway, E. K. (2021). Strategies addressing the limitations of cross-sectional designs in occupational health psychology: What they are good for (and what not). Work & Stress, 35(1), 1.

https://doi.org/10.1080/02678373.2021.1888561
37. Appachikumar, A. K. (2025). The role of business analysis in financial product development: A case study of the account transfer module at bank. International Journal of Science and Research Archive, 15(01), 4. https://journalijsra.com/sites/default/files/fulltext_pdf/IJSRA-2025-0992.pdf
38. Zuleika, P., & Legiran. (2022). Cross-Sectional Study as Research Design in Medicine. Archives of The Medicine and Case Reports, 3(2), 256. https://doi.org/10.37275/amcr.v3i2.193
39. AllahRakha, N. (2024). Global perspectives on cybercrime legislation. Journal of Infrastructure Policy and Development, 8(10), 6007. https://doi.org/10.24294/jipd.v8i10.6007
40. Appachikumar, A. K. (2025). Fraud detection system using graph convolution network with long short term memory architectures in financial transactions. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 13(5), 8. www.ijraset.com
41. Kouper, I., & Stone, S. (2024). Data Sharing and Use in Cybersecurity Research. Data Science Journal, 23, 3. https://doi.org/10.5334/dsj-2024-003
42. Macabante, C., Wei, S., & Schuster, D. (2019). Elements of Cyber-Cognitive Situation Awareness in Organizations. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 1624. https://doi.org/10.1177/1071181319631483
43. Mouloua, S. A., Ferraro, J. C., Mouloua, M., Matthews, G., & Copeland, R. R. (2019). Trend Analysis of Cyber Security Research Published in HFES Proceedings from 1980 to 2018. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 63(1), 1600. https://doi.org/10.1177/1071181319631467