An Interdisciplinary Understanding of The Human Factor of Cybersecurity

Eric Mung'aũ Preston

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Dr. Patricia Oliver

December 1, 2024

Abstract

Cybersecurity has become a prominent topic today due to daily cyber-attacks. A common element in most cyber-attacks is someone making a mistake that leads to them being compromised. This "human factor" is a prevalent problem within the cybersecurity industry that has been a constant issue to circumvent. However, while cybersecurity alone has some capability of handling the problem, it hasn't been possible to fully solve it by only addressing it within its field. This paper will present a potential solution to the human factor issue by utilizing the interdisciplinarity research process along with the disciplines of Psychology, Sociology, and Cybersecurity. These three disciplines will be able to tackle the human factor issue by explaining how behavioral, cultural, and technological influences around people cause them to be easy targets for cyber-attacks. The findings showed that impulsivity, cognitive biases, inhibitive organizational culture, enabling of poor cybersecurity practices in culture, and abrasive cybersecurity controls were the greatest factors that resulted in a cyber-attack. Due to how the human factor encompasses behavioral, social, and technological fields, more interdisciplinary research should be conducted in the future to explore new insights for solutions.

Keywords: Cybersecurity, Psychology, Sociology, human factor, culture, cognitive bias

Introduction

Several studies have indicated the impact of the "human factor" on security incidents. According to The IBM Security Services 2014 Cyber Security Intelligence Index, regarding the impact of security incidents, "over 95 percent of all incidents investigated recognize "human error" as a contributing factor." This includes actions such as the use of default or easy passwords and clicking on malicious attachments (IBM, 2014). Another study predicts that by

2025, the cost of global cybercrime will reach upwards of $10.5 trillion, which is a substantial increase from the prediction of $3 trillion in 2015 (Desolda et al., 2021).

Background

While these studies do not represent all types of cyber-related crime, cybersecurity incidents, regardless, have become a significant concern within our digitized economy due to cost and frequency in the past decade. Some of the attacks involve social engineering, which is a tactic of manipulating people into giving up information, and phishing, which are attacks that hide malicious software or malware within seemingly safe emails or links (Washo, 2021). These attacks are meant to circumvent cybersecurity, which can be described as "an evolving set of devices, risk management technologies, training approaches, and specific measures designed to protect the networks, programs, and data from any unauthorized access" (AlSharif et al., 2022).

With this being an issue that involves the cybersecurity discipline, there have been attempts to understand it from that perspective. For example, there may be a focus on the technological side that people interact with when looking at immediate security controls such as passwords and emails as common sources of attacks that need constant improvement (AlSharif et al., 2022). However, one aspect of the issue that can be minimized in the process of assessment is the converse human element that interacts with technology. For this reason, this interaction makes it critical for us to understand technological factors and human factors regarding this issue.

The human factor of cybersecurity can be comprehensively understood via the interdisciplinary implementation of cognitive bias, cultural influence, and control design from the disciplines of psychology, sociology, and cybersecurity, respectively. Furthermore, the issue can be significantly reduced with tailored education for the average person.

This study will focus on answering one research question: “What factors cause people to have a higher likelihood of being hit with a cyber-attack?” This question is meant to cover the factors tied to technological reasons and emphasize influences associated with people to create a more cohesive understanding of the research question.

Methodology

The methodology for this paper will be a conceptual research study facilitated by the utilization of an extensive review of existing literature on interdisciplinary topics to identify key concepts, theories, and gaps in knowledge. Additionally, the author will critically evaluate and interpret the existing literature to develop new ideas and perspectives.

Interdisciplinarity as a Method

The human factor is a significant cybersecurity threat. While cybersecurity continues to focus on solutions, the application of interdisciplinarity to the problem is crucial as it not only helps us understand the issue but also informs and proposes new solutions. This is due to how the problem itself involves two broad areas that need to be covered, which include the technological aspects of digital security and the internal and external factors that influence how humans interact with each other and technology. In sum, utilizing interdisciplinarity and, by extension, the interdisciplinary research process as an aspect of the methodology is necessary for ensuring a holistic understanding.

Literature Review

Several studies have been conducted to address the “human factor” of security incidents. Studies such as The IBM Security Services 2014 Cyber Security Intelligence Index indicated that over 95% of all incidents investigated recognize the human factor as a major contributing factor. Noted actions included the use of default or easy passwords, clicking on malicious attachments,

and accidentally leaking sensitive information (IBM, 2014). In addition to that, another study predicted that by 2025, the cost of global cyber-crimes would reach upwards of $10.5 trillion, a substantial increase from the prediction of $3 trillion in 2015 (Desolda et al., 2021). While cybersecurity is central in the mitigation of these challenges, an interdisciplinary approach that includes psychological and sociological approaches presents as the best model as it examines and combines the strengths of each discipline. The human factors within psychological and sociological findings are examined below.

Psychological Findings

Starting with a psychological approach, in its simplest terms defined as "the study of the mind and behavior" (American Psychological Association, 2018), can address how people individually act, which causes them to be susceptible to an attack.

A significant psychological human factor found to impact susceptibility to an attack is the lack of control or impulsivity when online. Hadlington (2017) defines impulsivity as "the urge to act spontaneously without reflecting on an action and its consequences." Additionally, further information from Hadlington (2017) stated that "impulsivity was negatively correlated to security behaviors, presenting the potential for this trait to predict risky cybersecurity behaviors." Moustafa et al. (2021) also provide supporting evidence of how behaviors such as self-control and a desire for immediate gratification can increase the likelihood of a cyber-attack.

Another human factor is how people can have a perceived sense of security through being unaware of or close-minded to greater threats. The perception of safety can come from different kinds of cognitive bias, such as familiarity and confirmation bias (Singh & Cheema, 2024). In this case, familiarity bias stems from a user becoming comfortable with something over time, despite there being changing elements, while confirmation bias has the user only seek

information that affirms their present beliefs. These two forms of bias leave people to find safety in systems they know or fall victim to attacks like phishing or social engineering (Nobles & Mcandrew, 2023). Furthermore, this bias can also enable harmful security behaviors such as bypassing security controls, not following protocols, or leaning on convenient options as opposed to more secure options (Kadena & Gupi, 2021).

This risk of having a sense of security heightens when people's personality traits also affect their cybersecurity awareness. In a study conducted by Halevi et al. (2016), using the Big Five personality Framework of neuroticism, extroversion, openness, agreeableness, and conscientiousness, it was found that neuroticism, defined as a tendency to experience negative emotion, was the worst trait associated with self-efficacy, making it the most likely to leave people susceptible to attacks. Conversely, more agreeableness, conscientiousness, openness, and less impulsivity were discussed in the findings of a literature review as deemed to make someone less likely to be in an attack (Jeong et al. 2019).

Altogether, from a psychological perspective, the human factor of cybersecurity stems from the cognitive biases people have when interacting with technology. This includes not only the inherent personality traits they have but also behaviors like bias and impulsivity that can form over time due to using the Internet, while at the same time, not being aware or able to recognize cybersecurity threats.

Sociological Findings

A sociological perspective "examines the social structures, norms, and dynamics that shape human behavior and interactions within society" and, from that, can analyze groups and, specifically, organizational culture that can influence people's cybersecurity behavior (Singh & Cheema, 2024).

The immediate factor that can negatively influence cybersecurity awareness is harmful organizational culture. Organizational culture is defined as "a pattern of basic assumptions – invented, discovered, or developed by a given group as it learns to cope with the problems of external adaptation and internal integration – that has worked well enough to be considered valid, and therefore, to be taught to new members as the correct way to perceive, think and feel about these problems" (Parsons et al., 2010). Furthermore, Parsons et al. (2010) argue that due to the deep connections between organizational culture and the people within it, the culture cannot just have recent cybersecurity controls to protect information; it needs to be rooted at the fundamental level for security to be effective. When neglecting aspects of cybersecurity within a culture, such as security policies, plans, employee feedback, and security updates, they can enable both cybersecurity practices to be poor and employees to accept it as normal operations, contributing to risk. Moreover, according to Jeong et al. (2019), when having a security culture that is understandable but non-intrusive, cyber-attacks can reduce in frequency.

Another significant risk that exists from poor cybersecurity social norms is social engineering. Social engineering can be defined as "the act of using manipulation to obtain access to confidential information" and is a danger due to how the attack capitalizes on the social networks people exist in every day (Washo, 2021). Some of the common factors are an innate desire to help, solving perceived small problems, or requests that are overwhelming in the request (Parsons et al., 2010). However, there is an alternative with a positive social influence in the form of a positive organizational culture that promotes cybersecurity. According to Rahman et al. (2021), it was stated that "people are more likely to behave securely if they see others around them to behave securely."

Additionally, a cultural factor that is beneficial to an organization is a lean toward understanding and communication. Pollini et al. (2022) focus not only on the importance of something like procedures but also on the value of people understanding and not blindly accepting them. Communication within a culture can also be effective for mitigating security risks by having both employees and management understand one another, as well as motivating employees to take time to care more about security independently (Parsons et al., 2010; Pollini et al., 2022).

In short, a sociological perspective shows that the human factor of cybersecurity originates from a poor organizational work culture. Due to the human desire to be a part of a social network, a harmful culture can influence them as strongly as a positive one, to inflict harmful practices as a result. That culture can also leave room for social engineering attacks, as it does not implement personal training or motivation to learn about cybersecurity.

Cybersecurity Findings

Finally, from a cybersecurity perspective, with its focus on the improvement of security controls to better protect devices, it can provide technical reasons as to why people are susceptible to cyber-attacks.

An immediate factor as to why people struggle with cybersecurity and become the largest factor in cybercrime is that they bypass or mitigate the already implemented controls due to a lack of education or incentive to fully utilize them. A security control to start with is passwords. A frequent issue that ends up happening is people having simplified passwords or writing them down on a piece of paper, which bypasses the purpose of that security control entirely. Common examples of information in weak passwords are birthdays and connected names (AlSharif et al., 2022). These pieces of information result in significant breaches due to the ease of connecting

the information with people and gaining access to more sensitive data. According to a study covering data from 2017, it showed that 81% of breaches were from “weak or stolen passwords” (Nobles, 2018). However, even with basic requirements for passwords such as different character types, a minimum number of characters, an expiration date, and password history, they can still end up as too much for people due to an overwhelming feeling of managing a significant amount of randomized information for a single action, or cognitive overload (AlSharif et al., 2022; Desolda et al., 2021; Parsons et al., 2010).

This difficulty with basic security controls then leads into the necessity of user-centric cybersecurity as a potential form of mitigation and how the lack of design is a contributing element to the human factor. Pollini et al. (2022) argue that due to the friction that cybersecurity controls push onto people, which causes them to “actively avoid security mechanisms that are difficult to use, and/or make mistakes that might undermine security,” the proposal is to focus on user-centric design and principles to improve the experience of users and effectiveness of cybersecurity. For example, some features to improve user experience include reducing the cognitive load with cybersecurity controls and interfaces, designing around inexperienced users, making security as efficient as possible, and providing informative feedback, which can significantly reduce user friction by making cybersecurity a more approachable concept to implement into regular behavior. The lack of or late implementation of these kinds of guidelines can result in users perceiving security as a secondary aspect, as well as generating confusion and frustration that may lead to bypassing controls entirely (Nurse et al., 2011).

An additional factor to consider with the human factor of cybersecurity is the level of integration of interdependence. Mittu and Lawless (2015) conducted a literature review that applies interdependence theory to conclude that teams have improved experiences with handling

cybersecurity and regulating cognitive bias due to sharing experiences as a team and offsetting the individual biases that could form. Another study described an assumption of interdependence theory as "a state of mutual dependence between the participants of an interaction affects, or skews, the individual beliefs or behaviors of participants" (Marble et al., 2015). While interdependence theory has the potential to negatively affect people's preferences by enabling harmful behaviors, there is also the potential for positive outcomes through team training (Mittu & Lawless, 2015). Furthermore, the quality of interdependence can also be improved when applied to cybersecurity technologies. According to Pollini et al. (2022), poor interdependence of cybersecurity system components such as "poorly written rules, faulty equipment, poor management practices or unclear procedures" can affect human performance and result in data breaches.

Overall, a cybersecurity perspective shows that the human factor of cybersecurity stems from cybersecurity controls that are either poorly implemented or made too complex for the average person, resulting in a clash that incentivizes people to mitigate their effectiveness or bypass them outright. A lack of user-centric or interdependent design further contributes to the issue by reducing the ease of use and increasing complexity to not account for inexperienced users.

In summary, this literature review found that multiple perspectives can be discovered when it comes to the human factor of cybersecurity, but there is a conflict between the insights. The conflict stems from inherent personality traits, personality traits forming over time, which group of traits has the greater impact in increasing the human factor of cybersecurity, and the need to have complex cybersecurity controls while at the same time making it accessible enough for inexperienced users to grasp. There are research gaps when it comes to including

interdisciplinarity as a factor within the research and the offer of solutions that not only educate people but also those that can become a part of their cognitive behavior. This study will address this gap by integrating the disciplines to address the factors that cause people to have a higher likelihood of being hit with a cyber-attack.

Results

The results of the study show that the factors that cause people to have a higher likelihood of being hit with a cyber-attack are impulsive personality traits, cognitive biases, harmful organizational culture, enabling of poor cybersecurity practices from said culture, and cybersecurity measures that are either poor in quality or too complex for people to easily manage.

The common ground between all found insights is the susceptibility and difficulty of influencing behavior for cybersecurity. To counteract this challenge, I would propose a steady implementation of cybersecurity knowledge through multiple avenues. This would include not only the workplace but also schools and universities. Now, two crucial factors for this approach to be effective are to emphasize information that will help people in daily situations and for both the human and technological aspects to be recognized equally. These strategies, in turn, could result in people having knowledge that feels beneficial to the activities they engage in within a day but also expand on cybersecurity's inherent connections to other disciplines. A practical example is to start with simple exercises like surveys and focus groups to learn about people's knowledge of cybersecurity practices or quizzes to test their ability. Next, basic cybersecurity information can be added to instill knowledge into people's behavioral actions when being online and to eventually become common behavior as well as form networks around cybersecurity knowledge.

Conclusion

In conclusion, the human factor of cybersecurity is a significant issue both within the cybersecurity industry and at a global level. When looking at the cause of the human factor through cybersecurity, while there will be an acknowledgment of both the technological and the human, the latter aspect may be given less weight. Because of this discrepancy, disciplines such as psychology and sociology are critical to understanding the human aspects of the problem as much as the technological ones. From a psychological perspective, people have both their inherent traits and biases that enable them to choose more convenient options when online, risking their security. From a sociological perspective, organizational culture can heavily impact cybersecurity practices and leave people susceptible to cyber-attacks by not training or motivating them to care about cybersecurity. From a cybersecurity perspective, poor and complex cybersecurity controls can contribute to the human factor in different ways by either enabling already present poor practices or generating friction that causes users to bypass them.

To address the difficulty of influencing people to care about cybersecurity practices, a proposed solution for education tailored to average online activities can influence behavior to care for cybersecurity more effectively. Additionally, it can also improve social networks by having that ingrained behavior be an influence on others. While this solution is a potential strategy, due to ever-evolving cyber-attacks and generational changes in behavior, more research should be conducted into this issue.

References

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science & Engineering*, *40*(3). https://www.researchgate.net/profile/Shailendra-Mishra-5/publication/354879445_Impact_of_Human_Vulnerabilities_on_Cybersecurity/links/62849ec22ecfa61d330aa07c/Impact-of-Human-Vulnerabilities-on-Cybersecurity.pdf

American Psychological Association. (2018, April 19). *APA Dictionary of Psychology*. Apa.org. https://dictionary.apa.org/psychology

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), 1-35. https://doi.org/10.1145/3469886

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7). https://www.cell.com/heliyon/fulltext/S2405-8440(17)30998-2

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., ... & Chen, J. (2016, November). Cultural and psychological factors in cyber-security. In Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services (pp. 318-324). https://dl.acm.org/doi/abs/10.1145/3011141.3011165?casa_token=dM2rLOAboCwAAAA:SKb7qx12M_nhjKYS9J7Z1By6QrIseXd3YDSPjwInMiKypmxpjHG47BeEGrZyzyAvMeJ0kC8MGHReA

IBM. (2014). IBM Security Services 2014 Cyber Security Intelligence Index. In *CRN* (pp. 1–12). IBM. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

J. Jeong, J. Mihelcic, G. Oliver and C. Rudolph, "Towards an Improved Understanding of Human Factors in Cybersecurity," 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 2019, pp. 338-345, doi: 10.1109/CIC48465.2019.00047. keywords: {Computer security;Human factors;Bibliographies;Psychology;cybersecurity-human-factors-personality-culture-demographics},

Kadena, E., & Gupi, M. (2021). Human factors in cybersecurity: Risks and impacts. *Security Science Journal*, *2*(2), 51-64. https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/54

Marble, J. L., Lawless, W. F., Ranjeev Mittu, Coyne, J. T., Abramson, M., & Sibley, C. (2015). The Human Factor in Cybersecurity: Robust & Intelligent Defense. *Advances in Information Security*, 173–206. https://doi.org/10.1007/978-3-319-14039-1_9

Mittu, R., & Lawless, W. F. (2015, March). Human Factors in Cybersecurity and the Role for AI. In *2015 AAAI Spring Symposium Series*. https://aaai.org/papers/10248-10248-human-factors-in-cybersecurity-and-the-role-for-ai/

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Nobles, C. & Mcandrew, I. The Intersectionality of Offensive Cybersecurity and Human Factors: A Position Paper. Scientific Bulletin, 2023, Sciendo, vol. 28 no. 2, pp. 215-233. https://doi.org/10.2478/bsaft-2023-0022

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. *2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, 21–26. https://doi.org/10.1109/css.2011.6058566

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment. https://apps.dtic.mil/sti/citations/ADA535944

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://doi.org/10.1007/s10111-021-00683-y

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June). Human factors in cybersecurity: a scoping review. In *Proceedings of the 12th International Conference on Advances in Information Technology* (pp. 1-11). https://doi.org/10.1145/3468784.3468789

Singh, B., & Cheema, S. S. (2024). Psychology in Cybersecurity: Unveiling the Human Dimensions of Digital Resilience. *International Journal of Advanced Networking and Applications, 16*(1), 6281-6290.

http://proxy.lib.odu.edu/login?url=https://www.proquest.com/scholarly-journals/psychology-cybersecurity-unveiling-human/docview/3086409290/se-2

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, 100126. https://doi.org/10.1016/j.chbr.2021.100126