Annotated Bibliography: Social Science and Cybersecurity

Amira Muaket

Old Dominion University

CYSE - 201

Professor: Matthew Umphlet

June 23rd, 2024

Annotated Bibliography

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. Computer Systems Science and Engineering, 40(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938

The authors of this article express how human error and other factors contribute to cybersecurity vulnerabilities. As technology advances the authors point out that there's been an increase in cybercrime such as security risks and cyber-attacks, including viruses, the internet, communications, and hackers, due to human error and other factors. “It is observed that more than 39% of security risks are related to the human factor, and 95% of successful cyber-attacks are caused by human error, with most of them being insider threats.”(Alsharif, Mishra, Alsheri, 2021 pg.1153). With that said, they conducted a research methodology by collecting data using online questionnaires revolving around the idea of awareness of cybersecurity. They used female and male candidates and categorized them by age (teens, adults, and seniors). The main categories they used to ask their questions were social engineering & social media, phishing emails, and passwords. The results concluded that there was a significant lack of awareness regarding vulnerabilities and cybersecurity, as well as poor security practices. Relating this to the social science of cybersecurity, we can examine how there's a need to exercise education and training on the matter of cybersecurity. In addition, as a society, we need to implement stronger policies and a better understanding of cybersecurity practices and frameworks. Thus focusing on the law, education, and anthropology. Overall, the authors stress that minimizing or fixing human errors is one of many ways to improve cybersecurity.

Moustafa AA, Bello A and Maurushat A (2021) The Role of User Behaviour in Improving Cyber Security Management. Frontiers in Psychology. Volume 12

https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.561011/full

The authors of this article wanted to address how adopting appropriate online behaviors can contribute to improving cybersecurity as a whole. They provide certain practices and frameworks that users can integrate into their daily routines while highlighting common flaws in human behavior when engaging online. Also, the article points out why certain behavior is displayed when engaging online due to certain psychological factors. The article first expresses the importance of complying with security policies as it is one of the key behaviors to enforce on users so they can protect their networks and computers. Then provides an extensive report of the top human errors that occur, which include falling victim to phishing, sharing passwords, and failure to update systems. This can happen due to cognitive and behavioral traits such as procrastination, future thinking, risk-taking behavior, and impulsivity. Once those are addressed the authors wanted to provide a way to improve security behavior by using psychological methods to encourage safety when engaging online. These consist of using novel polymorphic security warnings, rewarding and penalizing good and bad cyber behavior, and increasing thinking about future consequences of actions. Relating this to the social science of cybersecurity we can understand how certain behaviors and actions can affect cybersecurity policies and enforcement. It also allows us to understand why human error may occur due to certain psychological traits. Overall, the author wanted to implement and address personality traits and cognitive behavior in cybersecurity frameworks.

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences, Volume 12. https://doi.org/10.3390/app12052589

The author of this article wanted to observe and understand cybersecurity awareness among university students. He wanted to comprehend the level of security knowledge among these college students at Imam Abdulrahman Bin Faisal University by conducting a research case study. By providing an assessment comprising 15 questions of cybersecurity awareness to students regardless of gender and demographic, using three essential categories: password security, browser security, and social media security. While examining certain factors of how aware university students are about cybersecurity, such as education level, understanding and experience with cybercrime, and students' knowledge of cybersecurity. The research had over 450 candidates and concluded that the primary issue was a lack of awareness when it came to passwords, but browsing security and social media security were a good standing when the majority were aware and understood the importance of cybersecurity regarding those categories. “The knowledge about student password security in this study is still deficient. Students usually do not pay much attention to using good and correct passwords to protect their accounts or websites.” (Alqahtani, 2022) Relating this to social science in cybersecurity it examines the importance of education when wanting to implement cybersecurity practices and methods. While expressing sociological and psychological influences on students with their knowledge of cybersecurity. Overall, the author expresses having good cybersecurity relies on effective security awareness training and programs.

Salam A, & Mohammad A, (2023). Safeguarding Media Integrity: Cybersecurity Strategies for Resilient Broadcast Systems and Combating Fake News. Unique Endeavor in Business & Social Sciences,. https://unbss.com/index.php/unbss/article/view/35

The author wanted to place importance on safeguarding media integrity, by focusing on ways to implement cybersecurity strategies on broadcasting systems while combatting various methods in avoiding the spreading of fake news. This article wanted to provide effective measures to broadcasters, policymakers, and cybersecurity professionals to aid in preserving the authenticity and reliability of media and news. The article comprised a mixed-method research approach by conducting a pre-test and a post-test of various employees from different media organizations, including journalists, editors, and IT staff. The pre-test was created to gain knowledge of employees' understanding of cybersecurity policies. Once that test was done, they decided to implement a cybersecurity training program covering topics such as phishing awareness, password security, and data protection best practices. Then conducted a post-test about the material and compared the results. The pre-test showed extremely low scores regarding cybersecurity awareness, but with proper training, the post-test produced significantly high scores in the improvement of media awareness and behavior regarding cyber threats/attacks and cybersecurity. Relating to social science in cybersecurity, we can understand how policies and education a key components when addressing cybersecurity frameworks. As it proves effective measures in protecting the integrity of online and broadcasting media. We can also view how psychology plays a vital role when wanting to encourage companies and employees to implement rigorous cybersecurity training programs to safeguard against any potential breaches while maintaining integrity.