Article review: Cybersecurity when working from home during COVID-19: considering the human factors

Alan Schneider

Department of Cybersecurity, Old Dominion University – Norfolk

CYSE201S: Cybersecurity and Social Science

Matthew Umphlet

29 March 2024

The article I reviewed discusses whether individual cybersecurity behaviors were affected due to working from home during the COVID-19 pandemic When considering the articles relation to social science principles, (Whitty et al., 2024) the principle of relativism is applicable. Research conducted before the COVID-19 pandemic found that seventy five percent of businesses and thirty-eight percent of organizations had no explicit cybersecurity policies that employees were directed to follow when working from home (Pranggono & Arabo, 2020). Resulting in in an increased risk of breach affecting both the employee's organization and potentially exposing employees private and financial data. This leads to the conclusion that poor planning and policy direction on behalf of the organization is related to increased cyber risk for both employer and employee and mirrors the social science principle of relativism. The second principle is parsimony, while the authors used a social constructionist lens to frame how individuals adopt effective cybersecurity practices. The idea of lived experience influencing good or bad cyber hygiene was simple to understand and relate to. In the next paragraph I will discuss the research question the authors are looking to answer.

The articles abstract is framed as follows: "To examine the lives of Australian employees who moved to work from home during COVID-19 in an effort to gain insight into the intermingling of individuals' personal lives and technology to inform policies and educational programmes." (Whitty et al., 2024) The research questions were as follows. What were participants' lived experiences when transitioning from the office to home, and how did these impact cybersecurity learning and behaviors? What did cybersecurity mean for participants when working from home? How did participants learn about cybersecurity when working from home? What recommendations might we give to organizations based on our findings? The study found:

“that psychological (e.g. stress, anxiety, confidence, motivation) and sociological (e.g. sharing physical spaces, digital divide) factors impacted employees’ likelihood and ability to engage in effective cybersecurity practices. So, did new ways of using technology (e.g. teaching via Zoom), which elucidated unexpected but significant security concerns (e.g. naked children in virtual classrooms) (Whitty et al., 2024).” What kind of research methods were used by the authors to answer this question?

The type of research authors employed was an interpretative phenomenological analysis to understand twenty-seven participants’ lived experiences under lockdown. IPA analysis looks at how participants make sense of their world and what that experience means for them. With the type of research method in mind, what were the types of data and overall analysis done on the data? Data was collected through interviews conducted with twenty-seven Australian employes ranging from twenty-five to seventy-two years old. Sixty seven percent of the sample were men, and thirty four percent were women ranging in across multiple work sectors ranging from IT services and public relations to marketing, fundraising and financial planning, with the only commonality being that each participant had been working in an office environment before the pandemic and were required to work from home during the pandemic. Using a specific set of questions: “How did the participants experience the transition from the office to working from home? What does ‘effective cybersecurity behavior’ mean for participants, especially when working from home? Did participants experience any threats or attacks, and how did they deal with them? What type of advice/information (if any) was given to them to work securely at home? How did participants interpret the advice, and how easy or difficult was it to implement?” (Whitty et al., 2024) the authors were able to create a table of themes both superordinate and emergent themes to extract meaning of the participants experience.

So, with the types of data and data analysis in mind are their concepts discussed in class that can be related to the article? The first concept that comes to mind are that incorrect perceptions of safety combined with if assumptions that technology will keep the user safe in the absence of proper guidance and training can increase the risk of cyber victimization. The article captures that complex cybersecurity behaviors and practices needs to be taught well before any crises (such as the pandemic) due to the difficulty in learn new practices during times of stress. The second concept would be recognition and understanding of what social engineering is, what are some common types of social engineering attacks and how to recognize them. This concept becomes especially relevant when considering the increase in COVID-19 related social engineering scams targeting remote workers during the pandemic. The article concludes that cyber professionals must translate complex cybersecurity concepts and messages into a form of content that's understandable and executable to those who don't have the same training and technical expertise.

This article does not have a direct relation to the challenges, concerns, and contributions of marginalized groups, although the challenges of shared working space with family or roommates and greater difficulty separating work and home life creating greater stress conditions are factors that can affect individuals regardless of demographic. However, the article could also provide guidance to cyber professionals when considering best practices to apply to caregivers or housebound individuals unable to return to or participate in an office environment. Finally, the article contributes to a growing body of knowledge related to remote work and proper cyber training and awareness. It additionally provides an important perspective of the driving forces behind online behaviors of remote workers. Providing a platform in which future training and

awareness policies are designed with a more tailored approach instead of a one six fits all mindset seen in other organizations remote work policies and strategies.

References

Whitty, M. T., Moustafa, N., & Grobler, M. (2024b, January 24). *Cybersecurity when working from home during COVID-19: Considering the human factors*. OUP Academic. https://academic.oup.com/cybersecurity/article/10/1/tyae001/7588826

Pranggono, B., & Arabo, A. (2020). covid-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247