Article Review #1: Analyzing a study on cybersecurity practices for remote workers

Cali J. Zuk

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Mr. Diwakar Yalpi

October 2, 2024

Overview

The focus of this article review is a paper first published in the *Journal of Cybersecurity,* titled “Cybersecurity when working from home during COVID-19: considering the human factors”. The research was initiated in response to trends noted during the COVID-19 pandemic. It attempts to describe from a psychological and sociological perspective the issues faced in ensuring a cybersecurity culture during the massive shift of office work from primarily in person to remote (Whitty et al., 2024). Work from home presented many issues to employers due to the loss of control over both the employees’ working space and their information systems. An example of this is the variable responses to cybersecurity training that can be observed in the workplace; some employees take their security training very seriously and others may leave them playing in the background while doing other activities. This experience is therefore different than that of training conducted in a face to face office environment. The researchers were attempting to answer questions regarding the lived experiences of remote office workers, evaluating how they maintained cybersecurity when switching to remote work, analyzing how they were trained and learned about remote cybersecurity, and using these experiences to make recommendations for policy makers (Whitty et al., 2024, p. 2).

Method Review

The researchers had a sample size of 27 participants drawn from a representative pool of office workers in Australia who had been forced to switch to remote work (Whitty et al., 2024, p. 3). The study used a series of semi-constructed interviews with each participant, the responses were then subjected to a theme analysis utilizing the approach called interpretive phenomenological analysis or IPA for short. This method allows researchers to focused on lived experiences and in combination with a focus on learning rather than practice, means that

researchers can try to highlight challenges that may not have been considered by traditional information security practitioners. IPA utilizes analysts called coders who create charts with emergent themes from the interviews on one side and then superordinate themes or categories/groupings of related themes on the other (Whitty et al., 2024, p. 3). The superordinate themes create common areas of frustration across the lived experiences of all remote workers while the emergent themes describe the individual experiences and frustrations felt by the participants.

Analysis

The themes the researchers found reflected several areas of frustration that many people who worked during the pandemic likely felt. The researchers identified five superordinate themes that affected cybersecurity hygiene of transitioning office workers; summarized in Table 1 as: “Transition from the office to home”, “Working space at home”, “Understanding of cybersecurity”, “Awareness and education”, and “Digital Limitations” (Whitty et al., 2024, p. 4). Each of the themes presents a potential source of further research and policy advice. For example, “Digital limitations” is largely comprised of issues that can be resolved with technological changes, such as upgrading a worker’s computer or providing assistance to employees in upgrading their internet service. Other issues such as the ones deriving from the rough transition from a physical office to a home office may be addressed by wider culture changes. Likewise, addressing issues with the actual working environment may be solved by creating 3rd spaces for employees or having flexible work arrangements in the post-COVID working environment that allow employees to return to offices or shared office spaces that provide better working conditions. The themes identified not only extend to cybersecurity but also touch into arenas of social justice and technological accessibility not often considered by

policymakers. Further research in those arenas using the same methodology may also reveal actionable insights.

Conclusion

The identified themes in the study provide strong starting places for employers to create better environments for more secure remote work. The kinds of changes required however, will evidently cost money, whether that is from hardware and software costs to upgrade deficient technology, schemes to reimburse workers for the cost of internet service upgrades, or maintaining expensive office space with low occupancy rates. Many employers will not want to pay these costs despite the benefits that remote and hybrid work deliver to workers, and this is apparent in the widespread return to office orders that companies have issues to employees since the conclusion of the federal state of emergency. The benefits of remote work with the right modifications and employer support are vast, one being the increased accessibility of the creative economy to poor and rural people, two marginalized groups that may struggle to achieve the kinds of high income associated with those jobs. While these groups struggled in the beginning of the pandemic due to lack of broadband access and job market proximity; the shift to remote work extended an arm to them that the broad return to office mandates threaten to take away again. Companies that continue to allow for remote work while addressing the concerns found in the superordinate themes identified by the researchers will continue to have access to a broader workforce while allowing marginalized groups to maintain a lifeline of social mobility.

Works Cited

Whitty, M. T., Moustafa, N., & Grobler, M. (2024). Cybersecurity when working from home during COVID-19: Considering the human factors. *Journal of Cybersecurity, 10*(1). https://doi.org/10.1093/cybsec/tyae001