Hans Peterson

CYSE 201S

3/24/2024

Article Review 2

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

One of the social principles that is present in the article is parsimony; the researchers organized their findings into themes/subthemes. Within the subthemes, the researchers summarized the interviewees' disorganized, casual responses toward the interview questions, which provided clarity. Another social principle present in the article is empiricism. Throughout the article's results, there are transcriptions of interviewees' responses; these responses were then used to inform the recommendations that organizations/companies should take, such as the need to understand their workforces' psychological state. Another social principle present in the article is ethical neutrality. Before the study, researchers gained an ethics clearance. Also, the participants were asked for their consent in their interviews, and their names were kept anonymous (Ex. Participant 16).

There were no hypotheses, but there were research questions. Essentially, the researchers inquired about the interviewees' experiences in transitioning from the workplace to home during the COVID-19 pandemic and its impact on cybersecurity learning and behavior. They also asked participants how they understood cybersecurity and how they learned it while working at home. Lastly, the researchers would use their findings to provide recommendations to organizations.

Researchers used qualitative methods (semi-structured interviews) to conduct research. Specifically, they used interpretative phenomenological analysis (IPA), which focuses on

participants' experiences of their world and how they make sense of it. Researchers also used a hermeneutic approach, which focuses on reinterpreting data multiple times to hone the themes.

This study used recorded, semi-structured interviews to collect survey data from 27 Australians spread out across Australia. The interviews used open-ended questions to collect data, which were participants' personal experiences. It focused on their experiences, as they were unique and helped inform specific recommendations, such as how cybersecurity practices should be taught due to a workforce's varying levels of motivation. Research honed in on how culture clashed with cybersecurity practices.

One of the concepts present is human factors. In the article, cybersecurity training was found to be dull. The failure of organizations to consider how their workforce would react to training led to a failure in their workforce learning cybersecurity. Had training been personalized or made engaging, workers might consider learning cybersecurity practices. Another concept present is awareness of cybersecurity. In the article, the workforce lacked understanding of cybersecurity, and they viewed cybersecurity as an enigma. This lack of knowledge leads to weaker organizational cybersecurity, which is why training is crucial. This brings up another concept: cyber victimization. If staff are not knowledgeable in cybersecurity, they may use risky practices, increasing their chances of victimizing themselves. In the article, one of the participants assumes that they would not be a target of cybercrime because they are not protecting anything important. Another concept present is research methods; surveys were used to collect data, and throughout the article are survey responses that were used to inform the themes.

Marginalized groups like people in poverty could be more susceptible to cyber attacks. In the article, some of the participants had old equipment, shared devices, and poor internet connection. Old equipment could be susceptible to unpatched vulnerabilities, and family members and friends could access confidential information on work devices at home. Another marginalized group are seniors. The abrupt transition from workplace to home due to COVID-19 may have forced them to use newer technologies they were not accustomed to. As a result, their productivity and cybersecurity posture were stunted.

One of the article's major contributions was the recommendation for organizations to properly educate their employees; specifically, they should not use a one-size-fits-all approach since employees have varying levels of cybersecurity comprehension. Another contribution of the article was the recommendation for organizations to understand the limitations of home settings; these home settings are not always productive, especially in the case of employees with large families. They may also compromise cybersecurity and put employees in mental turmoil.

Link to article:

https://academic.oup.com/cybersecurity/article/10/1/tyae001/7588826?searchresult=1

Class resources used:

Module 2 powerpoint: Principles of Social Science and Cybersecurity

Module 3 powerpoint: Strategies to Study Cybersecurity through an Interdisciplinary Social Sciences Lens

Module 4 powerpoint: Cybersecurity and Human Factors

Module 5 powerpoint: Applying Psychological Principles of Cyber Offending, Victimization, and Professionals

Module 6 powerpoint: Psychology Research, Human Factors, and Cybersecurity