OPEN ACCESS

Journal of Advanced Research in Social Sciences
ISSN 2538-919X

Cybersecurity Concerns & Teleworking in the COVID-19 Era: A Socio-Cybersecurity Analysis of Organizational Behavior

Carlene Buchanan Turner[1*], Claude Turner[2], and Yuying Shen[1]

[1] Sociology Department, Norfolk State University, Virginia, USA
[2] Computer Science Department, Norfolk State University, Virginia, USA

ARTICLE INFO

Keywords:
Teleworking
Cybersecurity
Predictability
Efficiency
Interviews

ABSTRACT

This research project examines the relationship between teleworking cybersecurity protocols during the COVID-19 era and employee's perception of their efficiency and performance predictability. COVID-19 is the infectious disease caused by the most recently discovered coronavirus and it has been declared a pandemic by the World Health Organization. Since March 2020, many employees in the United States who used operate onsite, have been working from their homes (teleworking) to mitigate the spread of the virus through social distancing. The premise of this research project is that teleworking can transform these employees into unintentional insider threats or UITs. Iinterviews were conducted through video conferencing with nine employees in Virginia, USA to examine the problem. This is an interdisciplinary research project which brings together the disciplines of sociology and computer science. Narrative Analysis was used to unpack the interviews. The major findings from the research efforts demonstrate that employees are trusting of the cybersecurity protocols that their organizations implemented but they also believe they are vulnerable, and that the protocols are not as reliable as in-person working arrangements. While the respondents perceived that the cybersecurity protocols lend to performance predictability, they seem to think it disrupts their efficiency.

1. Introduction

This paper examines the relationship between employees' perception of their efficiency and performance predictability as a result of their organization's teleworking cybersecurity policies in the COV-19 era. The research is based on a socio-cybersecurity project. Socio-cybersecurity is defined as the social and cultural aspects of cybersecurity (Buchanan Turner & Turner, 2019; Turner & Turner, 2017). Within the emerging discourse there is a focus on the social problems of information assurance, the socio-psychological implications particularly for criminal justice, its role in modern bureaucracies and institutions, and the position of big data and research methodology in cybersecurity. The focus of this investigation is examining the role of cybersecurity in organizations as they are thrust into a teleworking arrangement because of the 2020 COVID-19 pandemic. The two research questions that are examined in this paper are: How is employees' efficiency impacted by an organization's cybersecurity policies in the COVID-19 pandemic era; and what is the relationship between the stringency of cybersecurity protocols within an organization and employees' teleworking predictability in responding to any security vulnerabilities? This is an exploratory research project as the COVID-19 pandemic is still unfolding across the world at the time this paper as written.

* Corresponding Author E-Mail Address: cmturner@nsu.edu

According to the World Health Organization, COVID-19 is the infectious disease caused by the most recently discovered coronavirus. This new virus and disease were unknown before the outbreak began in Wuhan, China, in December 2019. WHO defines a pandemic as the worldwide spread of a new disease (www.who.int). Pandemics cover the outbreak of an