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[3]
[1]Sociology Department, Norfolk State University, Virginia USA
[2] Computer Science Department, Norfolk State University, Virginia USA
[3] Sociology Department, Norfolk State University, Virginia USA

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 a UITs. Interviews 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.

Keywords: Teleworking, Cybersecurity, Predictability, Efficiency, Interviews.

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.

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 infectious strain among human across vast geographical areas (Husin, 2009). The Governor of the Commonwealth of Virginia declared a state of emergency because of the pandemic on March 12, 2020. The declaration implemented telework policies for state employees (www.governor.virginia.gov). Effectively, millions of American workers and employees across the world, started doing their jobs remotely from their homes using computer and internet access. This project will examine how this new social dynamic is shaped by cybersecurity protocols.

This research focuses on the efficiency and predictability criteria in the George Ritzer's McDonaldization framework, a sociology of organization theory. The research questions examine if efficiency (defined as the most optimal method for getting work done) and predictability (defined as the assurance that product and services will be the same over time and locales) are impacted by the restructured cybersecurity protocols.

2. Background

2.1 Literature Review

2.1.1. Pandemics

A pandemic on US soil is a novel reality for most Americans. Fighting a pandemic is erroneously perceived as something that happens in 'exotic' places like Africa. For example, the HIV/AIDS pandemic was seen as an African problem. "During his campaign for president, George W. Bush said that even though it was 'a country with many problems', Africa was not an area of strategic importance to the US" (Smith, 2004), so the pain of that pandemic was not seen as an American problem. This demonstrates that Americans may have a hard time seeing the corona virus as an everyday reality. Therefore, Americans may not have the easiest time adopting their individual liberties to living with a pandemic at their doorsteps.

Pandemics are usually understood as third world phenomena by many epidemiologists, public health practitioners, virologists, and yes sociologists. Acceptable discourse around pandemics would be situated in an African or Asian milieu by people outside of the Centers for Disease Control. For example Tamba M'Bayo's (2015) article explaining that the 2015 Ebola outbreak in Sierra Leone cannot be "divorced from the chronic issues of poverty, economic inequity, and social injustice that have been the bane of the country's lopsided development" (M'bayo, 2018, pg. 101) seems quite plausible. The American marketplace does not think of itself in this way (even if these conditions exist in America) so the COVID-19 pandemic was a cultural shock to the white-collar workforce, the group examined in this article

2.1.2 A Teleworking Economy

In early 2020, the pandemic impacted the working conditions of millions of Americans swiftly and without warning. Not only were many onsite employees forced to start working

from the security of their homes (teleworking), some employees started to operate in worksites reconfigured by public health concerns, and many others lost their jobs. These new realities are new for public health practitioners and epidemiologists because the HIV/AIDS pandemic for example, did not radically change the workplace like the COVID-19 pandemic.

Sociologist routinely advance that crises will shift the way the world economy works. For example, Giddens (2009) said that the 2008 economic crisis necessitated a new responsible brand of capitalism. Whenever there is an economic crisis (such as the unemployment rate in the USA rising to 11%) sociologists will say things such as "crises necessitates the development of fundamentally new ideas and concepts; they require new ways of relating citizens to markets, markets to states, and states to their citizens" (Giddens, 2009, pg. 205). Although Giddens was talking about the global climate change crisis, this is also applicable to a pandemic. In 2020, the novel corona virus (COVID-19) reshaped the economic field, with teleworking becoming a reality for a significant proportion of white collar workers.

The Asian marketplace has been investigating the impact that a pandemic can have on the economy for sometime now. These investigations have conculded that "a regional or global pandemic could last between 12 and 18 months" (Husin, 2009, pg. 84). The SARS (severe acute respiratory syndrome) epidemic for example, demonstrated to SouthEast Asian economies the need to prepare for fallouts impacting the health of the workforce.

The epidemiological community in the United States has also warned of the arrival of a pandemic on the US shores. In a 2008 analysis, Barlett and Borio detailed five major recommendations from the Centers of Disease Control for such an eventuality. Two of these recommendations are: (1) the voluntary home quaratine of uninfected contacts, and (2) the closure of businesses while maintaining most essential services. Additionally, in their analysis Barlett and Borio (2008) said that the US has had opportunities to prepared for a widespread pandemic. The anthrax outbreak of 2001 and Hurricane Katrina 2006 were two such events.

Alternative work schedules are becoming more popular in the modern American workplace. Teleworking (defined as work schedule where the employee completes official duties at home) is one such arrangement. In a research project on workers' turn-over and satisfaction with telework arrangements, Lee and Hong (2011) pointed out that teleworking is usually attractive to employees that have caregiving responsibilities at home. However, the COVID-19 pandemic has layered another variable in the decision to telework. Fear of contracting the disease and the need to social distance from fellow employees and customers (Barlett & Borio, 2008) is a major impetus for embracing telework. The major take-away from the Lee and Hong (2011) research project, is that employees who are afforded teleworking opportunities tend to percieve their employers as supportive, and in turn, they become more committed to their companies productivity.

2.1.3 Cybersecurity Concerns

The premise of this research is that with more employees migrating to a teleworking arrangement, organizations will become more susceptible to cybersecurity attacks. In a preliminary analysis of COVID-19 and terroristic vulnerabilities, Ackerman & Peterson (2020) posit that cyber-attacks could take several forms. A major form of incursion could include ransomware attack to disrupt the critical response infrastructure of hospitals. With the movement of almost every kindergartener through university student to online learning in the USA because of the COVID-19 pandemic, vulnerabilities were exposed in the e-learning platform. For example, in Norfolk Virginia, a 'Zoom' class room was hijacked and inappropriate material was shared with minors (Mayfield, 2020). These exploits are called

'zoom bombing' and are performed by uninvited 'party crashers.' In April 2020, the Federal Bureau of Investigation (FBI) reported that there was an increase in cybercrime since the declaration of the coronavirus pandemic in the USA (Cimpanu, 2020). Cybercrimes seek to attack the vulnerabilities exposed by the pandemic, not just through ransomware, hacking, and phishing, but through other means such as social engineering. The FBI has documented cybercriminal efforts at establishing fake COVID-19 charities, or establishing a fake personal protective equipment (PPE) delivery company, and other efforts aimed at exploiting anxious consumers (Cimpanu, 2020).

While teleworking may provide knowledge workers with the opportunity to social distance during the COVID-19 pandemic, it can also transform the worker into an unintentional insider threat or a UIT (Mehan, 2016). In cybersecurity, an unintentional insider threat occurs when a good employee "accidentally jeopardize security through unintentional data leaks or other errors" (Mehan, 2016, pg. 81). An organization only needs one unintentional inside threatened employee to be vulnerable.

Organizations' IT departments are usually efficient at protecting their online infrastructure onsite. However, social distance protocols have resulted in many operations that do not require physical manipulation (primarily jobs in the knowledge sector) to move to a teleworking environment. The a priori assumption may be that IT departments will lose control of their internet operations. However that may not be so. The COVID-19 teleworking environment may have resulted in extra vigilance by IT staff. Organizations that allow their employees to work from home have opted to utilize virtual private networks (VPN) as they secure the organization's internet traffic (Zur, 2020). The layer of security that VPNs offer, by obscuring employees actual location and IP addresses is worth the investment for some organizations. The existing literature (albeit limited) points out that there are still VPN vulnerabilities. Unintentional insiders can be phished through email, or organizations may not invest in the latest update or patches which may result in hackers infiltrating their systems (Zur, 2020). The reviewed literature offers an informed platform to conduct exploratory research on how a new panademic reshapes teleworkers and the cybersecurity infrastructure required to guarantee them efficient and predictable perforamnce.

2.2 Theoretical Framework

The research project is grounded in a social organization theory. The McDonaldization of Society theory by Ritzer (2019), which emanates from classical Weberian bureaucracy theory forms the theoretical base of the project. The theory allows for the analysis of the effectiveness of cybersecurity in today's organizations in terms of efficiency and predictability (Ritzer, 2019; Ritzer & Jurgenson, 2000; Weber, 2003).

Ritzer used McDonalds fast-food restaurants as the models of rationality in the 21st Century. These franchised operations embody formal rationality, because they are reliable, affordable, increasingly technological, and readily recognized as a modern institution. The definition of the McDonaldization theory is the evidence of rational operations in modern organizational bureaucracies, based on the precepts of (i) efficiency, (ii) calculability and (iii) predictability (Ritzer & Stepnisky, 2017). In many organizations during the COVID-19 pandemic, it will be assumed that most employees interact with the cybersecurity demands in a similar manner.

In a non-pandemic society, should an organization require all sales personnel to be re-certified in cybersecurity norms annually then that would be evidence of Ritzer's three prong

rationality. The required certificate would signify efficiency, predictability, and calculability. In an emergency such as the pandemic, it is as if the McDonald store was operating with primary reliance of non-human technology (Ritzer, 2019), and probably with just two human being onsite (everyone else working offsite). How then will the unit maintain efficiency and predictability? The proposed research intends to focus on the efficiency and predictability criteria in the Ritzer's framework.

The McDonaldization theory was also used to conceptualize the variables efficiency and performance predictability which are core in the project's research questions. Efficiency refers the most optimal method for getting work done, while performance predictability refers to consistent product and service delivery even if most employees are teleworking. The theory was key in framing a discussion of employees' perception of the cybersecurity protocols that were required as they teleworked.

3. Methodology

Qualitative video conferencing interviews (Zoom) were used to collect data from nine employees from the community around the university. The data from the interviews was the analyzed using Narrative Analysis to unpack some of the common themes from the interviews, by demonstrating the respondents' rationalize their perceptions (Schutt, 2019). In-depth qualitative interviews were used for this exploratory research because the phenomena of cybersecurity layered on to teleworking for organizations is novel. They aim is to gather data to situate this new reality in the interdisciplinary nexus of socio-cybersecurity, rather than to generalize to the wider population at this time.

The target population of this research were employees from companies in the city of Norfolk, Virginia as this was a Social Organization of the workplace project. The respondents came from the private and public sectors, the military and academia. The limitation of having a small non-probability sample was balance by having a diverse group of respondents. In terms of demographics there were: three Black women; one Black man; one Asian woman; one White woman; two White men; and one Latina woman. They were also varied in terms of age. Two respondents were under 30 years old, two were between 30-35, and five were between 40-45. The educational level varied as well. One respondent had a high school diploma, three had bachelor's degrees, three had master's degrees, one had a doctoral degree, and one respondent did not disclose.

Convenient sampling was used to recruit the research participants. The parameter of the non-probability sample afforded the recruitment of a mixture of employees and supervisors. The sample was drawn from the university's catchment area the city of Norfolk, Virginia. The demographic characteristics makes this city an ideal site for the research project. According to the American Fact Finder, the population in 2010 was 242,803; the civilian labor force is 111,290 (Norfolk Development, 2015); and Norfolk is the home to the world's largest naval complex with 23,601 armed forces employees (Norfolk Development, 2015). The median age is 30.6 years; and it is also a diverse city as 47% are white and 43% are black (American_FactFinder, 2010). The voluntary consent of all participants was ascertained. They were advised that the information collected from them will be anonymized and will also kept confidential by the project's PI. Permission was ascertained to audio-record the zoom interviews (only the interviewer's face was visible).

In operationalizing employees' efficiency and performance predictability because of the cybersecurity policies implemented during the COVID 19 lock-down in America, seventeen

open-ended content questions and five demographic questions were asked. Five of these questions were: (1) Were extra cybersecurity protocols required for teleworking in the COVID-19 era; (2) Has teleworking made us more vulnerable; (3) Should teleworking protocol continue after the lock-down; (4) How do you feel about teleworking; and (5) Which employees were more vulnerable to attacks? These indirect questions were geared at asking employees how the cybersecurity shaped their performance and impacted their efficiency.

4. Results

The findings from this exploratory research was presented using Narrative Analysis. Therefore, original quotes are present in the results section so that the impact of the subjects' responses are capture by the reader. The data from the interviews were helpful in exploring the research questions. For the question about the impact of cybersecurity protocols on employees perceived efficiency and performance predictability, the respondents first detailed the extra protocols their organizations required for teleworking in the COVD-19 era. The responses fall into non-cybersecurity categories such as those required by the Centers of Disease Control (mask, social distancing, temperature checks, etc.), and cybersecurity responses. Some of the cybersecurity-based answers seem to contradict efficient and enhanced performance. For example, one respondent said,

> *"Onsite you can just go sit and log unto your desktop. With COVID-19 you may need to go through three different channels to get to your desktop. However, the remote desktop gives you more secure tunnels to work in."*

The respondents describe the frustration of the extra steps but agreed that while it may slow the user down at first, it contributed to more predictable performances because threats are controlled.

With the abrupt transition to teleworking in March 2020, some companies were caught unprepared and some employees untrained. This contributed to the initial problems with being efficient and having positive predictable performances. A respondent detailed the following experience,

> *At first, people had to go with what they had. But once the issues were recognized then extra protocols began to be added. My organization bumped up things with more bandwidth. They also provided more training for us so we could continue to work at home.*

The elementary school teacher in the sample responded that predictable performance was impacted because of uncertainty about engaging students. She had the experience of having inappropriate pictures shared in her online classroom. She opined that this could not have happened if the class was being conducted face-to-face. She believes that this has made her more wary of her performance as the monitor of her classroom environment because she does not want to be the cause of an unintentional attack on her students.

Preliminary results from the in-depth interviews revealed that there were mixed reactions to the question of whether teleworking has made us more vulnerable. Three of the respondents said 'yes.' A government auditor responded that

> *"Many people have never teleworked. Employees and companies are figuring out the kinks as they go along. But hackers have been preparing for situations like these for a long, long time."*

Two of the respondents were not sure if we are more vulnerable, two did not offer a response, and the final two said no to this question. Respondents explained their negative response by saying with proper training, cybersecurity vulnerabilities can be reduced, and that companies I.T. departments are astute at covering all bases. The research teams' analysis of the results therefore is that more training needs to be put into place so that employees can understand and accept their roles in making their place of employment more secure.

Respondents were also asked if the COVID-19 teleworking protocols should remain after the lockdown and seven of them said yes, while two said organizations should return to 'normal' operations. The most popular reason for yes was opined by a respondent as follows,

> *"These protocols show companies the amount of work that can be done outside the office and the productivity that can be achieved outside the office. Going forward, they can be good for emergencies such as a snow day."*

Based on responses such as these, it seems that employees believe that they can achieve the same productivity (or even greater) teleworking than they can on their organization's compound.

Overall, employees' responses to the question 'how do you feel about teleworking' during the COVID-19 era were mixed. Of the eight responses to this question four said they enjoy it, like it, love and it works for me. A managerial level employee said,

> *"I enjoy it. It saves me on gas. It cuts down my commuting. I stay more organized. And it allows me to balance my family life better."*

However, four respondents were ambivalent about it. Saying, it was not great in the beginning, it has its plus and minus, it has its advantages and disadvantages, and its ok for an unfortunate situation. It was also pointed out that the lack of face to face contact can cut down on efficient communication as you may not be able to ask a co-worker 'but what do you mean' without going through 27 other people. It can therefore be concluded that the COVID-19 protocol for teleworking did not thwart employees' productivity but there were some weaknesses in the application of a wholescale remote workplace during this pandemic.

Finally, most of the respondents believed that anyone can be vulnerable to a cybersecurity attack while teleworking. A respondent opined that with a phishing attack there is a 100% chance of it working. It just depends on the user. Other responses were, older employees, because they are less aware, or another said younger workers because they are always surfing the web. Another respondent believed that managers are more vulnerable because they have access to more sensitive information as opposed to another respondent who said employees with top level security clearance were more secure because they were more vigilant. The exploratory nature of this research produced many interesting ideas from a small group of respondents, further research with a representative sample, and after the COVID-19 era has ended could result in more generalizable results.

Discussion and Conclusion

The most significant findings from this research is that employees are trusting of the cybersecurity protocols that their organizations implemented during the COVID-19 socially distanced teleworking era. However, they were more ambiguous about their efficiency and performance predictability. While employees trust VPNs and teleconferencing platforms, they believe they are vulnerable and not as reliable as more in-person working arrangements.

Ritzer's McDonaldization of Society (2019) is helpful in framing the perception of the respondents. In terms of efficiency (the optimal method of getting tasks accomplished), the respondents perceived that their organizations attempted to maintain this status. This aligns with the idea that teleworking shows how much work can be done off-site. However, at the beginning of the mass movement towards teleworking, employees also realized that their organizations had much work to do to be efficient. It was pointed out that employees first started working with what they had until the companies later added the necessary cybersecurity protocols.

In terms of perceived efficiency, not having to commute or being in a noisy office, means that employees have more time to commit to the job and they have less distractions from colleagues. While these are non-cybersecurity measures, they are possible it the worker is assured they have a safe network to stay at home.

Performance was not as predictable during teleworking, however. Predictability is the assurance that product and services will remain the same over time and locales. If teachers e-classrooms are vulnerable to hackers with inappropriate pictures, then there is a problem. Also, if electronic communication slows down productivity as opposed to getting a quick response from a colleague face-to-face, then productivity is also compromised. Being an unintentional insider threatened agent, is a source of anxiety for many teleworking employees (Mehan, 2016).

The literature review is also helpful in understanding the current pandemic and the need to be innovative to adapt. It is clear that the centers for Disease Control (Barlett & Borio, 2008) and Asian and African epidemiologists (Husin, 2009 and M'bayo, 2018) have provided explicit means to prepare for pandemics such as COVID-19, even if these were foreign to the general citizenry. Therefore, teleworking is a long-conceived solution for solving the spread of a corona virus. It also helps that the respondents in this exploratory study like teleworking. It increased their satisfaction with their jobs (Lee & Hong, 2011), even if it is as small as not commuting to work every week day, or having more kids with their friends. Admittedly, there are employees that miss the camaraderie of their colleagues and do not want this teleworking arrangement to persist. The termination of teleworking would signal the end of the threat of an airborne corona virus.

In conclusion, this exploratory research is topical and relevant because a dangerous pandemic is now gripping our society. It is important to understand how the economy will continue to work, and at the micro level, how employees will continue to maintain their livelihood, become more cybersecurity aware and even be satisfied employees.

Acknowledgment

This project was funded by the Center for Teaching and Learning at Norfolk State University, Virginia, USA.

References

Ackerman, G., & Peterson, H. (2020). Perspectives on Terrorism. *Terrorism Research Initiative, 14*(3), 59-73.

Ackerman, G., & Peterson, H. (2020). Terrorism and COVID-19: Actual and Potential Impacts. *Perspectives on Terrorism, 14*(3), 59-73.

American_FactFinder. (2010). *American FactFinder*. Retrieved from United States Census Bureau: https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=CF

Barlett, J. G., & Borio, L. (2008). The Current Status of Planning for Pandemic Influenza and Implications for Health Care Planning in the United States. *Clinical Infectious Diseases, 46*(6), 919-925.

Buchanan Turner, C., & Turner, C. (2019). Analyzing the Impact of Experiential Pedagogy in Teaching Socio-Cybersecurity: Cybersecurity Across the Curriculum. *The Journal of Computing Sciences in Colleges*, *34*(5), 12-22.

Cimpanu, C. (2020, April 18). *FBI says cybercrime reports quadrupled during COVID-19 pandemic.* Retrieved from ZDNet: https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/

Development, N. D. (2015). *Norfolk Virginia: Business Profile Data.* Retrieved from file:///C:/Users/Carlene%20Turner/Documents/EiR%20Proposal/norfolkbusinessprofiledata.pdf

Giddens, A. (2009). The Economic Crisis and Climate Change. In A. Hemerijck, B. Knapen, & E. van Doorne, *Aftershocks: Economic Crisis and Institutional Choice* (pp. 201-206). Amsterdam: Amsterdam University Press.

Husin, G. (2009). *Pandemic Preparedness in the Financial Sector: Pandemic Preparedness in Asia.* S. Rajaratnam School of International Studies. Singapore: S. Rajaratnam School of International Studies. Retrieved from http://www.jstor.com/stable/resrep05905.17

Lee, S.-Y., & Hong, J. H. (2011). Does Family-Friendly Policy Matter? Testing Its Impact on Turnover and Performance. *Public Administration Review, 71*(6), 870-879.

Mayfield, A. (2020, March 31). *Norfolk Zoom class hijacked, 'inappropriate materials' shared with students.* Retrieved from WAVY News - 10 on Your Side: https://www.wavy.com/10-on-your-side/norfolk-zoom-class-hijacked-inappropriate-materials-shared-with-students/

M'bayo, T. E. (2018). Ebola, Poverty, Economic Inequity and Social Injustice in Sierra Leone. *Journal of West African History, 4*(1), 99-128.

Mehan, J. E. (2016). The Unintentional Insider Threat. Chapter 3. In J. E. Mehan, *Insider Threat: A Guide to Understanding, Detecting, and Defending Against the Enemy from Within* (pp. 81-90). Cambridgeshire, UK: IT Governance Publishing.

Ritzer, G. (2019). *The McDonaldization of Society.* California: SAGE.

Ritzer, G., & Jurgenson, N. (2000). Production, consumption, prosumption: The nature of capitalism in the age of the digital 'prosumer'. *Journal of Consumer Culture, 10*(1), 13-36.

Ritzer, G., & Stepnisky, J. (2017). *Sociological Theory.* California: Sage Publishing.

Schutt, R. K. (2019). *Investigating the Social World: The Process and Practice of Research* (9th ed.). Boston: SAGE.

Smith, G. (2004). US Aid to Africa. *Review of African Political Economy, 31*(102), 698-703.

Turner, C., & Turner, C. (2017). Integrating Cybersecurity into the Sociology Curriculum: The Case of the Password Module. *Journal of Computing Sciences in Colleges, 33*(1), 109-117.

Weber, M. (2003). *General Economic History.* New York: Transaction Publishers.

Zur, R. (2020, April 10). *COVID-19 and cyberattacks: What you need to know*. Retrieved from eSchool News: https://www.eschoolnews.com/2020/04/10/covid-19-and-cyberattacks-what-you-need-to-know/?all