Aug 10th, 12:00 AM

Understanding the Cyber Safety Impacts of Digital Transformation on Vulnerable Businesses and Populations

Burcu Bulgurcu
Toronto Metropolitan University, bulgurcu@ryerson.ca

Understanding the Cyber Safety Impacts of Digital Transformation on Vulnerable Businesses and Populations

Emergent Research Forum (ERF)

Burcu Bulgurcu
Toronto Metropolitan University
bulgurcu@ryerson.ca

Abstract

The outbreak of the COVID-19 crisis has dramatically impacted the societal activities across the globe, forcing people to swiftly adapt to the unprecedented circumstances without any warning to prepare for the magnitude and duration of the crisis. The entire society, including the individuals, businesses, and governments, had to respond to the changes by digitally transforming lives or work processes without thoughtfully considering the best practices to deal with the arising challenges. The key goal of this research is to develop cyber resilience by proposing new guidelines and sources of advice for vulnerable businesses and populations on effective cybersecurity management, which in turn would lead the development of revised cybersecurity principles, awareness and training programs, and policies. This project provides a substantial opportunity to advance intellectual knowledge and theory on emerging and escalating cyber safety problems that arise due to the unexpectedly digitalized workforce and decentralized work-from-home environment.

Keywords

Online Safety, Digital transformation, Cybersecurity and Information Privacy, Vulnerable Groups, Small Businesses, Internet Safety for Young Children.

Introduction

The outbreak of the COVID-19 crisis has dramatically impacted the societal activities across the globe. A major change for most *businesses* was the sudden shift in ways of working by replacing traditional models of office work with home offices (Boland et al. 2020). The significant increase in the number of people working outside of their secured office networks presented an ideal environment for the opportunistic cybercriminals to target society in a variety of new ways, reflected by a surge in cybercrimes, phishing scams, and other types of malicious activities (McLaughlin and Currie 2020). A major change for *children* was digitalization of education, resulting in increased access to digital content. Excessive screen time has become a grave concern for young populations during the pandemic. Research shows that *cyberbullying* and harassment has significantly increased due to decreased online supervision and increased stress and isolation (Patchin 2021), harmfully effecting children's well-being and mental health (Pandya & Lodha 2021). Yet, this period has permanently changed the way education is perceived (McKenzie 2021).

The goal of the proposed research is to understand the scope and extent of this impromptu digital transformation, resulting in harmful consequences to the cybersecurity and online safety of vulnerable populations, including small businesses and young children, both of which were identified for their vulnerabilities in navigating through a digital threat environment. The core objectives and research questions are as follows:

1) The number of the most common cyber threats, including computer viruses, malware, phishing attacks have dramatically increased in the last two years (Help Net Security 2022). How do the

changes in the quantity and quality of cyber-attacks influence the small-size businesses with limited resources? How do they navigate this increasingly harmful threat environment?

2) How does increased screen time with decreased adult supervision affect children's online safety, including issues related to cyber-attacks, invasion of their privacy, and cyberbullying? How do parents responded to these changes to help their children navigate an emerging threat environment?

The nature of this research is exploratory, aiming to identify the grand challenges and consequences of this transformation as well as the groups that have been the most affected. Although the two research questions are not directly linked, they both aim to shed light on the populations that are vulnerable to potential cyber issues due to lack of resources, awareness, and training.

Background

The outbreak of the COVID-19 crisis has led to an explosion of cybersecurity incidents, phishing scams, and other malicious activities (O'Brien 2020). Since the beginning of 2020, there have been more than 445 million cyberattacks reported, which is double compared to those of 2019 (Help Net Security 2020). As criminals seek to exploit the public's concerns, numerous fraudulent emails and messages were sent to trick users into clicking on malicious links ranging from capitalizing on government support payments by imitating public institutions and legitimate authorities (Government of Canada 2020), exploiting the surge in the use of streaming services during the isolation period by giving away free subscription passes (Stawbridge 2020), selling government-issued online coronavirus tests or fake miracle cures to treat or prevent the disease (FDA 2020). According to Google, scammers are sending 18 million hoax emails about COVID-19 to Gmail users every day, making the virus to be the biggest phishing topic thus far (Tidy 2020).

The efforts of businesses to protect employees from a fatal virus while serving customers and maintaining business continuity have also increased their exposure to cyberthreats as they may have to deprioritize or relax cybersecurity to save human lives. Risk-mitigating behaviors could weakly be enforced for the sake of getting things done, while at the same time physical and psychological stressors compelled employees to bypass controls (Boehm et al. 2020). Greater use of online services, heightened activity on customer-facing networks, unsecured data transmissions without a proper VPN software over insecure cloud options or unencrypted networks presented new gaps for criminals to exploit. Large-scale adoption of telecommuting—performing work from locations other than the organization's facilities using work-from-home technologies—without having the opportunity to practice a safe transition from traditional offices to remote workplaces resulted in a rise of cyberattacks as companies dropped their online defenses. The mobile nature of devices used by remote employees as well as their lack of physical security made the data at increased risk of compromise. Businesses also have become increasingly reliant on video conferencing to stay connected, which has resulted in a surge of incidents whereby criminals gained unauthorized entry to videoconferencing calls to access private meetings and hijack screen controls (O'Flaherty 2020). Not having any guidelines on how to adopt the new normal, the society, businesses, and government realized the importance of cybersecurity management more than ever (Cavusoglu et al. 2004), looking for knowledge and best-practices to recover and adapt.

The other substantial gap in the cybersecurity literature is related to remote work. Because of the unprecedented context that the current COVID-19 crisis put the society in to ensure continuity of businesses through swift and unplanned digitalization and remote work, developing effective cybersecurity practices for remote work and home users have become more important than ever (Deeney 2020, Cyber Defense Magazine 2020). Currently, empirical research published on this area is very limited (Anderson and Agarwal 2010; Kritzinger and Solms 2010). Anecdotal evidence shows that the probability and severity of cyber-attacks affecting small businesses is high as they are more likely to lack the necessary resources and budget to protect their valuable assets (Bellon 2021). Therefore, this study will partially focus on small businesses as they have been identified as the vulnerable targets in business compared to larger organizations with stronger defence mechanisms.

The other vulnerable group for the safety of their online behavior during the pandemic has been young children. More than nine-in-ten U.S. parents with K-12 children at home reported that their children have had some online instruction since the outbreak, and over 30% of these parents said their child encountered at least one technology related obstacle to complete school work and it has been very difficult for them to

help their children use technology or the internet as an educational tool (Schaeffer 2021). During this time, children have been exposed to digital platforms more than ever with the necessities of remote education and other types of social activities due to lockdowns and social isolation. There is anecdotal evidence showing children becoming victims of insensitive digital access due to lack of rules or supervision around screen time (Livingstone 2021). Research also shows that cyberbullying victimization has increased during the pandemic (Gordon 2020), yet the results are not clear (Patchin 2021).

This project will focus on these challenging areas. The results will not only be responsive to the COVID-19 crisis but will have a broader and long-lasting impact on online safety related to rapid digitalization of society and workplaces, assisting with the development of effective awareness and training programs. COVID-19 has already changed the attitudes on the role of the offices (Boland et al. 2020, Davison 2020) and importance and feasibility of online learning. When the pandemic comes to an end, managers and educators across industries will use the lessons learned from this large-scale work-from-home experiment to digitally transform their business (Boland et al. 2020, Fletcher and Griffiths 2020), and with this shift in work circumstances, there will be even more emphasis on the importance of cybersecurity management (Yick 2020) and online safety (McKenzie 2021).

The findings of this project will advance theory and practice on emerging and escalating cybersecurity challenges that arise due to the unexpected digitalization and offer effective strategies to minimize these challenges, which in turn assist the development of revised cyber safety principles and awareness and training programs. An in-depth understanding of problems and potential solutions will enrich public discourse around cyberthreats and future remote work and digital use practices, some of which are expected to remain the same post-pandemic. Findings will offer economic benefits for businesses through enhanced security and reduction of the cost of recovery, regulatory benefits for government agencies through a better understanding of cybersecurity challenges for similar future crisis, and educational benefits for curriculum development.

Method

During the next twelve months, we will conduct an exploratory research in phases to understand the scope and extent of changes during the COVID-19 pandemic and their impact on the cybersecurity and online safety of two vulnerable groups: small business and young populations. In the first phase, we will conduct a comprehensive review on news sources, industry reports, and academic publications to identify the challenges and vulnerabilities that have emerged or intensified as a result of rapid digital transformation during the pandemic. Some of the themes that we will conduct our investigation on are related to: cybersecurity challenges related to remote work, excessive videoconferencing and Zoom bombing, mobility of data storage devices and other digital technologies, phishing attacks and scammers cashing in on COVID-19, cyberbullying, and invasion of privacy. This review will help develop the semi-structured interview questions that we will use in the next phases of the project for the interviews with the small businesses and focus groups parents of teens. Conducting in-depth follow-up interviews as a source of data collection is essential as our focus is to identify emerging and escalating cybersecurity issues and what they need to respond to this threat environment.

In the second phase, we will conduct semi-structured interviews with IT professionals from eight-to-ten case organizations to understand the effects of the revamped work practices on the challenged components of cybersecurity procedures. Sampling will include small size businesses and non-profit organizations that lack sufficient resources to invest in cyber-protective practices. We are in touch with the editors of a security magazine widely read by practitioners and Security Special Interest Group of Canada's Association of Information Technology Professionals to identify potential candidate organizations. The outcome of these interviews will be the development of taxonomies of the types of the major cybersecurity challenges small businesses are being confronted with during the pandemic and the ways by which they have responded. We will also conduct focus group with the parents of young teens from eight-to-ten families to understand the effects of their children's increased access to digital resources on their online safety as well as their approach to ensure their protection. The sampling method will be purposeful sampling, considering the demographic traits of the parents, including education, socio-economic-status, digital ability and competence, to be able to control for the potential influence of these factors. The focus group discussions will be aimed to answer whether parents have adapted any practices to protect their children against cyber-attacks, invasion of their privacy, cyber bullying, and access to harmful digital content.

Contributions

This research will offer a range of relevant, timely, and long-lasting benefits globally, including the civil society, private sectors, government agencies, and professional communities. The project will provide an important opportunity to advance intellectual knowledge and theory on emerging and escalating cybersecurity and online safety problems that arise due to the unexpectedly digitalized workforce and human lives. By examining the extent of the problems as well as the effectives of measures implemented during the pandemic, the findings will inform scholars and the society to revamp cybersecurity awareness and training programs. The results will enhance professional practice by proposing new guidelines and sources of advice on how to ensure cybersecurity while maintaining business continuity during environmental disruptors, which in turn would lead the development of enhanced cybersecurity measures, policy, curriculum, and awareness and training programs through emerging regulations and knowledge that can counter cyberthreats. Governments will benefit through a better understanding of cybersecurity challenges during a crisis to develop guidelines and impose regulatory policies for businesses and government agencies. Finally, economic benefits will be offered through enhanced security and reduction of the cost of recovery.

REFERENCES

Anderson, C. L., Agarwal, R. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), p. 613–643.

Boehm, J., Kalan, J., and Sportsman, N. 2020. "Cybersecurity's dual mission during the coronavirus crisis," *McKinsey & Company*. https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis

Bellon, L. 2021. "Small Businesses are facing big cybersecurity challenges in 2021," *Cisco Umbrella*.

Boland, B., Smet, A., Palter, R., and Sanghvi A., 2020. "Reimagining the office and work life after COVID-19," *McKinsey & Company*. https://www.mckinsey.com/business-functions/organization/our-insights/reimagining-the-office-and-work-life-after-covid-19

Cavusoglu, H., & Cavusoglu, S. R. (2004). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems* , 65-75.

Cyber Defense Magazine. 2020. "Why Cybersecurity Awareness is More Important During COVID-19," https://www.cyberdefensemagazine.com/why-cybersecurity-awareness/

Davison, R. M. 2020. "The Transformative Potential of Disruptions: A Viewpoint," *International Journal of Information Management*, p.102149.

Deeney, N. 2020. "Covid-19: Why Cyber Security Awareness is More Important Than Ever," McKinsey & *Company*. https://www.metacompliance.com/blog/covid-19-why-cyber-security-awareness-is-more-important-than-ever/

Fletcher, G., Griffiths, M. 2020. "Digital transformation during a lockdown," International Journal of Information Management, Vol: 55, p. 102185, https://doi.org/10.1016/j.ijinfomgt.2020.102185

Food and Drug Administration (FDA). 2020. "Beware of Fraudulent Coronavirus Tests, Vaccines and Treatments," https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments

Gordon, S. 2020. "Research shows rise in cyberbullying during COVID-19 pandemic," https://www.verywellfamily.com/cyberbullying-increasing-during-global-pandemic-4845901

Government of Canada. 2020. "Covid-19: Frauds and Scams," https://www.canada.ca/en/public-safety-canada/campaigns/covid19.html

Help Net Security. 2020. "445 million attacks detected since the beginning of 2020, COVID-19 wreaks havoc," https://www.helpnetsecurity.com/2020/04/29/2020-attack-rate/

McKenzie, L. 2021. "Students want online learning options post-pandemic," *Inside Higher Ed*.

McLaughlin, R., Currie, E. 2020. "Cybercrime booming during the pandemic," *CTV News*. https://bc.ctvnews.ca/cybercrime-booming-during-the-pandemic-1.5154896

O'Brien, C. 2020. "Coronavirus cons: How scammers are using COVID-19 fears to target Canadians," *CTV News,* https://www.ctvnews.ca/health/coronavirus/coronavirus-cons-how-scammers-are-using-covid-19-fears-to-target-canadians-1.4859688

O'Flaherty, K. 2020. "Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat," *Forbes*, https://www.forbes.com/sites/kateoflahertyuk/2020/03/27/beware-zoom-users-heres-how-people-can-zoom-bomb-your-chat/?sh=7a09f013618e

Patchin, J. 2021. "Bullying during the COVID-19 Pandemic," *Cyberbullying Research Center*, https://cyberbullying.org/bullying-during-the-covid-19-pandemic

Schaeffer, K. 2021. "What we know about online learning and the homework gap amid the pandemic," *Pew Research Center*

Stawbridge, G. 2020. "Warning over Coronavirus Netflix Scam," *MetaCompliance,* https://www.metacompliance.com/blog/warning-over-coronavirus-netflix-scam/

Tidy, J. 2020. "Google blocking 18m coronavirus scam emails every day," *BBC News*, https://www.bbc.com/news/technology-52319093

Yick, E. 2020. "Working from home: COVID-19 and the importance of cybersecurity," *Security Magazine*, https://www.orange-business.com/en/blogs/working-home-covid-19-and-importance-cybersecurity