Chapter 7
Cybersecurity and Data Privacy in the Digital Age: Two Case Examples

Olakunle Olayinka
University of Sheffield, UK

Thomas Win
University of West of England, UK

ABSTRACT

The COVID-19 pandemic has brought to the fore a number of issues regarding digital technologies, including a heightened focus on cybersecurity and data privacy. This chapter examines two aspects of this phenomenon. First, as businesses explore creative approaches to operate in the "new normal," the security implications of the deployment of new technologies are often not considered, especially in small businesses, which often possess limited IT knowledge and resources. Second, issues relating to security and data privacy in monitoring the pandemic are examined, and different privacy-preserving data-sharing techniques, including federated learning, secure multiparty computation, and blockchain-based techniques, are assessed. A new privacy-preserving data-sharing framework, which addresses current limitations of these techniques, is then put forward and discussed. The chapter concludes that although the worst of the pandemic may soon be over, issues regarding cybersecurity will be with us for far longer and require vigilant management and the development of creative solutions.

INTRODUCTION

Cybersecurity is not normally viewed as one of the digital technologies per se, but rather as a key issue within the overall digital transformation landscape. As the deployment of digital technologies becomes more prevalent, so the associated cybersecurity risks increase and must be managed. In 2020-21, as a result of the COVID-19 pandemic, many small businesses, which had hitherto operated primarily via physical locations, had to change to ensure they could operate remotely and have an online presence, in response

DOI: 10.4018/978-1-7998-7712-7.ch007

to social distancing and the lockdown measures implemented in many countries. At the same time, the pandemic highlighted the importance of healthcare organisations around the world in collaborating to contain it. To tackle this global challenge, healthcare organisations have obtained large amounts of both unstructured and structured patient healthcare data, in the search for critical insights into its spread and ultimately as a means of preventing it. However, increasing public concerns over data security, as well as associated government regulations, have made it a significant challenge for the organisations to share data, as part of their collaborative research into the pandemic.

These two scenarios provide a useful frame of reference within which to consider the significance of cybersecurity in the digital era. The research in both these contexts was qualitative and inductive, based on an integrative literature review and development of new concepts. In the case of the research into small businesses, semi-structured interviews with company personnel were also used to develop and validate findings. In inductive research, the researcher aims to explore a topic and develop a theoretical explanation of the phenomenon studied using collected and analysed data (Gill & Johnson, 2002). The inductive approach to research is concerned with developing theory from findings obtained (Flick, 2014) and the researcher should be observant, with a mind attuned to interpret that data. According to Collins (2018), the inductive approach to research is more suited for research where there is little existing study, so that collected data will help generate theoretical themes.

Following this introduction, the chapter consists of two main sections. First, cybersecurity in small businesses is examined to identify current responses to the threat of cybersecurity, and to identify areas where threats could be more readily recognised and managed. Second, the issues involved in data exchange for pandemic monitoring are explored, with a particular focus on data privacy and security concerns. Finally, a short concluding section summarises some of the emergent themes from both case examples.

CYBERSECURITY AND SMALL BUSINESS ENTERPRISES

Background

Small business enterprises (SBEs) can be defined as having less than 50 staff and are generally referred to as the backbone of most modern economies (Day, 2000). With the proliferation of the internet, mobile devices and cloud computing in today's digital economy, the relevance of SBEs has arguably increased in recent years. SBEs can now compete globally, access international markets and deliver new digital focused products in a cost-effective manner (Chen et al., 2016; Neirotti et al., 2008). An increasing number of SBEs are using digital technologies to innovate, outperform competition and ultimately stay in business. Many SBEs, however, have limited IT resources (Apulu et al., 2013), and yet cybersecurity threats and risks related to digitalisation for SBEs is at an all-time high (Irwin, 2021, June 29). According to The Washington Post (Riley, 2020, December 7), losses from cybercrime in 2020 were about $1 trillion. A recent Cyber Security Breaches Survey in the UK suggested that four in ten businesses (39%) experienced a cyber-attack in the last twelve months, while 77% of SBEs in the UK indicated that cybersecurity is a high priority for them (Gov.uk, 2021). According to Collett (2020, August 7), one SBE in the UK gets hacked every 19 seconds, and implementing digital technologies without clearly thought-out plans for security is a major risk that can be disastrous for small businesses.

There has been an increasing number of high-profile cybersecurity attacks in recent years that have resulted in loss of intellectual property, customer data and brand reputation (Dignan, 2021, May 13).