Chapter 6
Advancement of Cybersecurity and Information Security Awareness to Facilitate Digital Transformation: Opportunities and Challenges

Hamed Taherdoost
https://orcid.org/0000-0002-6503-6739
Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, Canada

Mitra Madanchian
Research and Development Department (Research Club), Hamta Business Corporation, Canada

Mona Ebrahimi
Research and Development Department (Research Club), Hamta Business Corporation, Canada

ABSTRACT

As the pace of changes in the digital world is increasing exponentially, the appeal to shift from traditional platforms to digital ones is increasing as well. Accomplishing digital transformation objectives is impossible without information security considerations. Business leaders should rethink information security challenges associated with digital transformation and consider solutions to seize existing opportunities. When it comes to information security, human beings play a critical role. Raising users' awareness is a meaningful approach to avoid or neutralize the likelihood of unwanted security consequences that may occur during transforming a system digitally. This chapter will discuss cybersecurity and information security awareness and examine how digital transformation will be affected by implementing information security awareness. This chapter will discuss the digital transformation advantages and serious challenges associated with cybersecurity, how to enhance cybersecurity, and the role of information security awareness to mitigate cybersecurity risks.

DOI: 10.4018/978-1-7998-6975-7.ch006

INTRODUCTION

Digital transformation is revolutionizing most businesses. Today, it is of significant importance for businesses to prioritize investment in digital transformation to stay successful in the competition. Recent changes in contemporary business have provided organizations with a valuable opportunity to leave their traditional manual processes and move toward digital technologies (Ted Saarikko, Ulrika H. Westergren, & Blomquist, 2020). Digital transformation is a necessity of today's digital age and one of the most recent manifestations of recent technological changes in the business environment. The impact of digitalization in operating, delivering value to customers, and providing a clear vision for the business in the competitive digital world of today is not negligible. The prevalent advent of powerful new technological devices with abundant opportunities that they provide for both people and organizations, signals the definite need for organizations to transform their business to digital platforms (Verhoef et al., 2021). It is also important to note that, digital transformation is not just the matter of shifting to digital technologies (Henriette, Feki, & Boughzala, 2015), it is about changing mindset, and alignment of attitude, strategy, people, resources and leadership (Goran, LaBerge, & Srinivasan, 2017). During recent years, digital transformation is recognized as an ecosystem and societal challenge and necessity (Gong & Ribiere, 2020), and thus, it has attracted the attention of researchers and practitioners to identify implications of digital transformation, its benefits, shortcomings and consequences (Zaoui & Souissi, 2020).

The world is gone digital and in this digital age that systems are growing in size and complexity, the scope of potential vulnerabilities has broadened as well. The revolution of internet technology and fundamental changes caused as a result of digital developments have increased electronic data transfer and the number of online transactions. Cyberattacks and unauthorized access to valuable data are respected as one of the top-ranked threats that any business may face through digital transformation. Since the amount of data transferred through digital platforms is increased, the likelihood to face data loss and cybercrime incidents is also increased dramatically (Aloul, 2012). Today, a great number of businesses rely on information including financial data, customers' profile data, legal data, and market and competition data (Taherdoost, 2020b). There are always possibilities to happen unwanted security incidents within systems that are dependent on information (Diesch, Pfaffa, & Krcmar, 2020). Thus, the vulnerability of information assets due to unpredictable attacks through a range of variable stealthy techniques by cybercriminals is considerable. Based on a report presented by the World Economic Forum (Vina, 2016), the cost of cybercrime is a staggering US$445 billion annually. Therefore, companies make attempts to minimize risks by paying prior attention to information security risks (Banfield, 2016). The information security program is one definite forward-thinking solution to address the risk of valuable data loss. Cybersecurity includes all of the information technology and data in the technological platform.

As the security of systems is a chain of different elements, achieving cybersecurity objectives is impractical without bearing in mind other influencing factors (Domínguez, Ramaswamy, Martinez, & Cleal, 2010). Human behavior is generally known as the greatest threat to cybersecurity (Crossler et al.,2013). During recent years that the Internet and technology usage has been growing exponentially, attackers have also adopted smarter techniques to exploit end-users' trust that steal their valuable information for their benefit. Based on prior research, "it is estimated that more than 6m stolen credentials are leaked every day, either free or sold on as lists" (Fortson, 2017). Thus, people who are constantly under threat while using any technological and internet-based platform to reveal their personal information are considered as one of the top reasons for data loss. To mitigate the information security issues related to humans as the main source (Banfield, 2016), users' awareness about information security should be