Chapter 8
Business Management and Strategy in Cybersecurity for Digital Transformation

Fahri Özsungur
https://orcid.org/0000-0001-6567-766X
Department of Labor Economics and Industrial Relations, Mersin University, Mersin, Turkey

ABSTRACT

Cyber security threatens vital elements of enterprises such as network, information, application, operational, sustainability, education, and trade secret. Digital transformation and widespread use of IoT caused by the pandemic reveal the importance of cybersecurity vulnerabilities. This study is prepared by a systematic review method for cybersecurity. The inspiration of this chapter is the cyberattacks that threaten the global economy and enterprises and the effects of cybercrime on management and strategy. The cybersecurity problem, which continues to increase with the pandemic in the manufacturing and service sector, is current and becoming a serious threat. This study reveals strategy development against cybersecurity threats; sustainability elements in management; measures to be taken against cybercrime, cyberattack, and cyberterrorism; and organizational and business culture management in digital transformation.

INTRODUCTION

Cybercrime and cyber attacks are among the most critical and important problems of today's digital World (Akhgar, Staniforth, & Bosco, 2014). The extraordinary situation that emerged with COVID-19 and the pandemic has made the global economy come to the fore in the operational processes of businesses. Digital elements, which are increasingly important, continue to be reflected in business life with digital transformation. The increasing effects of digital innovations on the managerial and strategic practices of the business have led to an increase in cyber attacks. Malicious attacks, cyber thieves are harming the global economy by seizing confidential and important information of businesses (Ismail, Shaaban, Naidu, & Serpedin, 2020).

DOI: 10.4018/978-1-7998-6975-7.ch008

Problems arising from cyber-attacks and systemic vulnerabilities of businesses require development, harmonization, and improvement in management and strategy (Hellström, 2007). Taking cybersecurity measures in the context of human resources, operations, sales, after-sales services, promotion, providing competitive advantage has become an important managerial and strategic need of today's businesses. It is a current issue to strengthen the strategies of businesses in the context of cybersecurity vulnerabilities, cyber-attacks, digital threats, cyber risks, and weaknesses due to these factors (Sallos, Garcia-Perez, Bedford, & Orlando, 2019). In the management and strategy literature, the management and strategy development of businesses and organizations is evaluated within a general framework (Phan, 2001; Chrisman, Hofer, & Boulton, 1988; Kotey & Meredith, 1997; Matricano, 2021). The theoretical framework and empirical research developed do not focus on strengthening strategy and managerial elements. This chapter brings to the literature that the requirements of today's digital world such as strengthening management and strategy, developing strategies based on digital and cyber protection, eliminating weaknesses in digital transformation. Eliminating the cyberattacks that threaten today's global economy and businesses and the weaknesses caused by digital transformation is a current issue and the chapter focuses on this issue. Therefore, in the chapter, digital transformation, effects of cybersecurity on businesses, data and information security, application and software security, network, and communication security, operational security, cyber-strategy development, sustainable training and adaptation, cybersecurity threats, cybercrime, cyberterrorism, cyber-management, and strategy issues are covered.

RESEARCH METHODOLOGY

This study was prepared by a systematic review method. The systematic review method consists of preparation for research → data collection → analysis of data → evaluation of data → implications → reporting (Beelmann, 2006; Petticrew & Roberts, 2008). The inspiration of this chapter is the cyberattacks that threaten the global economy and organizations, and the effects of cybercrime on management and strategy. The cybersecurity problem, which continues to increase with the pandemic in the manufacturing and service sector, is current and becoming a serious threat. In this context, the questions of the study were determined as follows:

- R1. What are the effects of cybersecurity on businesses?
- R2. What are the elements of cyber-strategy development in businesses?
- R3. How can cyber-management and strategy be strengthened in businesses?

After the study questions were determined, the keywords for literature review in academic databases (Google scholar, Web of Science, Emerald Insight, Taylor and Francis) were determined as follows: management, strategy, management and strategy, cyber, cyber attack, cybercrime, cybersecurity, digital transformation, digital management, digital strategy. 214 articles directly related to the topic were accessed in the search for keywords. The research, analysis, and reporting took approximately 1.5 weeks.

After the literature review was performed, the steps of summarizing, classifying, extracting data, discussing, categorizing, and presenting the information obtained from academic databases were followed in the study (Denyer & Tranfield, 2009; Martins et al., 2015). After these steps, the titles and content related to the researched subject were determined and reported.