Chapter 5
Strengthening Cybersecurity in Singapore:
Challenges, Responses, and the Way Forward

Ching Yuen Luk
Nanyang Technological University, Singapore

ABSTRACT

This chapter uses a historical perspective to examine the development trajectory of e-government in Singapore, the trends and patterns of cybercrimes and cyber-attacks, and the measures taken by the government to combat cybercrimes and cyber-attacks. It shows that the government has adopted a proactive, holistic, and cooperative approach to cybersecurity in order to tackle the ever-increasing cybersecurity challenges. It has regularly reviewed and improved cybersecurity measures to ensure their effectiveness and strengthened its defense capabilities over time through coordinating national efforts with public and private sectors and cooperating with regional and international counterparts. The chase for a perfect cybersecurity system or strategy is both impossible and unnecessary. However, it is important and necessary to establish a cybersecurity system or formulate a cybersecurity strategy that can monitor, detect, respond to, recover from, and prevent cyber-attacks in a timely manner, and make the nation stronger, safer, and more secure.

DOI: 10.4018/978-1-5225-5984-9.ch005

INTRODUCTION

Singapore is one of the most connected countries in the world. Due to the government's continuous effort to upgrade information technology (IT) infrastructure and implement e-government strategies, information and communications technology (ICT) serves as a powerful tool to modernize the civil service and enhance administrative efficiency, facilitate economic growth and foster interaction between citizens and government. However, Singapore's growing dependence on IT has made it become targets of cyber attacks in recent years. Singapore is likely to remain a prime target for cyber attacks for years to come, especially when it transforms into a Smart Nation and prioritizes digital economy. For these reasons, the government has put cybersecurity at the top of the agenda and is racing against time to build a safe, secure and trusted cyber environment. While there are some studies examining development of e-government in Singapore during a specific period of time, there is the lack of studies on the trends of cybercrimes and cyber attacks in the nation and the government's responses to such crimes and attacks. In order to fill the existing research gaps, this study uses a historical and policy perspectives to examine the development trajectory of e-government in Singapore, the trends and patterns of cybercrimes and cyber attacks, and the measures taken by the government to combat cybercrimes and cyber attacks.

BACKGROUND

Cybersecurity "refers to security issues related to digital assets connected to the Internet" (Thompson, 2017, p.84). It refers to the use of people, process and technology to "prevent, detect, and recover from damage to confidentiality, integrity, and availability of information in cyberspace" (Bayuk et al., 2012, p.3). Such damage is usually caused by cyber attacks or cyberterrorism. Being regarded as a non-traditional threat, cyberterrorism refers to premeditated, unlawful attacks against computer systems, networks, and data stored therein to intimidate or coerce a government or civilian population in furtherance of political, economic, social, religious or ideological objectives (Denning, 2000, p.29; Everard, 2008, p.119; Theohary and Rollins, 2015, p.1). Such attack is carried out anonymously and remotely through computer viruses, computer worms, denial-of-service (DoS) attacks, distributed denial of service (DDoS) attacks (Tehrani, 2017, pp.55-61), Domain Name System (DNS) attacks, malicious software such as Trojan horses, phishing or spamming. It causes different types and levels of damage, including stealing, erasing, or altering information (Al-Rodhan, 2011, p.37), deleting or corrupting stored data (Fidler, 2016, p. 480), denying services, remotely taking control of a system or devices