Cybersecurity Laws in Malaysia

2

Olivia Swee Leng Tan
https://orcid.org/0000-0002-5628-6883
Multimedia University, Malaysia

Rossanne Gale Vergara
Multimedia University, Malaysia

Raphael C. W. Phan
Multimedia University, Malaysia

Shereen Khan
Multimedia University, Malaysia

Nasreen Khan
Multimedia University, Malaysia

INTRODUCTION

The progression of information and communication technologies (ICT) use have been matched by the rise in corruption and abuse of technology for criminal activities. Regarding computer crimes in Malaysia, the Malaysia Computer Emergency Response Team (MyCERT) reported 3,743 incidents from January to May of 2019. Fraud incidents at 2,563 ranking the highest reported incidents for 2019 and "intrusion" incidents at 432 ranking the second highest incidents. In 2018, the total incidents reported to MyCERT was 10,699, of which "fraud" again had the highest reported incidents (5,123) and the second highest "intrusion attempt" at (1,805) of the total incidents. Between 2014-2017, the total number of incidents (Cyber harassment, Content related, Denial of Service, Fraud, Intrusion, Intrusion Attempt, Malicious Codes, Spam, Vulnerabilities report) gradually decreased from 11,918 incidents in 2014 to 7,962 incidents, a decrease of 3,956 or 33.2% in 2017. The statistics show that Malaysia's cybercrime incidents have increased again in 2018 despite the country's attempts at mitigating cybercrime. Cybercrimes are borderless and the threat of a cyberattack or cybercrime is there. To combat such criminal activities today in Malaysia, cyber laws have existed since 1997 to include: Computer Crimes Act 1997, Digital Signature Act 1997, Communications and Multimedia Act 1998, Payment Systems Act 2003, Electronic Commerce Act 2006, Personal Data Protection Act 2010 and Malaysian Penal Code to combat criminal activities such as fraud. While the cyber laws and law enforcement agencies exist in Malaysia, cybercrimes still pose a daunting challenge. The objective of this chapter is to analyse the existing cyber security legislations in Malaysia to combat cybercrimes in the country.

DOI: 10.4018/978-1-5225-9715-5.ch030

BACKGROUND

In 1991, Malaysia Vision 2020 by Prime Minister Mahathir Mohamad was presented during the Sixth Malaysia Plan. Malaysia Vision 2020 was the prime minister's vision for Malaysia to become a developed nation by 2020, which included his thoughts on how the nation can achieve this goal by meeting nine specific objectives These nine objectives as he pointed out in his vision were to establish the following:

1. United Malaysian nation
2. Secure and developed Malaysian Society
3. Mature democratic society
4. Fully moral and ethical society
5. Matured liberal and tolerant society
6. Scientific and progressive society, a society that is innovative and forward looking, one that is not only a consumer of technology but also a contributor to the scientific and technological civilisation of the future
7. Fully caring society and caring culture
8. Economically just society
9. Prosperous society, with an economy that is fully competitive, dynamic, robust and resilient.

Malaysia Vision 2020 catapulted initiatives to support Prime Minister Mahathir agenda, one of these listed as objective six: to establish a scientific and progressive society. Thus, Multimedia Super Corridor (MSC) Malaysia was launched in 1996 and the first cyber laws of Malaysia were introduced: Computer Crimes Act 1997, Telemedicine Act 1997, Copyright (Amendment) Act 1997, and Digital Signature Act 1997. Communication and Multimedia Act 1998 followed one year later and then: Payment Systems Act 2003, Electronic Commerce Act 2006, and Personal Data Protection Act 2010. The foundation established by these early cyber laws were to prepare the nation to embark on innovations and protect Malaysians using new innovations. The laws most relevant to current cybercrimes experienced in Malaysia will be discussed further in the subsequent section.

Malaysia, a country with a population of 32.7 million located in Southeast Asia was ranked third overall in the world behind Singapore and United States in the 2017 Global Cyber security Index (GCI), (International Telecommunications Union, 2017, July 6) and currently 8th place in the 2018 GCI global ranking. GCI is a survey that measures the commitment of the International Telecommunications Union (ITU) Member States to cyber security in order to raise awareness, which is driven by five pillars (legal, organisational, capacity building, and cooperation). However, as mentioned above, while the incidents reported by MyCERT have decreased from 2014-2017, the reported incidents have increased since then by 2,737 incidents in 2018. Table 1 below shows the top five reported incident categories (Fraud, Intrusion, Intrusion Attempt, Spam, Malicious Code) by MyCERT from 2010-2018, with the exception of "Cyber Harassment" making it to the top 5 incidents in 2018 overtaking Spam incidents. 2011 was the year Malaysia had the highest overall reported incidents in fraud (5,328) and spam (3,715). Intrusion (4,326) was the highest in 2012 and intrusion attempt (1,805) was highest in 2018, while malicious code (1,751) ranked highest in 2013. The trend overall shows that Fraud incidents across 2010-2018 consistently ranked the highest in incident reports with current 2018 statistics showing an increase in cyber harassment, intrusion attempt and malicious code incidents.