Security Frameworks in Contemporary Electronic Government

Ryma Abassi
Carthage University, Tunisia

Aida Ben Chehida Douss
Carthage University, Tunisia

A volume in the Advances in Electronic Government, Digital Divide, and Regional Development (AEGDDRD) Book Series

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Abassi, Ryma, 1980- editor. | Ben Chehida Douss, Aida, 1986- editor.
Title: Security frameworks in contemporary electronic government / Ryma Abassi and Aida Ben Chehida Douss, editors.
Description: Hershey, PA : Information Science Reference, [2018]
Identifiers: LCCN 2017061521| ISBN 9781522559849 (hardcover) | ISBN 9781522559856 (ebook)
Subjects: LCSH: Internet in public administration. | Computer security.
Classification: LCC JF1525.A8 S44 2018 | DDC 352.3/8028558--dc23 LC record available at https://lccn.loc.gov/2017061521

This book is published in the IGI Global book series Advances in Electronic Government, Digital Divide, and Regional Development (AEGDDRD) (ISSN: 2326-9103; eISSN: 2326-9111)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material.
The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

Advances in Electronic Government, Digital Divide, and Regional Development (AEGDDRD) Book Series

ISSN:2326-9103
EISSN:2326-9111

Editor-in-Chief: Zaigham Mahmood, University of Derby, UK & North West University, South Africa

MISSION

The successful use of digital technologies (including social media and mobile technologies) to provide public services and foster economic development has become an objective for governments around the world. The development towards electronic government (or e-government) not only affects the efficiency and effectiveness of public services, but also has the potential to transform the nature of government interactions with its citizens. Current research and practice on the adoption of electronic/digital government and the implementation in organizations around the world aims to emphasize the extensiveness of this growing field.

The Advances in Electronic Government, Digital Divide & Regional Development (AEGDDRD) book series aims to publish authored, edited and case books encompassing the current and innovative research and practice discussing all aspects of electronic government development, implementation and adoption as well the effective use of the emerging technologies (including social media and mobile technologies) for a more effective electronic governance (or e-governance).

COVERAGE

- Emerging Technologies within the Public Sector
- Case Studies and Practical Approaches to E-Government and E-Governance
- Public Information Management, Regional Planning, Rural Development
- ICT within Government and Public Sectors
- E-Governance and Use of Technology for Effective Government
- Frameworks and Methodologies for E-Government Development
- Social Media, Web 2.0, and Mobile Technologies in E-Government
- Current Research and Emerging Trends in E-Government Development
- Electronic Government, Digital Democracy, Digital Government
- Issues and Challenges in E-Government Adoption

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Advances in Electronic Government, Digital Divide, and Regional Development (AEGDDRD) Book Series (ISSN 2326-9103) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-electronic-government-digital-divide/37153. Postmaster: Send all address changes to above address.

Titles in this Series

For a list of additional titles in this series, please visit:
https://www.igi-global.com/book-series/advances-electronic-government-digital-divide/37153

Media Diplomacy and Its Evolving Role in the Current Geopolitical Climate
Swati Jaywant Rao Bute (Jagran Lakecity University, India)
Information Science Reference • ©2018 • 211pp • H/C (ISBN: 9781522538592) • US $195.00

Global Leadership Initiatives for Conflict Resolution and Peacebuilding
Andrew H. Campbell (International Peace and Leadership Institute, USA)
Information Science Reference • ©2018 • 331pp • H/C (ISBN: 9781522549932) • US $225.00

Financial Sustainability and Intergenerational Equity in Local Governments
Manuel Pedro Rodríguez Bolívar (University of Granada, Spain) and María Deseada López Subires (University of Granada, Spain)
Information Science Reference • ©2018 • 343pp • H/C (ISBN: 9781522537137) • US $205.00

Handbook of Research on Modernization and Accountability in Public Sector Management
Graça Maria do Carmo Azevedo (University of Aveiro, Portugal) Jonas da Silva Oliveira (ISCTE – Instituto Universitário de Lisboa, Portugal) Rui Pedro Figueiredo Marques (University of Aveiro, Portugal) and Augusta da Conceição Santos Ferreira (University of Aveiro, Portugal)
Information Science Reference • ©2018 • 539pp • H/C (ISBN: 9781522537311) • US $285.00

Knowledge-Based Urban Development in the Middle East
Ali A. Alraouf (Qatar Urban Planning, Qatar)
Information Science Reference • ©2018 • 310pp • H/C (ISBN: 9781522537342) • US $185.00

Nationalism, Social Movements, and Activism in Contemporary Society Emerging...
Emily Stacey (Swansea University, UK)
Information Science Reference • ©2018 • 135pp • H/C (ISBN: 9781522554332) • US $155.00

For an entire list of titles in this series, please visit:
https://www.igi-global.com/book-series/advances-electronic-government-digital-divide/37153

701 East Chocolate Avenue, Hershey, PA 17033, USA
Tel: 717-533-8845 x100 • Fax: 717-533-8661
E-Mail: cust@igi-global.com • www.igi-global.com

Table of Contents

Detailed Table of Contents

The growing menace of cyber-related crimes in Nigeria is giving the government and other stakeholders in the information and communication technology sector a cause to worry. Apart from taking a toll on the nation's economic sphere, it has also affected the image of the country negatively especially when viewed against the backdrop of the recent ranking of Nigeria as third in global internet crimes behind United Kingdom and the United States. This scenario, no doubt, requires urgent attention. This chapter, therefore, proffer solutions and recommend ways to make the country's cyberspace free from incessant criminal attacks.

Different systems require different levels of security according to the services they provide to their users. Cyberspace is the alliance of various networks together connected through internet service providers (ISPs). However, the alliance of these networks often faces security issues. Some use the internet as a path for illegal activities such as breaching of others computer or networks, damaging and stealing information, and blocking or denying legitimate users from services they subscribe. So, the purpose of this chapter is to review the responsibilities of ISPs in securing their customers' network, and find out whether there are legal provisions, or liabilities that are bindings on the ISPs to provide security for their customers. What protections are envisaged under the umbrella of safe harbors? Are ISPs responsible for end users' network security? The Swedish Court recently found The Pirate Bay (TPB) guilty of making copyright works available. Finally, this chapter will analyze the issues raised in the TPB along with ISPs liability.

The trend of e-governance and m-governance in governance is increasing rapidly and the instrument of governance is getting closer to the citizens. This chapter considers the trust and reputation of the digital environment of e-governance and m-governance in the world from the existing legal and judicial inkling. How sufficient are the international policies and benchmarks on the use of information communication technology (ICT) for e-governance and m-governance within and among nations to be trusted and judged to be of good repute among the users and has it been able to promote the use of e-governance and m-governance among the nations of the world? The theoretical framework that this chapter hinges on is the

Preface

The recent rise of emerging networking technologies such as social networks, content centric networks, IoT networks, etc. have attracted lots of attention from academia as well as industry.

Such technologies should help facilitate the socio-economic development in the countries as well as an effective operational management within central government. Making use of emerging technologies in systems of governance for a wide range participation and an intense involvement of citizens, institutions and civil society groups in the decision making process of governance is called e-Governance.

The United Nations defines e-Government as the use of Information and Communications Technologies (ICT) and its application by the government for the provision of information and public services to the people. E-Governance and m-Governance is also described by Agrawal, Sethi and Mittal (2015) and Meijer (2015) as a process of reform in the way government works, shares information, engages citizens and delivers services to external and internal clients for the benefit of both government and the clients that they serve.

Paradoxically, the use of such technologies in e-government/ m-government services raise issues relating to Security, Privacy and Data Protection.

In fact, in order to fully exploit the benefits of e-government, there is a number of special security requirements which are dictated by the sensitive nature of the data transmitted during e-government transactions. These data may include personal data, such as identity and contact details, government data, such as record / registration numbers and certificates, as well as financial data, such as credit card and bank account numbers. Furthermore, these security requirements have become even more crucial with the advent of m-government. Security and privacy are specific concerns in wireless communication because of the case of connecting to the wireless link anonymously. The citizens want that the government agencies should safeguard their key data from moving into the hands of unauthorized agencies or hackers, thus preventing its misuse (Mengistu et al. 2009).

This book discusses and addresses the difficulties and security related challenges faced in implementing e-government/m-government technologies and applications.

ORGANIZATION OF THE BOOK

The book is organized into 10 chapters. A brief description of each of the chapters follows:

Chapter 1 presents m-Government and its applications on public service delivery. In this chapter, authors investigate and discuss various themes namely E-Government, Mobile Government, different perspectives on Mobile Government, Mobile Government in developed countries, benefits and limitations of Mobile Government, way forward in implementing Mobile Government and future research in areas of Mobile Government.

Chapter 2 proposes COMPARCH as a compliance-driven system engineering framework for privacy and security in socio-technical systems. It consists of: (1) a risk-based requirement management process, (2) a test-driven security and privacy modeling framework and (3) a simulation-based validation approach. The satisfaction of the regulatory requirements is evaluated through the simulation traces analysis. Authors use as a running example an E-CITY system providing municipality services to local communities.

Chapter 3 presents the different aspects of the Information Centric Networking (ICN) and analyses its security services. Based on a case study, the authors of this chapter demonstrate that the ICN meets the security requirements in e-government services.

Chapter 4 aims to bring out, the priority of enhancing the level of public awareness of Non-Communicable Diseases (NCDs). To ensure public responsiveness, this research focuses on creating an effective solution to prevent risky behavior. The authors construct "Sahtek", a social media solution developed on the fundamentals of Social Marketing, to better coach and promote awareness of NCDs prevention.

Chapter 5 deals with strengthening Cybersecurity in Singapore. The author 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.

Chapter 6 analyses the connection between e-Governance and corruption in Nigeria. The focus in this chapter is that the more entrenched e-Governance is adopted in contemporary governance the lower the corruption tendency in government service delivery. The authors conclude on the premise that e-governance reduces the strength of corruption in any country and more investments are needed to enhance this development.

Chapter 7 examines cybercrime and the challenges of securing Nigeria's cyberspace against criminal attacks. Author proffers solutions and recommends ways to make the country's cyberspace free from incessant criminal attacks.

Chapter 8 reviews the responsibilities of Internet Service Providers (ISPs) in securing their customers' network. The author finds out also whether there are legal provisions, or liabilities that are bindings on the ISPs to provide security for their customers.

Chapter 9 considers the trust and reputation of the digital environment of e-governance and m-governance in the world from the existing legal and judicial inkling. The author discusses how sufficient is the international policies and benchmarks on the use of ICT for e-Governance and m-Governance within and among nations to be trusted and judged to be of good repute among the users. The theoretical framework that this chapter hinges on is the Actor Network theory (ANT).

Chapter 10 presents a taxonomy of anomalous DBMS-access detection systems. Along with the taxonomy, a mechanism to detect insider threats is also proposed to construct a model for normative behavior for insiders which is extracted from logs of DBMS queries. In this book chapter, authors demonstrate that n-grams do capture the short-term correlations inherent in the application and outlines challenges pertaining to the design of more effective anomaly-based intrusion detection systems to detect insider attack.

Ryma Abassi
Carthage University, Tunisia

Aida Ben Chehida Douss
Carthage University, Tunisia

REFERENCES

Agrawal, S., Sethi, P., & Mittal, M. (2015). E-Governance: An Analysis of Citizens' Perception. *IUP Journal of Information Technology*, *11*(3), 34.

Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly*, *32*(2), 198–206. doi:10.1016/j.giq.2015.01.001

Mengistu, Zo, & Rho. (2009). *M-government: Opportunities and Challenges to Deliver Mobile Government Services in Developing Countries*. Academic Press.

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

connected to the Internet of Things, paralyzing targeted critical infrastructure such as power systems, government or business operations, causing substantial financial loss, spreading misinformation, and increasing anxiety, stress, insecurity and threat perception of the general public (Gross et al, 2016, p.286). The damages caused by cyber attacks and the serious national security threat presented by cyber attacks have provoked considerable alarms among governments and various sectors of society. Governments worldwide have put cybersecurity at the top of their agenda and formulated cybersecurity policy or carried out cybersecurity measures to combat cyber attacks. The Singapore government is no exception.

THE DEVELOPMENT TRAJECTORY OF E-GOVERNMENT IN SINGAPORE

Singapore became an independent sovereign state on 9 August 1965. At that time, Singapore was a third-world nation with no natural resources, limited capital and poor infrastructure. In order to develop the economy, the government adopted an export-led industrialization strategy to attract foreign investment in labour-intensive manufacturing (Van Dijck & Verbruggen, 1987, p.406). In the late 1970s, the government realized that IT was a key to improve its economic competitiveness. It restructured manufacturing production towards capital, technology and skill-intensive activities (Van Dijck & Verbruggen, 1987, p.406). Since 1980, the government has promoted infocomm development through a series of national Inforcomm Plans and electronic government (e-government) Masterplans so as to facilitate socio-economic development and increase efficiency in government agencies.

Singapore's e-government has gone through different stages of development over time. It has evolved in tandem with each national Inforcomm Plan (Ministry of Finance & Infocomm Development Authority of Singapore, 2006, p.12) to provide better public service delivery and improve interaction between the government and various sectors of society. Since 1980, the government has launched five e-government Masterplans, which are supported by six national Infocomm Plans. Being the first e-government Masterplan, the Civil Service Computerisation Programme (CSCP) (1980-1999) was supported by three National Infocomm Plans: The National Computerization Plan (1980-1985), The National IT Plan (1986-1991), and A Vision of an Intelligent Island: The IT2000 Report (hereafter IT2000) (1992-1999). National Computer Board (NCB) was established as a central agency to oversee the implementation of the CSCP. From 1980 to 1985, the focus of the CSCP was on transforming a labour-intensive, paper-based work environment into a capital-intensive, automated work environment through computerization (Tan et al., 2013, pp.2-3). Training programmes were implemented for civil servants to gain the

necessary computer knowledge and foreign professionals were recruited to solve the problem of inadequate ICT manpower in the civil service. Computerization greatly improved operational efficiency in the civil service. From 1986 to 1991, the focus of the CSCP was on using networking technologies to bring about the fusion of computer and communications. Electronic Data Interchange (EDI) was employed to allow government agencies, private companies and professional bodies to exchange data and documents electronically in a structured format (Hioe, 2001). For example, TradeNet, LawNet and MediNet were developed based on EDI to provide one stop services for the trading, legal and health care communities. EDI eliminated manual document handling procedures, thereby reducing administrative costs and turnaround time as well as achieving greater data accuracy, efficiency and productivity.

When it came to the 1990s, the focus of the CSCP was shifted to using the Internet as a new channel to engage citizens and civil servants. In March 1995, the Singapore INFOMAP (http://www.sg), which was Singapore's national website, was launched to provide the Singapore Yearbook and other government publications (Ministry of Information and the Arts, 1995, p.3). Following that, the Government Resources on the Internet (GRIN) network was established to make the Internet available to the entire civil service (Wong et al., 2003, p.350). GRIN facilitated the online presence of government agencies. In 1996, about 50 government websites were established and a government intranet was also established to "link up more than 16,000 computers across government ministries and statutory boards" (Lee, 1996). In July 1997, Singapore ONE (a.k.a. One Network for Everyone) was launched to deliver interactive, multimedia applications and services to everyone in Singapore through a nation-wide broadband network. By 2001, more than 200 multimedia applications had been deployed over Singapore ONE, such as real-time news and video-on-demand (Khoong, 2001). Singapore ONE could be accessible from homes, schools, workplaces, community centres, public libraries, or shopping malls (National Computer Board, 1997). The implementation of the Singapore ONE was regarded by the government as a concrete move to transform Singapore into an Intelligent Island (National Computer Board, 1997).

In 2000, the government launched the fourth National Infocomm Plan known as Infocomm 21. Infocomm 21 aimed at transforming Singapore into a prosperous E-economy and an infocomm-savvy e-Society (Infocomm Development Authority of Singapore, 2000, p.5). The first e-Government Action Plan (eGAP I), which was developed as part of Infocomm 21, was launched to deliver integrated and customer-oriented electronic services to citizens and businesses respectively via the eCitizen Portal (www.ecitizen.gov.sg) and the G2B Portal (www.business.gov.sg), allow faster and secure access to the government network via developing Broadband Infrastructure for Government (BIG) and Government Access Infrastructure (GATE), and promoting e-learning in the civil service via the provision of InfoComm

Education Programme (IEP) and Technology Experimentation Programme (TEP) (Ministry of Finance & Infocomm Development Authority of Singapore, 2003, pp.6-8). In 2003, the government launched the fifth National Infocomm Plan known as Connected Singapore. Connected Singapore aimed to leverage ICTs to achieve pervasive wireless connectivity, create new economic opportunities, and achieve higher efficiency, effectiveness and customer satisfaction in the government and business sectors (Infocomm Development Authority of Singapore, 2003, pp.8-18). The second Government Action Plan (eGAP II), which was developed as part of Connected Singapore, was launched to provide citizens with more integrated and personalized e-government services, foster citizen engagement through online consultation portal, and facilitate inter-operability and information sharing across agencies through The Service-Wide Technical Architecture (SWTA) (Ministry of Finance & Infocomm Development Authority of Singapore, 2003, pp.2-5).

In 2006, the government launched the sixth National Infocomm Plan known as the Intelligent Nation (iN2015) Masterplan. The iN2015 Masterplan was a 10-year masterplan with the aim of using ICT to turn Singapore into a digitally inclusive society and a more competitive economy (Infocomm Development Authority of Singapore, 2010, p.3). Following the direction of the iN2015 Masterplan, the fourth e-government Masterplan known as iGov 2010 was launched to (1) increase reach and richness of e-services; (2) increase citizens' mindshare in e-engagement; (3) enhance capacity and synergy in government; and (4) enhance national competitiveness advantage (Ministry of Finance & Infocomm Development Authority of Singapore, 2006, p.4). In 2011, the fifth e-government Masterplan known as eGov 2015 was launched to increase the interaction among the government, citizens and businesses through three strategic thrusts: (1) co-creating for greater value, where users were empowered to co-create new services by using available government datasets; (2) connecting for active participation, where new channels such as crowdsourcing tools were used to engage citizens and tap on their views; and (3) catalysing Whole-of-Government transformation, where public infrastructure and services were transformed through cloud computing and the Government Business Analytics programme (Ministry of Finance et al., 2011, pp.6-15).

After more than three decades of development, e-government in Singapore has become more and more sophisticated. As a result, Singapore has a remarkable performance in e-government and high ranking in international e-government surveys (See Table 1 in Appendix 1 and Table 2 in Appendix 2). For example, it ranked fourth in United Nations E-government Survey 2016 (United Nations, 2016, p.111) and has been ranked first in Waseda–IAC International E-Government Ranking Survey for three consecutive years from 2015-2017. Singapore is well regarded as one of the regional and world leaders in e-government. To further embrace the benefits of digital transformation, the government in November 2014 launched the

Smart Nation initiatives, with an aim to merge information technology into five key domains: public sector services, business productivity, transport, home and environment, and health and enabled ageing (Smart Nation Singapore, 2017). It is anticipated that the use of the latest technologies can increase citizens' everyday convenience and improve their quality of life, facilitate greater business efficacy and support innovation in different areas (GovTech, 2017).

THE PROBLEMS OF CYBERCRIME AND CYBER ATTACKS IN SINGAPORE

However, Singapore's growing dependence on information technology to develop the economy and society not only increases its vulnerability to cybercrime, but also increases its vulnerability to cyberterrorism with potentially catastrophic consequences. Over the past decade, cybercrime in Singapore has been increasing in frequency and severity. Singaporeans have become targets of cyber criminals due to their increasing reliance on the Internet to obtain information, have online shopping and transaction, and connect with friends (Cyber Security Agency of Singapore, 2017a, p.26). They fall victim to different types of cybercrime, including e-commerce scam, Internet love scam, email impersonation scam, credit-for-sex scam, multiple payment online purchase scan, phony PayPal email scam, and cyber extortion (Singapore Police Force, 2015; Singapore Police Force, 2017b). In Singapore, e-commerce scam, Internet love scam and credit-for-sex were the top three categories of online cheating cases (Cyber Security Agency of Singapore, 2017a, p.26). In 2016, there were 2,105 e-commerce scam cases and caused the loss of S$1.5 million (Singapore Police Force, 2017a, p.7). Internet love scam has become more frequent and caused substantial financial losses of S$24 million in 2016 (Singapore Police Force, 2017a) (See Table 3 in Appendix 3). In the first half of 2017, there were 349 cases of Internet love scam, causing the loss of S$22.1 million (Singapore Police Force, 2017b, p.3).

Police investigations revealed that scammers befriended their victims through social media platforms and online dating (Singapore Police Force, 2011, p.6). Most of these scammers were foreigners who used various cons such as being detained by Customs to dupe victims of their money. The borderless nature of the Internet makes cybercrimes difficult to solve (Sun, 2017 August 29). The continuous rise in cybercrime has become a major concern for the police and law enforcement agencies.

Meanwhile, the nation's increasing use of the Internet also creates opportunities for attackers to cause disruption or destruction. In fact, Singapore has been the target of cyber attacks for more than a decade. Four waves of Trojan email attacks were launched against civil servants in several ministries between 2004 and 2005 (Loh,

2010, p.43). In 2009, Singapore became the target of Trojan e-mail attacks again when the Asia-Pacific Economic Cooperation (APEC) meetings were held in the nation. At least seven waves of Trojan e-mail attacks were launched against members of the APEC Organising Committee and delegates of various APEC countries to infiltrate their computers and extract privileged information (Loh, 2010, p.44). "The malware used in these attacks were highly sophisticated and stealthy enough to evade the detection of most anti-virus programs" (Loh, 2010, p.45). Besides, the establishment of anti-tracking operation set-ups indicated that the perpetrators were both technically savvy and security conscious. In recent years, cyber attacks in Singapore have become more frequent and come in different forms, inflicting varying levels of damage and status. They have provoked considerable alarm in many government agencies and received extensive media attention. In 2013, a wave of cyber attacks occurred in Singapore. A hacker who went by the moniker "The Messiah" performed a series of high-profile attacks from March to November 2013 (Ng, 2015 January 23). He hacked into the Fuji Xerox web server to steal bank statements belonging to 647 premium clients of Standard Chartered Bank (Sreedharan, 2013 December 7). Besides, he hacked into the websites of People's Action Party Community Foundation (PCF), the Ang Mo Kio Town Council, Singapore's newspaper *Straits Times*, and a fan site for popstar Sun Ho (Ng, 2015 January 23). He also posted an online video threatening that the infamous hacker group Anonymous, which he claimed to be part of, would "go to war" with the Singapore Government by having aggressive cyber intrusion if the government implemented the internet licensing framework (Lee, 2013). The hacker was arrested in early November. However, another wave of cyber attacks was launched against the nation in the same month, defacing the websites of Seletar Airport, Prime Minister's Office, the Istana, which was the official residence of President Tony Tan, and 13 schools. Meanwhile, the website of the Singapore Art Museum was breached twice in November, leading to its data containing personal information of over 4,000 individuals being illegally published on an overseas website (Kok, 2013 November 30).

In early 2014, there was a security breach of the IT system of the Ministry of Foreign Affairs. But the affected devices were immediately isolated and security measures were appropriately implemented to further strengthen the network. In June the same year, SingPass accounts, which were set up for Singapore residents to perform online transactions with government agencies, were breached (Ng, 2014 June 5). A total number of 1,560 SingPass accounts were breached while 419 of these users had their passwords illegally reset (Ng, 2014 June 5). Consequently, security measures were strengthened by introducing two-factor authentication for access to e-government services (TODAY, 2017 May 12). In March 2015, a cyber attack was launched against the website of Curtin University's Singapore campus.

The defaced website displayed a smiley emoticon and a militant group's flag with the message "Hacked by Islamic State (ISIS) — we are everywhere" (TODAY, 2015 March 10). As a result, the website was taken offline for a day and then restored after resolving the security breach. In 2016, cyber attacks of website defacements and phishing attacks were launched against the government sector while e-mail scams, phishing and ransomware attacks were launched against individuals and small and medium enterprises (SMEs) (Cyber Security Agency of Singapore, 2017a, p.5). Ransomware attacks were launched against the healthcare sector, which made patient data inaccessible to medical practitioners (Cyber Security Agency of Singapore, 2017a, p.4). A total number of 19 CryptoLocker and Locky ransomware cases from individuals and SMEs were reported to the Cyber Security Agency of Singapore (CSA) (Cyber Security Agency of Singapore, 2017a, p.6). Meanwhile, over 60 command and control servers, nearly 1,800 website defacements, and over 2,500 phishing URLs were detected in Singapore in 2016 (Cyber Security Agency of Singapore, 2017a, p.6). The statistics indicated that cyber attacks in Singapore have become more frequent, widespread and severe.

In February 2017, a cyber attack was launched against the I-net system of the Ministry of Defence (MINDEF), which resulted in the theft of the personal data of 850 national servicemen and employees from MINDEF (Lee, 2017 March 1). The stolen personal data included National Registration Identity Card (NRIC) numbers, dates of birth, and telephone numbers (Chua, 2017 April 3). Based on the investigation, MINDEF's Deputy Secretary for Technology said that this was a targeted and well-panned attack with the aim of accessing official secrets (Loke, 2017 February 28). But no classified military data was lost in the attack because the data was stored on a separate system that was not connected to the Internet (Loke, 2017 February 28). In April 2017, advanced persistent threat (APT) attacks were launched against the National University of Singapore (NUS) and Nanyang Technological University, with the aim of stealing government information and research documents. Investigations by the CSA indicated that the attacks on these two universities were not coordinated because "they did not originate from the same place, and were not conducted by the same people" (Ong, 2017 May 12). In May the same year, the WannaCry ransomware attack, which locked users' files unless they paid a designated sum in virtual currency, were launched against the digital directory service at some shopping malls in Singapore (Channel NewsAsia, 2017 May 14). But no money or bitcoins were paid to the hackers and the affected systems were fixed and fully restored the following day (Channel NewsAsia, 2017 May 14). While the WannaCry ransomware attack had infected over 230,000 computers in about 150 countries (Mullin and Lake, 2017 August 4), the scale of the attack was moderate in Singapore without affecting any government agencies and critical information infrastructure (Toh, 2017 May 13).

Since cyber attacks are increasing in frequency, scale, diversity, and sophistication and have a much broader target, they inflict wide-ranging damage on the victim and have far-reaching impact on the economy and society. It is apparent that no country, institutions or individuals can be completely immune to cyber attacks. Singapore is likely to remain a prime target for cyber attacks for years to come, especially when it transforms into a Smart Nation and boosts the digital economy. In fact, Singapore in 2014 ranked fifth in Cyber Vulnerability Index (CVI) in the survey conducted by Deloitte, indicating that it was nine times more vulnerable to cyber attack than other Asia-Pacific economies (Deloitte, 2016, pp.19-20). Hence, the government needs to be more vigilant and devote more time and resources to strengthening its cyber security.

CYBERSECURITY MEASURES IN SINGAPORE

The Implementation of Infocomm Security Masterplans

The formulation and implementation of Infocomm Security Masterplans represents the government's continuous commitment and unremitting efforts to provide a secure and reliable infocomm environment that is vital to the functioning of the economy and society. Infocomm Security Masterplan provides a strategic roadmap for strengthening the nation's cybersecurity. It is reviewed regularly to ensure its relevance and applicability so that the nation can keep pace with the constantly changing cyber threat landscape and address evolving cybersecurity challenges. In February 2005, the first Infocomm Security Masterplan was developed through a multi-agency effort under the guidance of the National Infocomm Security Committee (NISC) (Infocomm Development Authority of Singapore, 2005). It was a three-year Masterplan having a budget of S$38 million to build new capabilities within the public sector to manage internal and external cyber threats and enhance the overall cybersecurity of the nation (Infocomm Development Authority of Singapore, 2005). One of the key initiatives was the establishment of National Cyberthreat Monitoring Centre (NCMC), which consisted of the Cyber-Watch Centre (CWC) to provide the 24-hour monitoring of critical IT installations in the public sector and Threat Analysis Centre (TAC) to analyse cyber-threat data.

In 2008, the second Infocomm Security Masterplan was implemented to protect CIIs in the nation and enhance the competencies of public sector, private sector and the general public against cyber threats (Infocomm Development Authority of Singapore, 2008). It was a five-year Masterplan having the budget of S$70 million to carry out key initiatives (Infocomm Development Authority of Singapore, 2008). Sector-specific infocomm security programmes were developed to assess and develop

customised solutions that could meet unique security requirements of CII owners (Infocomm Development Authority of Singapore, 2008). Meanwhile, Cyber Security Awareness Alliance was formed to raise awareness and adoption of good cyber security practices among businesses and individuals through seminars and workshops (Infocomm Development Authority of Singapore, 2008). It co-organized some well received initiatives such as National Infocomms Security Competition and Infocomm Security Seminar (Ministry of Home Affairs, 2014). In 2013, a five-year National Cyber Security Masterplan 2018 (NCSM2018) was implemented to increase the level of maturity and sophistication of Singapore's infocomm security (Infocomm Development Authority of Singapore, 2013a, p.4). Some of the key initiatives that the government undertook included (a) the implementation of the CII Protection Assessment programme and the National Cyber Security Exercise programme to enhance security and resilience of CIIs to deal with sophisticated cyber attacks; (b) upgrading the detection capabilities of CWC and the analysis capabilities of TAC via advanced techniques and technologies; (c) raising cybersecurity security awareness and promoting the adoption of appropriate security measures amongst businesses and individuals through the implementation of the Cyber Security Awareness and Outreach programme; and (d) increasing the number and skill levels of cybersecurity professionals through the implementation of the National Cybersecurity R&D Programme and the establishment of the DigiSAFE Cyber Security Centre (Infocomm Development Authority of Singapore, 2013a, pp.12-7). In July 2016, National Cybercrime Action Plan (NCAP) was implemented to deter, detect and disrupt cybercriminal activities effectively. The government's strategies to combat cybercrime could be grouped into four priority areas, which included (a) educating and empowering the public to stay safe in cyberspace through outreach programme and a one-stop self-help portal; (b) enhancing the government's capabilities to combat cybercrime through the use of the latest technologies and strengthening coordination between Singapore Police Force (SPF) and government agencies; (c) strengthening cybersecurity legislation; and (d) strengthening local partnerships and international engagements (Ministry of Home Affairs, 2016, pp. 2-3).

The Establishment of New Institutions to Handle Cybersecurity-Related Issues

The growing volume and sophistication of cyber attacks poses a serious threat to national security, public safety, and the economic and social well-being of a nation. New institutions need to be established to handle cyber threats and attacks more effectively. They possess legal authorities, financial resources, specialized expertise, skills, technologies and equipment required for monitoring, detecting, responding to, recovering from and preventing cyber attacks. Over the past two decades, the

government has established different institutions to handle cybersecurity-related issues. In October 1997, the Singapore Computer Emergency Response Team (SingCERT) was established by the Infocomm Development Authority of Singapore (IDA), in collaboration with NUS to "facilitate the detection, resolution and prevention of security related incidents on the Internet" (The Singapore Computer Emergency Response Team, 2015). Beyond its work in Singapore, SingCERT collaborated with foreign CERTs to manage cyber incidents across borders. It was a founding member of the Asia Pacific Computer Emergency Response Team (APCERT) in 2002 to support the cooperation between national CERTS in the Asia Pacific region (Tan, 2004). In 2007, the CWC was established by IDA. It was staffed with 12 security professionals comprising security engineers and analysts and adopted new security tools such as security event correlation (Yu, 2006) to provide alerts on cyber attacks for the relevant government agencies so that appropriate preventive measures could be taken in a timely manner (Infocomm Development Authority of Singapore, 2013b). In 2014, the CWC enhanced its detection capabilities to detect network data loss and malware threat through the use of advanced technology such as intrusion detection sensors and intelligence feeds (Infocomm Development Authority of Singapore, 2013b). In the first half of 2018, the government will call a tender for the first Government Security Operation Centre (SOC), which will replace the CWC to detect cyber threats through the use of artificial intelligence and the analytics smarts (Tham, 2017 May 25).

In 2009, the Singapore Infocomm Technology Security Authority (SITSA) was established under the Internal Security Department of the Ministry of Home Affairs (MHA) as a specialist authority to safeguard Singapore's national security against external threats, such as cyber-attacks and cyber-espionage (Cyber Security Agency of Singapore, 2016a, p.7). Its main responsibilities included protecting CII in the water, energy, transportation and finance sectors against cyber attacks, raising the level of readiness to counter cyber-attacks against the nation, and creating a process for monitoring and reporting security incidents (Lemon, 2009). Recognizing that there was a lack of skilled cyber security professionals in the nation, the government in November 2014 set up a Cyber Security Lab (CSL) within the Home Team Academy (Phneah, 2013), which is one of the seven departments of the MHA. Its main responsibility was to enhance the capabilities of officers, CII regulators and operators in preventing, detecting and responding to cyberthreats through training (Phneah, 2013). Courses were split into three levels: basic, intermediate, and advanced (Ng, 2014). The curriculum covered a wide range of topics, including cyber security fundamentals, malware analysis and digital forensics (Networks Asia, 2016). Apart from teaching individual cyber skills, CSL also taught team-based cyber skills through group dynamic exercises (Ng, 2014). The first batch of training participants came from various sectors, including Monetary Authority of

Singapore, Infocomm Development Authority, the Land Transport Authority and the Energy Market Authority (Ng, 2014). Besides, CSL was responsible for forging closer public-private sector collaboration in the protection of CII (Phneah, 2013).

In April 2015, CSA was established as a national agency under the Prime Minister's Office and was managed administratively by the Ministry of Communications and Information (MCI) (Cyber Security Agency of Singapore, 2016a, p.7). It subsumed SingCERT and SITSA to "provide centralised supervision over the nation's key cyber security functions" (Ng, 2015), "lead the cyber security master plan" (Tan, 2015 January 28) and "carry out both cybersecurity capability development and crisis management across all CII sectors" (The Ministry of Communications and Information and the Cyber Security Agency of Singapore, 2017, p.1). CSA's responsibilities included coordinating public- and private-sector efforts against cyber threats (Ng, 2015) and enhancing the cybersecurity awareness of the general public through outreach programmes (Cyber Security Agency of Singapore, 2017b). It was also "empowered to develop and enforce cybersecurity regulations, policies, and practices" (Cyber Security Agency of Singapore, 2016a, p.7). For example, CSA in late 2015 commenced work on a new Cybersecurity Bill and in July 2017 released the Bill for public consultation. CSA has been working closely with the Smart Nation Programme Office (SNPO) to ensure that there will be cybersecurity-by-design for the Smart Nation project (Kwang, 2015 August 4). In 2015, the Cybercrime Command was established by the SPF as a unit within the Criminal Investigation Department (Bhunia, 2017a) to "develop specialist expertise in cyber investigation, digital forensics and cybercrime policy, and also to improve Police readiness for, and response to, emerging cyber threats" (Bhunia, 2017a). Besides, it oversees full-time Cybercrime Response Teams (CRTs) (Networks Asia, 2016), which was set up by the SPF in all six of its frontline Police Divisions in December 2015 to enhance cybercrime response capabilities (Bhunia, 2017a). CRTs "have a level of proficiency and expertise in investigations and digital forensics" (Networks Asia, 2016). In February 2017, the Cybercrime Command created the "Alliance of Public-Private Cybercrime Stakeholders" to forge active collaboration between law enforcement and the private sector and enhance cybercrime awareness in the private sector to detect, deter and prevent cybercrime (Ministry of Home Affairs, 2017a). The Alliance serves as a new public-private industry platform to allow 40 partners from global IT companies, the financial industry, E-commerce platforms, remittance agencies and telecommunications service sector to strengthen communication with the police and they convene biannually to share updates on cybercrime (Cashshield, 2017). It helps accelerate the pace at which the public and private sectors can take preventive measures or collective action against cybercrimes, especially those that are transnational in nature (Tan, 2017 July 5).

Developing a Robust Legislative Framework

Cybercrime legislation is an integral component of a national cybersecurity strategy. The advent of the Internet gave rise to new forms of crime (Leung, 2003, p.4) that could no longer be addressed by existing legislation. As a result, new and proper legislation is enacted to specifically investigate, prosecute and adjudicate cybercrime. It clearly defines the acts constituting offences and corresponding penalties that can create a strong deterrent effect. To remain effective, cybercrime legislation is regularly reviewed and updated to keep up with the rapidly evolving cybercrime landscape. In Singapore, the landmark Computer Misuse Act (CMA) was enacted in 1993 to introduce "specific offences and penalties targeted at computer crimes" (Kor, 2017). Being modelled after the United Kingdom's Computer Misuse Act 1990, the CMA criminalized unauthorized access to computer material, unauthorized modification of computer material, unauthorized access with intent to commit an offence involving property, fraud, dishonesty or which causes bodily harm, unauthorized use or interception of computer service, and abetments (Singapore Statutes Online, 1993). In 1998, the Computer Misuse (Amendment) Act was introduced to "provide for enhanced penalties proportionate to the different levels of potential and actual harm caused" (Zhou, 2011), criminalize unauthorized obstruction of use of computer and unauthorized disclosure of access code, grant police officer the power to access decrypted data when conducting an investigation, and make it an offence to obstruct the lawful exercise of the powers of a police officer or refuse to assist a police officer in an investigation (Singapore Statutes Online, 1998). In 2003, CMA was amended to fight against cyberterrorism by allowing "police to take pre-emptive action based on credible information before hackers strike to protect computer networks from unauthorized entry" (CNN.com, 2003 November 11). "In 2013, the CMA was amended to include cybersecurity measures and renamed the Computer Misuse and Cybersecurity Act (CMCA)" (Ministry of Home Affairs, 2017b). The CMCA empowered the Minister of Home Affairs to issue a certificate to authorise or direct any person or organisation to take measures necessary to prevent, detect or counter cyber threats to Singapore's national security, essential services, defence or foreign relations (Chang, 2013, p.13). Anyone convicted for obstruction or non-compliance could face a fine of up to S$50,000 or imprisonment for up to 10 years or both (Chang, 2013, p.14). In April 2017, the CMCA was amended to handle the evolving tactics of cybercriminals, the transnational nature and increasing scale of cybercrime (Ministry of Home Affairs, 2017b). There were four key amendments. Firstly, it criminalized the act of obtaining, retaining, supplying and transmitting personal information obtained through cybercrime (OrionW LLC, 2017). Secondly, it criminalized the act of obtaining or retaining certain specified items which could be used to commit a computer crime (OrionW LLC, 2017). Thirdly, it extended the

territorial scope of the CMCA by criminalizing cybercrimes committed overseas (OrionW LLC, 2017). Fourthly, it allowed prosecutors to amalgamate cybercrime charges in certain circumstances (OrionW LLC, 2017).

After several amendments, the range and scope of CMA provisions have been progressively enhanced to cope with the changing tides of cyber-crime and technology (Kor, 2017). Nevertheless, the government recognized that the CMCA alone was not enough to deal with the rapidly evolving cybersecurity landscape of Singapore, especially when cyber attacks had become more frequent, sophisticated and impactful (Cyber Security Agency of Singapore, 2017c). A new cybersecurity legislation was needed to allow the government to take pro-active measures to protect CII across the public and private sectors, facilitate sharing of cybersecurity information across critical sectors and respond to cyber threats in an expedient manner (Cyber Security Agency of Singapore, 2017c). For this reason, a proposed Cybersecurity Bill was released in July 2017 for public consultation that ended in early August. It is expected that the new Cybersecurity Bill will be introduced to Parliament in 2018.

Strengthening Regional and International Cooperation

Given the cross-border nature and complexity of cybercrime and cyber threats, no single country can successfully combat cybercrime or cyber threats alone using the traditional siloed approach. Meanwhile, the shortage of cyber security workforce presents a challenge to combat cybercrime or cyber threats in a timely and efficient manner. Jurisdictional issues also present a challenge to combat cybercrime and cyber threats because perpetrators or organized crime gangs are located overseas. Under these circumstances, bringing perpetrators to justice requires coordinated effort and collaborative response from governments, law enforcement agencies, and stakeholders in different regions. It is only by having collective efforts and strengthening international cooperation that capacity building, the sharing of cyber threat intelligence, the collection of evidence and the training of cybersecurity professionals can be facilitated to combat cybercrime and cyber threats more effectively. On the international front, Singapore has been actively enhancing strategic partnership with Western counterparts in the area of cyber security. For example, Singapore and the United States in August 2016 signed a cybersecurity Memorandum of Understanding (MOU) to formalise their commitment to work together in key areas that included regular information exchanges between CERTS in two places, conducting joint cybersecurity exercises, sharing of best practices on CII protection, and coordination in cyber incident response (Cyber Security Agency of Singapore, 2016b). Singapore also had bilateral agreement with France, the United Kingdom, the Netherlands, Australia and Germany, which covered cybersecurity cooperation in key areas including regular information exchanges, sharing of best practices, and

cyber security talent development (Bhunia, 2017b). On the regional front, Singapore has been continuously forging closer cybersecurity cooperation with other Asian countries (Infocomm Development Authority of Singapore, 2013a, pp.23-4). For example, Singapore and India in 2015 signed a cybersecurity MOU to establish formal cooperation in key areas such as cooperation between CERTS in these two places, sharing of best practices and joint training and research (Bhunia, 2017b). In September 2017, Singapore and Japan signed a Memorandum of Cooperation to strengthen cybersecurity awareness, information exchanges, sharing of best practices and joint regional capacity building (Tan, 2017 September 19). Meanwhile, Singapore has been actively contributing to cybersecurity capability building in the Association of Southeast Asian Nations (ASEAN) region through the annual ASEAN CERT Incident Drill (ACID), ASEAN Network Security Action Council (ANSAC), and ASEAN cybersecurity and cybercrime workshops (Cyber Security Agency of Singapore, 2016a, p.45). In September 2017, Singapore announced that it would use S$1.5 million from the ASEAN Cyber Capacity Building Programme (ACCP) it set up in 2016 to train incident responders and operators in the ASEAN region for the next three years (Bhunia, 2017c). It is expected that up to 18 candidates will be trained and equipped with knowledge about "security operations centre (SOC) operations and management, and other relevant technical areas of cybersecurity" (Bhunia, 2017c) so that they will be able to monitor and respond to cyber threats effectively. Singapore's devotion to strengthening regional coordination and cybersecurity capability building has contributed to stronger regional cohesion and ensured a safe and secure cyberspace.

Raising Cybersecurity Awareness Among Businesses and Individuals

Cybersecurity is a shared responsibility. To avoid becoming easy targets for cyber criminals, businesses and individuals are also responsible for engaging in appropriate online behaviour and taking precautionary measures to protect their computers. Nevertheless, enterprises in Singapore have yet to adopt sufficient cybersecurity practices to address relevant cybersecurity risks and protect their data assets such as customer information, financial information and intellectual property. In 2017, a survey conducted by Accenture revealed that one in four cyberattacks resulted in an actual security breach in large enterprises in Singapore, which equated two to three effective attacks per month for the average company (Accenture, 2017a, p.4; Accenture, 2017b). Nevertheless, it took months or more than a year for large enterprises to detect such security breach (Accenture, 2017a, p.4). While facing frequent cyberattacks, only 41 percent of large enterprises surveyed would invest extra money to protect customer data, which was 3 percent lower than the global

average (Accenture, 2017a, p.5). Besides, only 31 percent of large enterprises surveyed would invest extra money to mitigate against financial losses caused by security breach, and only 8 percent of large enterprises surveyed would invest in cybersecurity training, which was much lower than the global average of 17 percent (Accenture, 2017a, p.5). Meanwhile, SMEs that accounted for 99 percent of the nation's enterprises and 50 percent of the nation's Gross Domestic Product (GDP) (www.gov.sg, 2017) did not have sufficient cybersecurity measures due to the lack of awareness, cost, and the shortage of IT staff (Channel NewAsia, 2016 April 11). In fact, adopting a proactive approach to cybersecurity matters to large enterprises and SMEs because any security breach can lead to incalculable losses in terms of finance, reputation, consumer trust and loyalty. A proactive approach to cybersecurity requires enterprises to regularly conduct cybersecurity risk assessment in order to find out and address security vulnerabilities in computer systems in advance. This can also help enterprises identify cybersecurity priorities when facing budget constraints and the shortage of IT staff. For enterprises that do not have cybersecurity budget constraint, they can adopt data breach prevention tools to ensure data safety. For enterprises that have budget constraint, they can adopt a more cost-effective but often overlooked approach to cybersecurity by regularly updating software patches. They can also sign up for alerts and advisories at the website of SingCERT (www.csa.gov.sg/singcert) on how to pre-empt cyber incidents (Lee, 2017 May 30).

Meanwhile, it is also important to strengthen the cyber defence capability of enterprises by providing on-site or online cybersecurity training for their employees. Cybersecurity training should be provided on a regular basis and make it compulsory for all the employees. It can raise the cybersecurity awareness of employees and ensure that they stay alert for the latest cyber security threats. Employees should be instructed to use strong password and change it frequently. They should also be instructed to report any suspicious links or emails they receive to IT staff. In October 2015, the government introduced a free plug-and-play digital Employee Cyber Security Kit (ECS Kit) to help enterprises "achieve a structured employee education program with minimal time, investment and manpower" (Hui, 2015 Oct 27). The ECS Kit took employees through the five stages of behavioural change in the Transtheoretical Model: awareness, design, knowledge, action and reinforcement (Networks Asia, 2015). The CSA also reaches out to SMEs to promote the awareness and adoption of cyber security practices by regularly holding talks and conferences (Lee, 2017 May 30).

There is also a pressing need to enhance cybersecurity awareness among individuals and change their attitudes and behaviours towards cybersecurity. Both international and local surveys indicate that Singaporeans do not take enough precautionary measures to protect their computing devices. Internationally, the Global Digital Assets survey conducted by McAfee showed that while 73 percent

Singaporeans surveyed were familiar with online security risks such as identify theft or monetary theft, about 87 percent of Singaporeans surveyed did not take any precautionary measures to protect their tablets and about 69 percent of Singaporeans surveyed did not install any security software to protect their smartphones (Precious Communications, 2013). Another problem was that 50 percent of Singaporeans surveyed used the same password for all websites (Precious Communications, 2013). This undermined password security and put their online accounts at risk because hackers could easily gain access to all of their accounts on every website as long as hackers could crack the password. Locally, Cybersecurity Public Awareness Survey conducted by the CSA in August 2016 indicated that many Singaporeans had not integrated good cyber hygiene practices into their daily routines although they agreed that individuals were responsible for cybersecurity. According to the survey, 73 percent of 2,000 respondents surveyed agreed that all Singaporeans had a role to play in cybersecurity (Cyber Security Agency of Singapore, 2017d, p.12). While 86 percent of respondents surveyed created strong password by using a combination of letters, numbers and symbols (Cyber Security Agency of Singapore, 2017d, p.6), many of them did not store their passwords securely. While 33 percent of respondents stored passwords on their computers or wrote down passwords on paper, 31 percent of respondents used the same password for work and personal accounts (Cyber Security Agency of Singapore, 2017d, p.7). These storage methods were not secured at all because anyone who had physical access to that paper or the computers could steal passwords easily and compromise victims' online accounts. Besides, passwords stored in the computers could also be stolen by hackers easily if no encryption was used. The survey also found that 24 percent of respondents did not enable Two-Factor Authentication (2FA) when the option was available because they thought that it was time consuming and unnecessary (Cyber Security Agency of Singapore, 2017d, p.7). According to the survey, 41 percent of respondents did not conduct virus scan on files or devices before opening because most of them thought that it was time consuming to do so (Cyber Security Agency of Singapore, 2017d, p.11). In addition, 32 percent of respondents did not install security applications on their mobile phones because they thought that such applications were unnecessary and took up too much storage space (Cyber Security Agency of Singapore, 2017d, p.4). Both the international and local survey results showed that the government needs to raise cybersecurity awareness among individuals and introduce good cyber hygiene practices to them through different channels. Recognizing that it is important to establish good cyber hygiene at an early age, the government produced and distributed a series of activity book to educate primary school students on cyber safety and personal data protection (GoSafeOnline, 2017). The books contained fun and engaging activities such as word search and maze for students to learn about cybersecurity knowledge in an interesting way (Cyber Security Agency of

Singapore and Personal Data Protection Commission, 2016). They also contained parent-child activities to encourage parents to engage in meaningful conversations with their children about cyber safety and reinforce the values children have learnt in the book. Besides, the government made use of television program to cultivate a cybersecurity-conscious culture and educate ordinary citizens on cyber crime prevention. Episodes covering cybercrimes such as ransomware were produced and broadcast on free-to-air television channels (Cyber Security Agency of Singapore, 2017a, p.38). The government also established the GoSafeOnline and SingCERT websites to provide Internet users with up-to-date cybersecurity news, resources and tips to protect their computing devices from cyber threats (Cyber Security Agency of Singapore, 2017a, p.38).

FINDINGS AND DISCUSSION

The case study of Singapore shows that the government has adopted a proactive, holistic and cooperative approach to cybersecurity in order to tackle ever-increasing cybersecurity challenges. It has regularly reviewed and updated cybersecurity measures to ensure their effectiveness and strengthened its defence capabilities over time through coordinating national effort with public and private sectors and cooperating with regional and international counterparts. The government has demonstrated strong political will and long-term commitment to combating cyber attacks and ensuring a safe and secure cyberspace. 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 mitigate and avoid cyber risks or threats, detect and respond to cyber attacks in a timely manner, and strike a balance between cybersecurity and efficiency. Besides, cybersecurity is a shared responsibility. The government alone is insufficient to tackle an unprecedented increase in volume, sophistication and severity of cyber attacks. The business sector and individuals also play an important role in cybersecurity.

FUTURE RESEARCH DIRECTIONS

The development of cybersecurity strategy or measures is an ongoing effort. At the time of this study, the new Cybersecurity Bill has not been introduced to Parliament. Future studies can examine the impact of new cybersecurity legislation on combating cyber attacks in the nation or compare the new cybersecurity legislation

with cybersecurity legislation in other Asian or Western countries. Future studies can also examine citizens' views on cybersecurity measures or their cybersecurity awareness so that the government can find ways to strengthen current measures or introduce new measures to protect citizens from cyber attacks.

CONCLUSION

To conclude, the government in Singapore has made unremitting efforts to combat cybercrime and cyber attacks. Facing the increasing volume and sophistication of cyber attacks, the government has demonstrated strong political will and determination to introduce, review and improve cybersecurity measures so that the nation has a safe and trusted cyberspace and maintains high cybersecurity standards, which are vital to the economic and social well-being of the nation. Looking forward, the government's commitment to carrying out cybersecurity measures will make the nation stronger, safer and more secure.

REFERENCES

Accenture. (2017a). *Building Confidence: Facing the Cybersecurity Conundrum in Singapore*. Retrieved November 18, 2017, from https://www.accenture.com/t20170406T010037Z__w__/sg-en/_acnmedia/PDF-38/Accenture-Facing-Cybersecurity-Conundrum-Singapore.pdf

Accenture. (2017b). *Accenture Survey: One in Four Cyberattacks in Singapore Result in a Security Breach, Yet Most Organisations Remain Confident in Their Ability to Protect Themselves*. Retrieved November 18, 2017, from https://www.accenture.com/sg-en/company-newsroom-accenture-survey-one-four-cyberattacks

Al-Rodhan, N. R. F. (2011). *The Politics of Emerging Strategic Technologies: Implications for Geopolitics, Human Enhancement and Human Destiny*. London: Palgrave Macmillan. doi:10.1057/9780230304949

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook*. Hoboken, NJ: Wiley. doi:10.1002/9781118241530

Bhunia, P. (2017a). *Public-Private Alliance Launched by Singapore Police Cybercrime Command*. Retrieved November 6, 2017, from http://opengovasia.com/articles/7778-public-private-alliance-launched-by-singapore-police-cybercrime-command

Bhunia, P. (2017b). *Singapore Enters into Seventh Bilateral Agreement on Cybersecurity Cooperation*. Retrieved November 13, 2017, from http://opengovasia.com/articles/7785-singapore-enters-into-seventh-bilateral-agreement-on-cybersecurity-cooperation

Bhunia, P. (2017c). *New Steps from Singapore Government to Build Cybersecurity Capabilities in Singapore and ASEAN Region in Collaboration with Industry*. Retrieved November 13, 2017, from http://opengovasia.com/articles/8020-new-steps-from-singapore-government-to-build-cybersecurity-capabilities-in-singapore-and-asean-region-in-collaboration-with-industry

Cashshield. (2017). *A Pact Against CyberCrime: CashShield and the Singapore Police Force Join Forces to Secure the Digital World*. Retrieved November 6, 2017, from http://www.cashshield.com/a-pact-against-cybercrime-cashshield-and-the-singapore-police-force-join-forces-to-secure-the-digital-world/

Chang, W. (2013). *Amendments to Singapore's Computer Misuse Act*. Retrieved November 4, 2017, from http://www.cnplaw.com/en/media/files/services/EFPLP.pdf

Channel NewAsia. (2015, May 11). *Cyber Security Agency, IDA Maintain High Level of Vigilance over Govt Networks: Yaacob*. Retrieved October 26, 2017, from http://www.channelnewsasia.com/news/singapore/cyber-security-agency-ida-maintain-high-level-of-vigilance-over--8264556

Channel NewAsia. (2016, April 11). *New Cybersecurity Act to be Tabled in 2017: Yaacob Ibrahim*. Retrieved November 18, 2017, from http://www.channelnewsasia.com/news/singapore/new-cybersecurity-act-to-be-tabled-in-2017-yaacob-ibrahim-8088054

Channel NewsAsia. (2017, May 14). *Tiong Bahru Plaza's Digital Directory Hit by Global Ransomware Attack: Mall Operator*. Retrieved October 30, 2017, from http://www.channelnewsasia.com/news/singapore/tiong-bahru-plaza-s-digital-directory-hit-by-global-ransomware-8846096

CNN.com. (2003, November 11). *Singapore Clamps Down on Hackers*. Retrieved November 4, 2017, from http://edition.cnn.com/2003/TECH/internet/11/11/singapore.internet.reut/

Cyber Security Agency of Singapore. (2016a). *Singapore's Cybersecurity Strategy*. Retrieved November 5, 2017, from https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

Cyber Security Agency of Singapore. (2016b). *Singapore Strengthens Partnership with the United States*. Retrieved November 13, 2017, from https://www.csa.gov.sg/news/press-releases/singapore-us-mou

Cyber Security Agency of Singapore. (2017a). *Singapore Cyber Landscape 2016*. Retrieved October 29, 2017, from https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecyberlandscape2016.ashx?la=en

Cyber Security Agency of Singapore. (2017b). *Our Organisation*. Retrieved November 5, 2017, from https://www.csa.gov.sg/about-us/our-organisation

Cyber Security Agency of Singapore. (2017c). *MCI and CSA Seek Public Feedback on Proposed Cybersecurity Bill*. Retrieved November 4, 2017, from https://www.csa.gov.sg/news/press-releases/mci-and-csa-seek-public-feedback-on-proposed-cybersecurity-bill#sthash.g9mjneAk.dpuf

Cyber Security Agency of Singapore. (2017d). *Cybersecurity Public Awareness Survey 2016 Key Findings*. Retrieved November 15, 2017, from https://www.csa.gov.sg/~/media/csa/documents/key_findings/key%20findings-cybersecurity%20public%20awareness%20survey%202016.ashx?la=en

Cyber Security Agency of Singapore, & Personal Data Protection Commission. (2016). *Cyber Safety Issue 2*. Retrieved November 18, 2017, from https://www.csa.gov.sg/gosafeonline/~/media/gso/images/activity_book/cyber_security_activity_book_2.ashx?la=en

Deloitte. (2016). *Asia-Pacific Defense Outlook 2016: Defense in Four Domains*. Retrieved July 25, 2017 from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-ap-defense-outlook-2016-160216.pdf

Denning, D. E. (2000). Cyberterrorism: The Logic Bomb versus the Truck Bomb. *Global Dialogue*, *2*(4), 29–37.

Everard, P. (2008). NATO and Cyber Terrorism. In Centre of Excellence Defence Against Terrorism (Ed.), Responses to Cyber Terrorism (pp. 118-126). IOS Press.

Fidler, D. P. (2016). Cyberspace, Terrorism and International Law. *Journal of Conflict and Security Law*, *21*(3), 475–493. doi:10.1093/jcsl/krw013

GoSafeOnline. (2017). *Cyber Safety Activity Book*. Retrieved November 18, 2017, from https://www.csa.gov.sg/gosafeonline/resources/activity-book

GovTech. (2017). *Opening GOH Address by Dr. Janil Puthucheary for GovInsider Innovation Labs World Conference 2017*. Retrieved October 25, 2017, from https://www.tech.gov.sg/media-room/speeches/2017/09/opening-goh-address-by-dr-janil-puthucheary-for-govinsider-innovation-labs-world-conference-2017

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The Psychological Effects of Cyber Terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284–291. doi:10.1080/00963402.2016.1216502 PMID:28366962

Hioe, W. (2001). *National Infocomm Strategy and Policy: Singapore's Experience*. Retrieved October 18, 2017, from http://www.unapcict.org

Hui, C. (2015, Oct 27). *Cyber Security in Businesses Gets a Boost with New Employee Kit*. Retrieved November 18, 2017, from http://www.channelnewsasia.com/news/business/cyber-security-in-businesses-gets-a-boost-with-new-employee-kit-8234376

Infocomm Development Authority of Singapore. (2000). *Infocomm 21: Singapore Where the Digital Future Is*. Retrieved August 31, 2017, from https://www.imda.gov.sg/about/corporate-publications/past-publications/past-infocomm-plans

Infocomm Development Authority of Singapore. (2003). *Connected Singapore: Unleashing Potential, Realizing Possibilities, through Infocomm*. Retrieved August 31, 2017, from https://www.tech.gov.sg/-/media/GovTech/About-us/Corporate-Publications/Past-infocomm-plans/Connected.pdf?la=en

Infocomm Development Authority of Singapore. (2005). *Three-year Infocomm Security Masterplan Unveiled*. Retrieved November 12, 2017, from https://www.imda.gov.sg/about/newsroom/archived/ida/media-releases/2005/20050712110643

Infocomm Development Authority of Singapore. (2008). *Plan Aims to Bolster National Readiness to Counter Cyber Threats*. Retrieved November 12, 2017, from https://www.tech.gov.sg/media-room/media-releases/2008/04/new-s70m-masterplan-to-boost-singapores-infocomm-s

Infocomm Development Authority of Singapore. (2010). *Realising the iN2015 Vision: Singapore: An Intelligent Nation, A Global City, Powered by Infocomm*. Retrieved August 31, 2017, from https://www.tech.gov.sg/-/media/GovTech/About-us/Corporate-Publications/PDFs/iN2015-Reports/realisingthevisionin2015.pdf

Infocomm Development Authority of Singapore. (2013a). *National Cyber Security Masterplan 2018*. Retrieved November 12, 2017, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Singapore_2013_AnnexA.pdf

Infocomm Development Authority of Singapore. (2013b). *Enhanced Cyber-Watch Centre to Strengthen Infocomm Security*. Retrieved November 6, 2017, from https://www.tech.gov.sg/-/media/GovTech/Media-Room/Media-Releases/2013/5/AnnexDpdf.pdf

Khoong, H. Y. (2001). *Khoong Hock Yun, Assistant Chief Executive, Infocomm Development, IDA Singapore – Speech CIAPR Forum - Singapore Day Symposium, Grand Hyatt Shanghai, China*. Retrieved October 19, 2017, from https://www.imda.gov.sg/about/newsroom/archived/ida/speeches/2001/20061212150610

Kok, X. H. (2013 November 30). MOM Site Duplicated, Art Museum Site Breached. *Today*. Retrieved October 26, 2017, from http://www.todayonline.com/singapore/mom-site-duplicated-art-museum-site-breached

Kor, V. (2017). *Cybersecurity: A Concentric Approach*. Retrieved November 4, 2017, from https://www.tech.gov.sg/TechNews/Opinions/2017/04/07/08/06/Cybersecurity-A-Concentric-Approach

Kwang, K. (2015, August 4). Internet 'Was Not Designed for Safety': Cyber Security Agency Chief. *Channel NewsAsia*. Retrieved November 6, 2017, from http://www.channelnewsasia.com/news/singapore/internet--was-not-designed-for-safety--cyber-security-agency-chi-8237784

Lee, C. (2017, May 30). *Cyber Security Resources, Grants Available to SMEs*. Retrieved November 18, 2017, from http://www.todayonline.com/voices/cyber-security-resources-grants-available-smes

Lee, H. L. (1996). *Speech - Launch of the Singapore Government Internet Web Site and Intranet*. Retrieved August 30, 2017, from https://www.imda.gov.sg/about/newsroom/archived/ida/speeches/1996/20050728144718

Lee, T. (2013). *'Anonymous' Hackers Threaten War with Singapore Government*. Retrieved October 26, 2017, from https://www.techinasia.com/youtube-anonymous-hacker-group-threatens-war-singapore-govt-video-removed-viral

Lee, U. (2017 March 1). *Mindef's Internet System Breached in Cyberattack*. Retrieved October 26, 2017, from http://www.businesstimes.com.sg/technology/mindefs-internet-system-breached-in-cyberattack

Lemon, S. (2009). *Singapore to Form National Cyber-Security Agency*. Retrieved November 5, 2017, from https://www.cio.com/article/2424366/government/singapore-to-form-national-cyber-security-agency.html

Leung, E. (2003). *Speech by the Secretary for Justice at Internet Law Symposium*. Retrieved November 19, 2017, from http://www.doj.gov.hk/eng/archive/pdf/sj260903e.pdf

Loh, P. J. (2010). APEC Trojan Email Attacks. *Home Team Journal*, *2*, 43-6. Retrieved October 26, 2017, from https://www.mha.gov.sg/HTA/Documents/Home%20Team%20Journal%20Issue%202.pdf

Loke, K. F. (2017, February 28). *MINDEF Internet System Breached; Data Stolen from National Servicemen, Employees*. Retrieved October 26, 2017, from http://www.channelnewsasia.com/news/singapore/mindef-internet-system-breached-data-stolen-from-national-servic-7617146

Ministry of Finance, Ministry of Information, Communications and the Arts, & Infocomm Development Authority of Singapore. (2011). *E-government Masterplan 2011-2015: Collaborative Government*. Retrieved August 31, 2017, from https://www.tech.gov.sg/-/media/GovTech/About-us/Corporate-Publications/eGov/eGovBOOK1115.pdf?la=en

Ministry of Finance, & Infocomm Development Authority of Singapore. (2003). *Singapore E-government*. Retrieved August 31, 2017, from https://www.tech.gov.sg/-/media/GovTech/About-us/Corporate-Publications/eGov/eGap-II.pdf?la=en

Ministry of Finance, & Infocomm Development Authority of Singapore. (2006). *iGov2010: From Integrating Service to Integrating Government*. Retrieved August 31, 2017, from https://www.tech.gov.sg/-/media/GovTech/About-us/Corporate-Publications/eGov/iGov.pdf?la=en

Ministry of Home Affairs. (2014). *2014 National Security Conference at Suntec Singapore Convention & Exhibition Centre - Opening Address by Mr S Iswaran, Minister, Prime Minister's office, Second Minister for Home Affairs and Trade & Industry*. Retrieved November 12, 2017, from https://www.mha.gov.sg/Newsroom/speeches/Pages/2014-National-Security-Conference-at-Suntec-Singapore-Convention---Exhibition-Centre---Opening-Address-by-Mr-S-Iswaran,-Min.aspx

Ministry of Home Affairs. (2016). *National Cybercrime Action Plan*. Retrieved November 12, 2017, from https://www.mha.gov.sg/Newsroom/press-releases/PublishingImages/Pages/Launch-of-the-National-Cybercrime-Action-Plan-at-RSA-Conference-Asia-Pacific-Japan/NCAP%20Document.pdf

Ministry of Home Affairs. (2017a). *Official Launch of Interpol World 2017 – Speech by Mr Desmond Lee, Second Minister for Home Affairs and Second Minister for National Development*. Retrieved November 6, 2017, from https://www.mha.gov.sg/newsroom/speeches/Pages/Official-Launch-of-Interpol-World-2017-%E2%80%93-Speech-by-Mr-Desmond-Lee.aspx

Ministry of Home Affairs. (2017b). *Computer Misuse and Cybersecurity (Amendment) Bill*. Retrieved November 4, 2017, from https://www.mha.gov.sg/Newsroom/press-releases/Pages/Computer-Misuse-and-Cybersecurity-(Amendment)-Bill-.aspx

Ministry of Information and the Arts. (1995). *Speech by BG (NS) George Yeo, Minister for Information & the Arts and Minister of Health, at the Launch of SINGAPORE INFOMAP on Wednesday, 8 March 1995 at 10.00 am*. Retrieved October 19, 2017, from http://www.nas.gov.sg/archivesonline/data/pdfdoc/yybg19950308s.pdf

Mullin, G., & Lake, E. (2017, August 4). What Is Wannacry Ransomware? Malware Used to Cripple NHS in 2017 Cyber Attack. *The Sun*. Retrieved October 30, 2017, from https://www.thesun.co.uk/tech/3562470/wannacry-ransomware-nhs-cyber-attack-hackers-virus/

National Computer Board. (1997). *National Computer Board Annual Report 1996/1997*. Retrieved August 30, 2017, from https://www.imda.gov.sg/about/newsroom/archived/ida/speeches/1997/20050728143225

Networks Asia. (2015). *Singapore Business Federation unveils Employee Cyber Security Kit for SMBs*. Retrieved November 18, 2017, from https://www.networksasia.net/article/singapore-business-federation-unveils-employee-cyber-security-kit-smbs.1446085033

Networks Asia. (2016). *Singapore Launches National Cybercrime Action Plan*. Retrieved November 6, 2017, from https://www.networksasia.net/article/singapore-launches-national-cybercrime-action-plan.1469025526?source=transform-security&qt-breaking_news_most_read=0

Ng, J. (2014). *Staying Ahead of Digital Criminals through Robust Cyber Security Training*. Retrieved November 11, 2017, from https://www.hometeam.sg/article.aspx?news_sid=20141113RNtrYzE8rlqH

Ng, J. (2015). *New Cyber Security Agency Set to Lead the way in Combating Emerging Cyber Threats*. Retrieved November 5, 2017, from https://www.hometeam.sg/article.aspx?news_sid=201501282Uakllrzrg7S

Ng, J. Y. (2014 June 5). 1,560 SingPass User Accounts Breached. *Today*. Retrieved October 29, 2017, from http://www.todayonline.com/singapore/1560-singpass-user-accounts-breached

Ng, K. (2015 January 23). Hacker 'Messiah' Pleads Guilty to 39 Computer Misuse Charges. *Today*. Retrieved October 26, 2017, from http://www.todayonline.com/singapore/hacker-messiah-pleads-guilty-cyberattacks

Ong, J. (2017 May 12). *NUS, NTU Networks Hit by 'Sophisticated' Cyber Attacks*. Retrieved October 29, 2017, from http://www.channelnewsasia.com/news/singapore/nus-ntu-networks-hit-by-sophisticated-cyber-attacks-8840596

Orion, W. LLC (2017). *Amendments to the Computer Misuse and Cybersecurity Act*. Retrieved November 4, 2017, from http://www.orionw.com/blog/news/security/amendments-to-the-computer-misuse-and-cybersecurity-act

Phneah, E. (2013). *Singapore to Open Cyber Security Lab to Train Law Enforcers*. Retrieved November 6, 2017, from http://www.zdnet.com/article/singapore-to-open-cyber-security-lab-to-train-law-enforcers/

Precious Communications. (2013). *McAfee Survey Reveals Average Internet User in Singapore Has S$57,500 Of Under-Protected 'Digital Assets'*. Retrieved November 16, 2017, from http://www.mynewsdesk.com/sg/preciouscommunications/pressreleases/mcafee-survey-reveals-average-internet-user-in-singapore-has-s-57-500-of-under-protected-digital-assets-871659

Singapore Police Force. (2011). *Annual Crime Brief 2011*. Retrieved November 1, 2017, from https://www.police.gov.sg/news-and-publications/statistics?page=2

Singapore Police Force. (2015). *Annual Crime Brief 2014*. Retrieved November 1, 2017, from https://www.police.gov.sg/news-and-publications/statistics?page=1

Singapore Police Force. (2016). *Annual Crime Brief 2015*. Retrieved November 1, 2017, from https://www.police.gov.sg/news-and-publications/statistics?page=1

Singapore Police Force. (2017a). *Annual Crime Brief 2016*. Retrieved November 1, 2017, from https://www.police.gov.sg/news-and-publications/statistics?page=1

Singapore Police Force. (2017b). *Mid-year Crime Statistics for January to June 2017*. Retrieved November 1, 2017, from https://www.police.gov.sg/news-and-publications/statistics?page=1

Singapore Statutes Online. (1993). *Computer Misuse Act 1993*. Retrieved November 4, 2017, from http://160.96.185.113/aol/search/display/view.w3p;page=0;query=DocId%3A%228a3534de-991c-4e0e-88c5-4ffa712e72af%22%20Status%3Apublished%20Depth%3A0%20%20TransactionTime%3A%2216%2F02%2F2017%22;rec=0;whole=yes

Singapore Statutes Online. (1998). *Computer Misuse (Amendment) Act 1998*. Retrieved November 4, 2017, from http://statutes.agc.gov.sg/

Smart Nation Singapore. (2017). *Enablers*. Retrieved October 25, 2017, from https://www.smartnation.sg/about-smart-nation/enablers

Sreedharan, S. (2013, December 7). 647 StanChart Clients' Bank Statements Stolen. *Today*. Retrieved October 26, 2017, from http://www.todayonline.com/singapore/647-stanchart-clients-bank-statements-stolen?page=1

Sun, D. (2017, August 29). *More Falling for Online Love Scams*. Retrieved November 1, 2017, from http://www.tnp.sg/news/singapore/more-falling-online-love-scams

Tan, B., Ling, P. S., & Cha, V. (2013). The Evolution of Singapore's Infocomm Plans: Singapore's E-government Journey from 1980 to 2007. In G. Pan (Ed.), *Dynamics of Governing IT Innovation in Singapore: A Case Book* (pp. 1–39). World Scientific. doi:10.1142/9789814417839_0001

Tan, C. Y. (2004). *Taking the Lead on Regional Infocomm Security*. Retrieved November 5, 2017, from https://www.tech.gov.sg/media-room/speeches/2004/10/taking-the-lead-on-regional-infocomm-security

Tan, T. M. (2017, July 5). Private Sector, Police Tie up to Fight Cyber Criminals. *Straits Times*. Retrieved November 6, 2017, from http://www.straitstimes.com/singapore/courts-crime/private-sector-police-tie-up-to-fight-cyber-criminals

Tan, W. (2015, January 28). New National Agency to Tackle Cyber Threats. *Today*. Retrieved November 5, 2017, from http://www.todayonline.com/singapore/new-national-agency-tackle-cyber-threats

Tan, W. (2017, September 19). *S'pore Gives S$1.5m to Boost ASEAN Cyber Security*. Retrieved November 13, 2017, from http://www.todayonline.com/business/spore-gives-s15m-boost-asean-cyber-security

Tehrani, P. M. (2017). *Cyberterrorism: The Legal and Enforcement Issues*. World Scientific Publishing Europe Ltd. doi:10.1142/q0063

Tham, I. (2017, May 25). New Govt Centre to Detect Cyber Threats. *Straits Times*. Retrieved November 6, 2017, from http://www.straitstimes.com/tech/new-govt-centre-to-detect-cyber-threats

The Ministry of Communications, & Information and the Cyber Security Agency of Singapore. (2017). *Public Consultation Paper on the Draft Cybersecurity Bill*. Retrieved November 5, 2017, from https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/consult_document.ashx?la=en

The Singapore Computer Emergency Response Team. (2015). *Frequently Asked Questions*. Retrieved November 5, 2017, from https://www.csa.gov.sg/singcert/about-us/faqs

Theohary, C. A., & Rollins, J. W. (2015). *Cyberwarfare and Cyberterrorism: In Brief*. Retrieved October 25, 2017, from https://fas.org/sgp/crs/natsec/R43955.pdf

Thompson, E. (2017). *Building a HIPAA-Compliant Cybersecurity Program: Using NIST 800-30 and CSF to Secure Protected Health Information*. Apress. doi:10.1007/978-1-4842-3060-2

TODAY. (2015, March 10). *Curtin Singapore's Website Defaced by Hackers Claiming to Represent ISIS*. Retrieved October 29, 2017, from http://www.todayonline.com/singapore/curtin-singapores-website-defaced-hackers-claiming-represent-isis

TODAY. (2017, May 12). *NUS-NTU Hack: Other Recent Cyber Breaches in Singapore*. Retrieved October 26, 2017, from http://www.todayonline.com/singapore/recent-cyber-security-attacks

Toh, E. M. (2017 May 13). Global Cyber Attack: Don't Pay the Ransom, Says S'pore's Cyber Security Agency. *Today*. Retrieved October 30, 2017, from http://www.todayonline.com/singapore/singapores-govt-agencies-and-critical-infrastructure-not-affected-global-cyber-attack-csa

United Nations. (2003). *UN Global E-government Survey 2003*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2003-Survey/Complete-Survey.pdf

United Nations. (2004). *United Nations Global E-government Readiness Report 2004: Towards Access for Opportunity*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2004-Survey/Complete-Survey.pdf

United Nations. (2005). *United Nations Global E-government Readiness Report 2005: From E-government to E-inclusion*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2005-Survey/Complete-survey.pdf

United Nations. (2008). *UN E-government Survey 2008: From E-government to Connected Governance*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2008-Survey/Complete-survey.pdf

United Nations. (2010). *United Nations E-government Survey 2010: Leveraging E-government at a Time of Financial and Economic Crisis*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2010-Survey/Complete-survey.pdf

United Nations. (2012). *United Nations E-government Survey 2012: E-government for the People*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2012-Survey/Complete-Survey.pdf

United Nations. (2014). *United Nations E-government Survey 2014: E-government for the Future We Want*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf

United Nations. (2016). *United Nations E-government Survey 2016: E-government in Support of Sustainable Development*. Retrieved October 23, 2017, from http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf

United Nations Division for Public Economics and Public Administration, & American Society for Public Administration. (2002). *Benchmarking E-government: A Global Perspective*. Retrieved October 23, 2017, from https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/English.pdf

Van Dijck, P., & Verbruggen, H. (1987). The Case of Singapore. In H. Linnemann (Ed.), *Export-oriented Industrialization in Developing Countries* (pp. 381–415). Singapore: Singapore University Press.

Waseda University, & International Academy of CIO. (2014). *WASEDA – IAC 10th International E-Government Ranking 2014*. Retrieved October 23, 2017, from http://www.e-gov.waseda.ac.jp/pdf/2014_e-gov_press_release.pdf

Waseda University, & International Academy of CIO. (2015). *2015 WASEDA – IAC International E-Government Ranking Survey*. Retrieved October 23, 2017, from http://www.e-gov.waseda.ac.jp/pdf/2015_Waseda_IAC_E-Government_Press_Release.pdf

Waseda University, & International Academy of CIO. (2016). *The 12th Waseda - IAC International e-Government Rankings Survey 2016 Report*. Retrieved October 23, 2017, from http://www.e-gov.waseda.ac.jp/pdf/2016_E-Gov_Press_Release.pdf

Waseda University, & International Academy of CIO. (2017). *THE 13TH WASEDA – IAC International Digital Government Rankings 2017 Report*. Retrieved October 23, 2017, from http://www.e-gov.waseda.ac.jp/pdf/2017_Digital-Government_Ranking_Press_Release.pdf

Wong, Y. Y. J., Gerber, R., & Toh, K. A. (2003). A Comparative Study of Diffusion of Web-based Education (WBE) in Singapore and Australia. In A. Aggarwal (Ed.), *Web-Based Education: Learning from Experience* (pp. 347–370). Hershey, PA: IGI Global. doi:10.4018/978-1-59140-102-5.ch021

Yu, E. (2006). *S'pore: New Center to Monitor Govt Systems*. Retrieved November 6, 2017, from http://www.zdnet.com/article/spore-new-center-to-monitor-govt-systems-2039419454/

Zhou, J. (2011). Singapore Law on Information Technology. *IT Connect*, 20. Retrieved November 4, 2017, from http://enewsletter.ntu.edu.sg/itconnect/2011-08/Pages/SingaporeLawOnIT.aspx

KEY TERMS AND DEFINITIONS

Computer Misuse Act: A legislation that is enacted to specifically investigate, prosecute and adjudicate cybercrime in Singapore.

Critical Information Infrastructure: Networks or information and communications systems that deliver essential services such as electricity, telecommunications and transportation.

Cyber Security Agency of Singapore: A national agency to oversee cybersecurity strategy and agencies' cybersecurity operations, and enhance public awareness of cybersecurity through education and outreach.

Infocomm Security Masterplan: A strategic roadmap for strengthening cybersecurity in Singapore.

Singapore Computer Emergency Response Team: It is a group of experts that detects, resolves, and prevents security-related incidents on the internet.

SingPass: A security measure that is used in Singapore for verification of identity when people have online transaction with government agencies.

Smart Nation: An initiative launched by the Singaporean government in 2014 to solve problems, create more opportunities and make society more connected through the extensive use of information technology.

APPENDIX 1

Table 1. Singapore's E-government Ranking in United Nations E-government Survey

Year	Ranking
2001	4
2003	12
2004	8
2005	7
2008	23
2010	11
2012	10
2014	3
2016	4

(Data Source: United Nations E-government Survey, 2001-2016)

APPENDIX 2

Table 2. Singapore's E-government Ranking in WASEDA – IAC International E-Government Ranking Survey

Year	Ranking
2005	3
2006	3
2007	2
2008	2
2009	1
2010	1
2011	1
2012	1
2013	1
2014	2
2015	1
2016	1
2017	1

(Data Source: WASEDA – IAC International E-Government Ranking Survey, 2014-2017)

APPENDIX 3

Table 3. Internet Love Scams in Singapore (2010- 2016)

	2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
No. of cases	21	62	--	81	198	385	636
The amount of money cheated	S$824,000	S$2.3 million	--	S$5.8 million	S$8.8 million	S$12 million	S$24 million

(Data Source: Singapore Police Force, 2011; Singapore Police Force, 2015; Singapore Police Force, 2016; Singapore Police Force, 2017a)