COMPUTER LAW & SECURITY REVIEW 000 (2018) 1–4

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Singapore's cybersecurity strategy

Kah Leng TER

NUS Business School, National University of Singapore, Singapore

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Cybersecurity
Legislation

ABSTRACT

Imminent cybersecurity threats of a massive global scale have led countries to review and strengthen their national cybersecurity strategies and to enact new and bolder legislation that is both comprehensive and far-reaching. This paper discusses how Singapore's enactment of the Cybersecurity Act 2018 is one such attempt to foster a secure and resilient national infocomm environment against cyberattacks.

© 2018 Kah Leng Ter. Published by Elsevier Ltd. All rights reserved.

Rapid digitisation and increased cyber connectivity has led to a surge in sophisticated cybersecurity threats. Singapore, the most globally connected country in the world,[1] and rated the top in the world on cybersecurity strategy,[2] has responded by formulating infocomm security master plans since 2003 and a high-level National Cyber Security Strategy in October 2016. The Strategy sets out Singapore's vision, goals and priorities for cybersecurity. It aims to: (1) strengthen the resilience of critical information infrastructures by taking a coordinated national approach to ensure the continuity of essential services in the face of cyberattacks; (2) develop a vibrant cybersecurity ecosystem comprising a skilled workforce; (3) work with local industry and the community to promote a strong awareness of the importance of cybersecurity and (4) forge strong international partnerships in dealing with transnational cyber threats and cooperate with computer emergency response teams internationally on cybersecurity incidents.

Singapore's commitment to cybersecurity is reinforced in the latest five-year National Cybersecurity Masterplan 2018 which will provide strategic directions in securing the infocomm environment not only in the government and critical information infrastructure, but also in the business and people sectors. At the same time, a balanced approach will be taken between security requirements and the ease of conducting business and daily activities. The vision of Masterplan 2018 is for Singapore to be a "Trusted and Robust Infocomm Hub" by 2018. It focusses on three key areas: (1) enhancing the security and resilience of critical information infrastructure; (2) increasing efforts to raise infocomm security awareness and adopting security measures among businesses and users; and (4) growing Singapore's pool of infocomm security experts. The allocation of at least 8% of the government's infocomm technology budget to developing cybersecurity talent and the cyber security ecosystem underscores Singapore's commitment to engender a secure and resilient infocomm environment and a vibrant cyber security ecosystem.

The objectives, policies and strategies laid down in the Cybersecurity Masterplan 2018 and the Cybersecurity Strategy are reflected in the provisions of the Cybersecurity Act, enacted on 5 February 2018 and expected to come into force in the second half of the year.

The Cybersecurity Act has generally won the support of industry respondents and cybersecurity professionals. In response to feedback received from the public consultation which was open from 10 July to 24 August 2017, a few but significant amendments were introduced. The Act sets out three core objectives: (1) to provide the Cyber Security Agency of Singapore ("CSA") with powers to manage and respond to cybersecurity threats and incidents; (2) to provide a framework for the regulation of critical information infrastructure ("CII"); and (3) to establish a framework for the sharing of cybersecurity information with and by the CSA and the protection of such information. The fourth objective to establish a light-

E-mail address: bizterkl@nus.edu.sg

[1] According to the McKinsey Global Institute Report 2016.

[2] Survey by the UN International Telecommunication Union (ITU) based on Singapore's legal, technical and organizational institutions, educational and research capabilities and cooperation in information-sharing networks.

https://doi.org/10.1016/j.clsr.2018.05.001
0267-3649/© 2018 Kah Leng Ter. Published by Elsevier Ltd. All rights reserved.

Please cite this article as: K.L. TER, Singapore's cybersecurity strategy, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.05.001

touch licensing scheme for cybersecurity service providers has been narrowed down, following industry concerns raised in the public consultation.

1. The Cyber Security Agency: Commissioner for Cybersecurity

The CSA was set up in April 2015 to oversee and coordinate Singapore's cybersecurity strategy. Under the Cybersecurity Act, the Commissioner of Cybersecurity, appointed by the relevant Minister, will have extensive supervisory, regulatory and enforcement powers. He is to identify and designate as critical information infrastructure any computer or computer system which is necessary for the continuous delivery of essential services. In order to determine whether it is a CII, the Commissioner may require by notice certain information in advance from the person operating the computer or computer system. Failure to comply with the notice, without reasonable excuse, is a criminal offence carrying a fine of up to $100,000 and or imprisonment for up to 2 years. However, any person to whom the notice is issued is not obliged to do so if the information is subject to any right, privilege or immunity conferred by or under any law, contract or rules of professional conduct (referred to as "protected information") in relation to the disclosure of such information. Hence, this will protect a person's right to legal professional privilege.

The Commissioner is to coordinate national efforts and monitor cybersecurity threats to Singapore's national security, defence, economy, foreign relations, public health, public order and safety or essential services, whether such cybersecurity threats occur in or outside Singapore. In investigating a cybersecurity threat, he may examine anyone relevant to the investigation, take statements and require relevant information to be furnished. The power to obtain information when responding to cyber breach incidents raised concerns during the public consultation and the CSA has clarified that it intends to focus on technical information, not personal data. Furthermore, the person affected is not obliged to provide the information if it is "protected information".

The Commissioner's powers are more intrusive in cases of serious cybersecurity threats and incidents. These are threats which create a real risk of significant harm to a CII; disrupt the delivery of an essential service; or are a real threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. In furtherance of his duties, the Commissioner may direct persons to carry out remedial measures, for example cleaning up malware-infected computers; installing software updates to address cybersecurity vulnerabilities and temporarily disconnecting infected computers from the network until the first two measures have been carried out; and the redirection of malicious data traffic to designated computer servers. The Commissioner may also require CII owners to assist with investigations, which may include monitoring, scanning or preserving the state of the computer, and allowing investigating officers to install software on it; entering premises where relevant computers are located; and taking possession of computers to carry out further examination or analysis with the consent of the owner or if other conditions are met.

In the case of emergency cybersecurity events, the Minister effectively has the power to take any measures necessary to prevent, detect or counter any threat.

While the powers conferred on the Commissioner appear to be wide and sweeping, the Consultation Paper to the Cybersecurity Bill gives the assurance that there will be an internal governance process within the CSA to ensure that all its powers are exercised responsibly and in accordance with the Act, and only by qualified persons.

Concerns were also raised during the public consultation over the broad powers of the CSA, with some respondents calling for safeguards. In response, the CSA emphasised that the powers of investigation are calibrated depending on the severity of the cyber threat. CSA does not have broad powers to oversee every computer in Singapore and the statutory powers of the CSA are only exercisable in the event of a cybersecurity incident. Furthermore, there are checks and balances to prevent the misuse of disclosed information and CSA officers may be prosecuted if they misuse any information that is obtained.

2. Critical information infrastructure

The vulnerability of CII has been exposed by the WannaCry and NotPetya ransomware attacks affecting critical infrastructure such as energy and power supply. Singapore was not affected but is vulnerable. In 2017, hackers broke into the networks of the National University and the Nanyang Technological University to steal government-related data, both universities being involved in government-linked projects for the defence, foreign affairs and transport sectors. In a separate incident, the personal data belonging to 850 national servicemen and defence ministry staff were hacked.

The Cybersecurity Act therefore seeks to strengthen Singapore's CII that provide essential services by identifying eleven critical sectors: government, security and emergency services, healthcare, into-communications, banking and finance, energy, water, media, land transport, aviation and maritime. A CII means a computer or a computer system which has been designated by the Commissioner as a CII. The Commissioner may do so by notice if satisfied that the computer or computer system is necessary for the continuous delivery of an essential service and its loss or compromise will have a debilitating effect on the availability of the essential service in Singapore; and the computer or computer system is located wholly or partly in Singapore. The CII owner is then required to perform certain duties which will increase the entity's accountability for protecting the CII and to ensure its cybersecurity. The owner of a CII is defined as the legal owner of the CII and every joint owner where the CII is jointly owned by more than one person.

This narrow definition of "owner" is welcome in the light of industry concerns that while a CII can be "owned" by a person who has effective control over the operations of the CII and the ability to carry out changes to the CII, the same CII can also be "owned" by a person responsible for ensuring the continuous function of the CII. It is now clear that suppliers and third party vendors helping with the operations of a CII will not fall within the definition of "owner" in relation to the CII.

Please cite this article as: K.L. TER, Singapore's cybersecurity strategy, Computer Law & Security Review: The International Journal of Technology Law and Practice (2018), https://doi.org/10.1016/j.clsr.2018.05.001

Download English Version:

https://daneshyari.com/en/article/6890445

Download Persian Version:

https://daneshyari.com/article/6890445

Daneshyari.com