2024 Amendments to the Cybersecurity Act 2018 of Singapore – Key Changes

Background

The Cybersecurity Act 2018 of Singapore (**Act**) provides for the protection of critical information infrastructure (**CII**) and the regulation of cybersecurity service providers in Singapore. The Act was recently amended by the Cybersecurity (Amendment) Bill (Bill No. 15/2024) (**Bill**), which was passed by Parliament on 7 May 2024 and will come into operation on a date to be notified by the Minister. The Bill introduces significant changes to the Act, which will affect various stakeholders in the technology and cybersecurity ecosystem, including vendors, subcontractors, and service providers providing services to support CII or essential services.

These amendments seek to address recent technology developments and changes in industry practices and extend regulatory coverage of the Act to address evolving cybersecurity risks. For example, in light of the increasing prevalence of cloud computing and software-as-a-service deployments, CII and essential systems may extend beyond physical systems located on the owner's premises to remote servers in data centres in Singapore and abroad. Malicious actors are also increasingly focusing on exploiting vulnerabilities in third-party services *via* supply chain attacks in order to gain access to core systems of interest. The Bill therefore represents a timely update to the cybersecurity regulatory framework in Singapore.

This update summarises the key changes introduced by the Bill.

Overview of Key Changes

Expansion of the Act's scope to cover new classes of regulated persons and systems

Under the Bill, the regulatory ambit of the Act will be expanded to cover four new classes of regulated persons and systems:

(a) **Third-party-owned CII (TPO CII)**: TPO CII will be regulated under a new Part 3A of the Act which allows the Commissioner of Cybersecurity (**Commissioner**) to designate a provider of an essential service as responsible for the cybersecurity of its TPO CII, which may include the third-party hosting, storage, and computing infrastructure (amongst other infrastructure) which the provider relies upon to deliver the essential service.

Providers of essential services so designated may include providers of services essential to national security, the economy, public health and safety, amongst other services, such as banking, healthcare, energy, water, and transport services.

Such designated persons will have to comply with various obligations under Part 3A of the Act, such as obtaining specified legally binding commitments from owners of TPO CII, cooperating with the Commissioner, reporting cybersecurity incidents, conducting audits and risk assessments, and complying with codes of practice and standards of performance. This will likely have implications on contractual arrangements between designated providers of essential services and their vendors, contractors, and service providers.

(b) **Major foundational digital infrastructure (FDI) service providers**: FDI services are services which are crucial to the functioning of digital services, while major FDI services are FDI services which, if not provided normally, would be likely to disrupt or cause deterioration of the operation of a large number of businesses or organisations in Singapore. Examples of major FDI services include cloud computing services and data centre facility services.

Major FDI service providers will have to comply with the obligations under Part 3D of the Act, such as reporting cybersecurity incidents, cooperating with the Commissioner, and complying with codes of practice and standards of performance.

(c) **Entities of special cybersecurity interest (ESCIs)**: ESCIs hold sensitive information or perform functions of national interest, such that if they are compromised, there may be a significant detrimental effect on Singapore's interests. ESCIs may include universities, research institutions, media organisations, non-governmental organisations, and similar entities.

ESCIs will have to comply with the obligations under Part 3C of the Act, such as reporting cybersecurity incidents, cooperating with the Commissioner, and complying with codes of practice and standards of performance.

(d) **Owners of systems of temporary cybersecurity concern (STCCs)**: STCCs are temporarily high-risk systems that could seriously affect national interests if compromised. They may include systems supporting high-profile international events or national pandemic responses. Businesses that own STCCs will have to comply with the obligations under Part 3B of the Act, such as reporting cybersecurity incidents, cooperating with the Commissioner, and complying with codes of practice and standards of performance.

In addition, the Bill provides for the application of certain portions of the Act to virtual computers and virtual computer systems. These may include virtual private servers, virtual machines, containers, simulated or emulated systems, amongst other virtual systems.

Changes to existing CII regime

Following the amendments to the Act, existing CII owners will be known as owners of "provider-owned CII" (as opposed to TPO CII). The Bill further provides for various changes to the existing CII regime:

(a) The geographical scope of provider-owned CII has been expanded. Under the amended Act, provider-owned CII may include computers or computer systems owned by a person in Singapore but located wholly outside Singapore, provided that such computer or computer system is necessary to continuously deliver an essential service.

(b) Owners of provider-owned CII will be subject to additional obligations under the amended Act. For example, the scope of written directions which the Commissioner may issue to owners of provider-owned CII has been expanded to include directions relating to compliance with prescribed cybersecurity-related standards (technical or otherwise).

(c) Furthermore, owners of provider-owned CII must additionally notify the Commissioner of prescribed cybersecurity incidents relating to a computer or system which is: (i) under the owner's control, but is not interconnected with, and does not communicate with, the CII; or (ii) under the control of a supplier to the owner, and is interconnected with, or communicates with, the CII.

Expansion of regulatory powers and enforcement regime

The Bill also expands the Commissioner's regulatory powers and enforcement regime under the Act. For example:

(a) It confers additional powers on the Commissioner to monitor licensed cybersecurity service providers (i.e., providers of managed security operations centre (SOC) monitoring services and penetration testing services). These additional monitoring powers include powers to conduct audits and inspect records, accounts, and computer systems.

(b) It introduces civil penalties as an alternative to prosecution for contraventions of the Act, allowing the Commissioner, with the Public Prosecutor's consent, to bring civil actions in court. The civil penalties payable may be up to 10% of the defendant's annual turnover or SGD 500,000, depending on the specific obligation breached.

Conclusion

Given the complexity and breadth of the amendments introduced by the Bill, businesses operating in Singapore may wish to consider whether they are regulated and, if so, assess their compliance under the amended Act.

Businesses regulated under the amended Act (including new classes of regulated entities) should review their cybersecurity policies and practices to ensure that they are well prepared to perform their obligations, including facilitating cybersecurity audits and conducting risk assessments as required. They should also be prepared to respond to any requests or directions from the Commissioner, and (in consultation with their legal advisors) manage and respond to cybersecurity incidents promptly. Businesses should also be aware of the potential penalties and liabilities for contraventions of the amended Act, and take steps to mitigate their risks and liabilities.

If you have any questions or concerns about the Bill or the Act, or if you require any assistance in reviewing your cybersecurity policies and practices, please do not hesitate to contact us.

LAM Chung Nian
Head – Intellectual Property, Technology & Data Group
d: +65 6416 8271
e: chungnian.lam@wongpartnership.com
Click here to view Chung Nian's CV.

Kylie PEH
Partner – Intellectual Property, Technology & Data Group
d: +65 6416 8259
e: kylie.peh@wongpartnership.com
Click here to view Kylie's CV.

Connect with WongPartnership.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com

-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
Gruba Law
27/F 88 Corporate Center
141 Valero St., Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w grubalaw.com

wongpartnership.com