LEGAL UPDATE

OVERVIEW OF THE CYBERSECURITY (AMENDMENT) BILL

1. On 7 May 2024, the Parliament of Singapore passed the Cybersecurity (Amendment) Bill (the "**Bill**") to amend the existing Cybersecurity Act 2018 (the "**CSA**").

2. This legal update provides an overview of the amendments and sets out their impact on existing owners of computers or computer systems when the Bill comes into operation on a date to be notified in the Gazette.

3. The CSA came into force on 31 August 2018 and established a comprehensive legal framework to protect computers or computer systems in key sectors such as transport, healthcare, water, energy, finance and media from escalating cyber threats. The Bill extends this framework to cover additional digital infrastructures, impose stricter cybersecurity standards and broaden incident reporting requirements. These enhancements aim to "*strengthen our cybersecurity, and increase trust in using online services in Singapore*", and are specifically "*calibrated to address the risks to the nation, our economy, and our way of life while balancing compliance costs*".[1]

Amendments to the CSA

4. The Bill introduces five key amendments:

   a) Strengthening the existing regulations for owners of Critical Information Infrastructure ("**CII**") (which has been renamed Provider-owned Critical Information Infrastructure ("**PCII**") under the Bill);

   b) Introduction of regulations for designated providers who are responsible for the cybersecurity of Third-party-owned Critical Information Infrastructure ("**TCII**");

   c) Introduction of regulations for owners of Systems of Temporary Cybersecurity Concern ("**STCC**");

   d) Introduction of regulations for Entities of Special Cybersecurity Interest ("**ESCI**"); and

   e) Introduction of regulations for major Foundational Digital Infrastructure ("**FDI**") service providers.

12 June 2024

For any queries relating to this article, please contact

Tan Tee Jim, SC
tanteejim@leenlee.com.sg

Basil Lee
basillee@leenlee.com.sg

Authors:

Tan Tee Jim, SC
Basil Lee
Chee Kai Hao
Poon Chong Ming

Lee & Lee
25 North Bridge Road
Level 7
Singapore 179104
Tel: +65 6220 0666

For more legal updates, please visit the News & Publication Section of Lee & Lee's website at www.leenlee.com.sg, or follow Lee & Lee's Facebook page at www.facebook.com/leenlee.com.sg/ and Lee & Lee's LinkedIn page at https://lnkd.in/g6bNfv8G.

Disclaimer: The copyright in this document is owned by Lee & Lee.

No part of this document may be reproduced without our prior written permission.

The information in this update does not constitute legal advice and should not form the basis of your decision as to any course of action.

[1] *Singapore Parliamentary Debates*, Official Report (7 May 2024) vol 95 (Dr Janil Puthucheary, Senior Minister of State for Communications and Information).

© 2024 Lee & Lee. All Rights Reserved

A. Strengthening the existing regulations for owners of PCII

5. At present, Sections 3 and 7 of the CSA provide that a CII refers to a computer or a computer system located in Singapore which is necessary for the continuous delivery of an essential service. The essential services include aviation, land transport, maritime, banking and finance, energy, water, info-communications, media, the functioning of the Government, security and emergency services, and healthcare.

6. When a computer or computer system is designated as a CII by the Commissioner of Cybersecurity (the "**Commissioner**"), such designation would be valid for 5 years, and the owner of the CII would have to comply with the obligations under Part 3 of the CSA. The obligations include providing necessary information to the Commissioner, reporting certain cybersecurity incidents in respect of the CII to the Commissioner as well as carrying out a cybersecurity audit once every 2 years and a cyber risk assessment once a year.

7. As mentioned above at paragraph 4(a), CII has now been renamed PCII to distinguish it from TCII which would also be regulated under the Bill (see below paragraphs 10-13).

8. Under Clause 12 of the Bill (which amends Section 14 of the CSA), PCII owners would not only be obliged to report cybersecurity incidents relating to the PCII and computers or computer systems interconnected with or communicate with the PCII, but would also have to report incidents that affect (i) other computers or computer systems under the owner's control, and (ii) computers or computer systems which are under the control of a third-party supplier that are interconnected with, or that communicates with, the PCII.

9. This is to address the evolving techniques used by malicious actors to initiate attacks on computer systems at the periphery or along the supply chains of the PCII, instead of the PCII itself. The broadened scope of the obligation would enable the Commissioner to take proactive steps to protect the PCII if the Commissioner is alerted in advance that the owners' immediate suppliers have been compromised, thereby pre-empting potential disruptions to essential services.

B. Introduction of regulations for designated providers who are responsible for the cybersecurity of TCII

10. When the CSA was first enacted, the norm was for CII to be physical systems which were entirely owned or controlled by the CII owner and on the CII owner's premises (i.e., PCII). However, with the advent of cloud services provided by external vendors, a gap arose in the existing CSA, as providers would not be subject to any obligations when their CII has been outsourced to external vendors, and the vendors become the "owner" of the CII instead of the providers. For example, if a bank engages the services of a digital infrastructure service provider for CII which the bank operates and the CII is owned by the service provider, the bank would have no obligation to notify the Commissioner of cybersecurity incidents or to conduct cybersecurity audits and risk assessments, among others.

11. To remedy the gap, Clause 14 of the Bill introduces Part 3A to the CSA which imposes obligations on providers that have outsourced their CII to a third-party vendor. The obligations ensure that the providers remain responsible for the cyber resilience of the computers or computer systems that are vital to the provision of their essential services. Providers therefore cannot outsource this responsibility.

© 2024 Lee & Lee. All Rights Reserved

12. The obligations introduced under Part 3A include the duty for providers to furnish information relating to the TCII, report the change in ownership of the TCII, report cybersecurity incidents in respect of TCIIs, and conduct cybersecurity audits and risk assessments of the TCIIs.

13. The providers are also required to obtain a legally binding commitment from the owners of the TCIIs (i.e. the third-party vendors) that they will notify and furnish the providers with the necessary information to allow the providers to perform their duty under Part 3A to notify and furnish information required by the Commissioner. This legally binding commitment must also state that the TCII can meet comparable cybersecurity standards. If such a commitment could not be obtained by a provider, or if there is a failure by the TCII owner to notify the provider or furnish the required information to the provider, or to maintain the cybersecurity standards, the Commissioner may direct the provider to stop using the TCII.

C. Introduction of regulations for owners of STCC

14. Clause 15 of the Bill introduces Part 3B to the CSA, which provides for the regulation of a new category of systems known as STCC. STCC owners are subject to obligations similar to those of PCII owners.

15. STCCs are computers or computer systems that, for a time-limited period, are at high risk of cyberattacks. These systems, if compromised, would have serious detrimental effect on Singapore's national interests. Examples include the temporary systems in tracking and distributing vaccination during the COVID-19 pandemic, or temporary systems supporting high-key international events such as the Trump-Kim Summit in 2018 or the Youth Olympic Games in 2010.[2]

16. To designate a computer or computer system as an STCC, the Commissioner must be satisfied that, for a limited period of time, the system is at a high risk of a cybersecurity threat or incident, and that the loss or compromise of the system would have a serious detrimental effect on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

17. When designated as an STCC, the owner of the STCC is obliged to furnish information relating to the STCC and to report the cybersecurity incident in respect of STCC.

D. Introduction of regulations for ESCI

18. Clause 16 of the Bill introduces Part 3C to the CSA which provides for the designation of entities as ESCI. Obligations imposed on ESCI are relatively moderate as compared to those imposed on PCII, TCII and STCC, as the impact on Singapore's national interests resulting from cyberattacks on ESCIs would not be as severe as the other systems.

19. ESCIs are viewed as attractive targets for malicious threat actors because the disclosure of sensitive information in their computer systems, or the disruption of the functions that their computer or computer system perform, would have a detrimental effect on Singapore's interests.

[2] *Singapore Parliamentary Debates*, Official Report (7 May 2024) vol 95 (Dr Janil Puthucheary, Senior Minister of State for Communications and Information).

© 2024 Lee & Lee. All Rights Reserved

A potential example would be universities.[3] However, the list of entities designated as ESCI will not be disclosed publicly, to avoid drawing unnecessary attention to these ESCIs.

20. To designate an entity as an ESCI, the Commissioner must be satisfied that the entity stores sensitive information in a system which is under the entity's control, or uses a computer system under the entity's control to perform a function which, if disrupted, will have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore.

21. Entities designated as an ESCI will be obligated to furnish information and report cybersecurity incidents which relate to the system of special cybersecurity interest or any other computer or computer system under the entity's control, where the incident will result in a breach in the availability, confidentiality, or integrity of the entity's data or has a significant impact on the business operations of the entity. This is a narrower requirement compared to those of PCII, TCII and STCC.

E. Introduction of regulations for major FDI service providers

22. Clause 17 of the Bill introduces Part 3D to the CSA, whereby providers of major FDI services will be regulated.

23. FDI services are defined in the Bill as any service which promotes the availability, latency, throughput, or security of digital services, and is specified in the Third Schedule to be added to the CSA. They include both cloud computing services (which can be delivered from a computer or computer system in or outside Singapore) and data centre facility services (which relies on a computer or computer system in Singapore encompassed within a facility in Singapore).

24. To designate an FDI service provider as a major FDI service provider, the Commissioner must be satisfied that the loss or impairment of the provision of that service is likely to lead to or cause disruption or deterioration of the operation of a large number of businesses or organisations in Singapore (when the service is provided from within or outside Singapore to persons in Singapore), or of the operation of a large number of businesses or organisations in or outside Singapore (when the service is provided wholly or partially from Singapore).

25. A major FDI service provider will be obligated to furnish information relating to the FDI and to report cybersecurity incidents in respect of the FDI, or any other computer or computer system under the provider's control, where the incident results in a disruption or degradation to the continuous delivery in Singapore of the FDI service, or has a significant impact on the major FDI service provider's business operations in Singapore.

Other amendments

A. "Computer" and "Computer system" will include virtual computers/computer systems for specific provisions

[3] *Singapore Parliamentary Debates*, Official Report (7 May 2024) vol 95 (Dr Janil Puthucheary, Senior Minister of State for Communications and Information).

© 2024 Lee & Lee. All Rights Reserved

26. Under the existing CSA, computers or computer systems are considered physical computers built out of dedicated physical hardware. However, the CSA has been amended to include "virtual computer" and "virtual computer system" in the definitions of "computer" and "computer system" respectively. The amendments will affect the scope of the regulations concerning PCII, TCII, STCC, and ESCI.

27. The amendments align with the technological advancements, as it is now possible for a computer or computer system to be totally virtual. Relevant owners or entities are now responsible for the cybersecurity of their virtualised computers or computer systems, and not other parties supplying the underlying physical infrastructure.

B. Designation of PCII that is wholly outside of Singapore

28. Under the CSA, the Commissioner is only able to designate a PCII if the computer or computer system is entirely, or partly, in Singapore. This means that the CSA is currently unable to regulate a PCII that is wholly located outside of Singapore.

29. When the Bill comes into operation, a new provision will be introduced to the CSA to allow a computer or computer system located wholly outside Singapore to be designated as a PCII, provided that its owner is in Singapore and that the computer or computer system would have been designated as a PCII under Section 7(1) if it had been located wholly or partly in Singapore. This allows the CSA to deal with situations where a PCII located overseas is supporting an essential service in Singapore.

C. Cyber Security Agency of Singapore will be given more leeway to respond to cybersecurity threats and incidents

30. Clause 13(b) of the Bill introduces a significant amendment to Section 15(4) of the CSA. This amendment bolsters the enforcement capabilities under the CSA against PCII owners who have failed to comply with the CSA. Specifically, it authorises the Deputy Commissioner, an Assistant Commissioner or authorised officers to inspect the PCII facilities if the Commissioner believes that the PCII owner has either not fulfilled its required duties or has submitted information that is false, misleading, inaccurate or incomplete under Section 10 of the CSA.

31. Currently, Part 5 of the CSA addresses the regulation of individuals providing licensable cybersecurity services. To strengthen the enforcement of this part, Clause 18 of the Bill grants additional powers to licensing officers. These powers enable officers to monitor compliance actively and intervene when necessary. The new powers include rights of entry, inspection as well as the authority to demand the production of records, accounts and documents from licensed cybersecurity service providers. The failure to comply without a reasonable excuse is a criminal offense.

D. Court can now order the payment of a civil penalty for a person who contravenes the CSA

32. With the expansion of obligations for PCII owners, the Bill permits the Commissioner, with the consent of the Public Prosecutor, to seek civil penalties in Court. This approach provides the flexibility to address various degrees of non-compliance based on factors such as the risk posed, the severity of the breach and the specific circumstances of each case.

© 2024 Lee & Lee. All Rights Reserved

Ramifications of the CSA amendments for our clients

33. If you are a provider of a computer or computer system which may potentially be designated as a CII, you should know that:

    a) The computer or computer system can be designated as a CII even if it is wholly located overseas; and

    b) The computer or computer system can be designated as a CII even if it is completely virtual.

34. If you are an existing provider who already owns a CII (as designated by the Commissioner), you should know that:

    a) You must now also report incidents that affect other computers or computer systems under your control, and computers or computer systems under the control of a supplier that is communicating with your CII; and

    b) Any of your other computer or computer system which are wholly located overseas, or virtual, can now also be designated as a CII.

35. If you are a provider who has engaged a third-party vendor to operate the computer or computer system for your service, and this computer or computer system would have otherwise been designated as a CII if the computer or computer system was owned by you, you should know that:

    a) These CIIs may be designated as a TCII, and you as a provider would have separate obligations to fulfil; and

    b) If you are the third-party vendor in this scenario, you may be expected to provide a legally binding commitment to the provider.

36. If you are an owner of an STCC, an ESCI, or a major FDI service provider, you should take note of the new obligations discussed above.

Conclusion

37. As computers and computer systems become increasingly essential in every aspect of our society and lives, they have become prime targets for sophisticated cyberattacks. There is thus a need for more robust measures to safeguard our digital ecosystems. It is also important for our cybersecurity laws and regulations to stay abreast of technological developments, especially with the breakneck pace of developments in this area. In this regard, the Bill is important and timely.

38. If you have any question regarding the above, please contact our Mr. Tan Tee Jim, SC (tanteejim@leenlee.com.sg) or Mr. Basil Lee (basillee@leenlee.com.sg).

© 2024 Lee & Lee. All Rights Reserved

About Lee & Lee

Lee & Lee is one of Singapore's leading law firms being continuously rated over the years amongst the top law firms in Singapore. Lee & Lee remains committed to serving its clients' best interests, and continuing its tradition of excellence and integrity. The firm provides a comprehensive range of legal services to serve the differing needs of corporates, financial institutions and individuals. For more information: visit www.leenlee.com.sg.

The following partners lead our departments:

Kwa Kim Li Managing Partner kwakimli@leenlee.com.sg	Quek Mong Hua Litigation & Dispute Resolution quekmonghua@leenlee.com.sg	Owyong Thian Soo Real Estate owyongthiansoo@leenlee.com.sg
Tan Tee Jim, *SC* Intellectual Property tanteejim@leenlee.com.sg	Adrian Chan Corporate adrianchan@leenlee.com.sg	Louise Tan Banking louisetan@leenlee.com.sg

© 2024 Lee & Lee. All Rights Reserved