MARSH

CLIENT ALERT

CYBERSECURITY BILL PASSES INTO LAW IN SINGAPORE

On Monday, February 5, 2018, the proposed Cybersecurity Bill was passed into law in Singapore, implementing new licensing and regulatory requirements for owners of Critical Information Infrastructure (CII) and cybersecurity service providers. The Bill provides a framework for the regulation of CIIs and formalises the duties of CII owners in ensuring the cybersecurity of their respective CIIs.

WHO ARE CONSIDERED CII OWNERS?

CII refers to a computer or computer system (as designated by the Commissioner of Cybersecurity) that is necessary for the continuous delivery of essential services, the loss or compromise of which will have a debilitating effect on the availability of the essential service in Singapore.

CII owners are, in turn, defined as the legal owners of such CII. CII owners that provide the following 11 essential services in Singapore are subject to reporting and other obligations under the Bill.

ESSENTIAL SERVICES CATEGORIES

Energy

- Electricity generation, electricity transmission, or electricity distribution services.
- Services for the supply or transmission of natural gas for electricity generation.

Water

- Water supply services.
- Services relating to collection and treatment of used water.
- Services relating to management of storm water.

Banking & Finance

- Banking services, including cash withdrawal and deposits, corporate lending, treasury management, and payment services.
- Payments clearing and settlement services.
- Securities trading, clearing, settlement, and depository services.
- Derivatives trading, clearing, and settlement services.
- Services relating to maintenance of monetary and financial stability.
- Currency issuance.
- Services relating to cash management and payments for the Government.

Aviation

- Air navigation services.
- Airport passenger control and operations.
- Airport baggage and cargo handling operations.
- Aerodrome operations.
- Flight operations of aircraft.

Maritime

- Monitoring and management of shipping traffic.
- Container terminal operations.
- General and bulk cargo terminal operations.
- Cruise and ferry passenger terminal operations.
- Pilotage, towage, and water supply.
- Bunker supply.
- Salvage operations.
- Passenger ferry operations.

Info-Communications

- Fixed telephony services.
- Mobile telephony services.
- Broadband internet access service.
- National domain name registry services.

Healthcare

- Acute hospital care services.
- Services relating to disease surveillance and response.

Land Transport

- Rapid transit systems operated under a licence granted under the Rapid Transit Systems Act (Cap. 263A).
- Bus services operated under a bus service licence granted under the Bus Services Industry Act 2015 (Act 30 of 2015).
- Monitoring and management of rapid transit systems operated under a licence granted under the Rapid Transit Systems Act.
- Monitoring and management of bus services operated under a bus service licence granted under the Bus Services Industry Act 2015.
- Monitoring and management of road traffic.

Security & Emergency Services

- Civil defence services.
- Police and security services.
- Immigration services.
- Registration services under the National Registration Act (Cap. 201).
- Prison security and rehabilitation services.

Government

- Services relating to the electronic delivery of Government services to the public.
- Services relating to the electronic processing of internal Government functions.

Media

- Services relating to broadcasting of free-to-air television and radio.
- Services relating to publication of newspapers.
- Security printing services.

CYBERSECURITY SERVICE PROVIDERS

The new law also incorporates a licensing framework for cybersecurity service providers and imposes on such service providers a duty to keep records.

The following are licensable cybersecurity services:

- Managed security operations centres (SOC).
- Penetration testing services.

Failure to adhere to the provisions relating to cybersecurity service providers may result in the revocation of licenses, the incurring of significant fines, penalties and/or an imprisonment term.

CII OWNERS OBLIGATIONS

While this is not an exhaustive list of the Bill requirements, CII owners may be required to adhere to a code of practice and must also comply with the following obligations as set out in the Bill:

- Notify the commissioner of a cybersecurity incident.
- Establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents.
- Conduct a cybersecurity risk assessment once a year.
- Provide an audit of the compliance of the CII once every two years.
- Participate, at the request of the commissioner, in cybersecurity exercises.

Please refer to the *Cybersecurity Bill* for all requirements.

IMPLICATIONS OF NON-COMPLIANCE

Under the new laws, CIIs that fail to notify a cyber incident to the commissioner or do not comply with the commissioner's instructions could face penalties of up to $100,000 and/or potential imprisonment. For further obligations and implications, please refer to the Cybersecurity Bill.

CYBER INSURANCE AS A SOLUTION

Cyber insurance is an integral part of a risk transfer strategy for any company reliant on an operational technology or information technology dependent infrastructure. Please contact your Marsh broker for further advice on effective cyber products.

DIRECTORS & OFFICERS CONCERNS

Cybersecurity risks and evolving cyber regulation are dominating boardroom conversations. Directors and Officers have come to the realisation that the potential liability arising from such risks for themselves, as well as their organisation, is nearly unlimited. Increasingly, regulators and shareholders will hold management accountable for poor risk management and cyber governance.

SUMMARY

The change in legislation may require immediate action from organisations to ensure the ability to comply with the new requirements. Compliance with the requirements following a breach could be costly – all affected organisations need to assess and understand the risk of these potential costs and to consider how best to manage and transfer them.

This new bill does not supersede or replace the Personal Data Protection Act (PDPA). Consideration should be given to the compliance of both legislations.

RICHARD GREEN
Cyber Leader, Asia
+65 6922 8136
Richard.D.Green@marsh.com