ATMD Bird & Bird

Summary of Changes to the Computer Misuse Act (Cap. 50A, 2007 Ed.)

January 2013

Introduction

The Computer Misuse (Amendment) Bill (Bill No. 36/2012) (the "Bill") was introduced on 12 November 2012 and passed on 14 January 2013. The Bill amends the Computer Misuse Act (Cap. 50A, 2007 Ed.) (the "Act") to allow the Government to take more timely and effective measures to prevent, detect and counter cyber attacks on critical information infrastructure[1] that may threaten Singapore's national security, essential services, defence or foreign relations. Here are the highlights.

Renaming of the Act

The Act will be renamed the "Computer Misuse and Cybersecurity Act".

Strengthened cybersecurity measures and requirements

The Minister is now empowered to issue a certificate to direct a person or an organisation (referred to as a "specified person" in the Act) to adopt measures or comply with requirements necessary to:

- prevent;
- detect; or
- counter

a threat to a computer, computer service or class of computers or computer services ("threat").

This power only applies where the threat relates to the national security, essential services, defence or foreign relations of Singapore.

The Minister's powers include:

- requiring or authorising a specified person to direct another person to provide information necessary to identify, detect or counter any threat;
- requiring a specified person to provide the Minister or an authorised public officer information (real-time or otherwise) obtained from a computer controlled or operated by the specified person and that is necessary to identify, detect or counter any threat;
- requiring a specified person to provide to the Minister or an authorised public officer a report of a breach (or an attempted breach) of security fitting the description specified in the Minister's certificate; and
- enabling a specified person to exercise powers under Sections 39 and 40 of the Criminal Procedure Code (Cap. 68, 2012 Ed.) in fulfillment of his obligations.

Cybersecurity measures and requirements made paramount

The new measures or requirements referred to above overrides any:

- obligation;
- limitation;
- right;
- privilege; or
- immunity

imposed and/or conferred by any law, contract, or rules of professional conduct.

The above also applies to any direction given by a specified person for the purpose of taking any measure or complying with any requirement given by the Minister.

The new laws, however, do not confer any rights to the production of or access to any information subject to legal privilege.

Expansion of existing definition of "essential services"

The new law expands the existing definition of "essential services" to include:

- land transport infrastructure;
- aviation; and
- shipping.

Provision of immunity from civil and criminal liability

The new law explicitly confers immunity from any civil or criminal liability that may be incurred while fulfilling an obligation under the new law.

[1] "Critical Information Infrastructure" refers to essential information systems and assets including telecommunication networks, banking infrastructure, water, electricity, gas and public transportation systems.

Criminalisation of non-compliance and obstruction

A specified person who fails to comply with the Minister's directions without reasonable excuse will be guilty of an offence and be liable on conviction to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding 10 years or to both.

Any person who, without reasonable excuse:

- obstructs a specified person from complying with the latter's obligations; or
- fails to comply with any direction given by a specified person

shall be guilty of an offence and liable on conviction to a fine not exceeding S$50,000 or to imprisonment for a term not exceeding 10 years or to both.

Erecting safeguards to protect information obtained

Any information obtained by a specified person can only be used or disclosed in the following circumstances:

- to prevent, detect or counter a threat;
- to inform any police officer or law enforcement authority of a commission of an offence under the Act or any other written law; or
- to comply with a requirement of a court, the Act or any other written law.

In all other circumstances, the person from whom information is obtained, or the third party to whom confidential information belongs, must give written permission to use or disclose the information.

A person who fails to comply with the above will be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding 12 months or to both.

Contacts

For more details or any inquiries, please contact:

Koh Chia Ling

Partner

T : +65 6428 9847

chialing.koh@twobirds.com