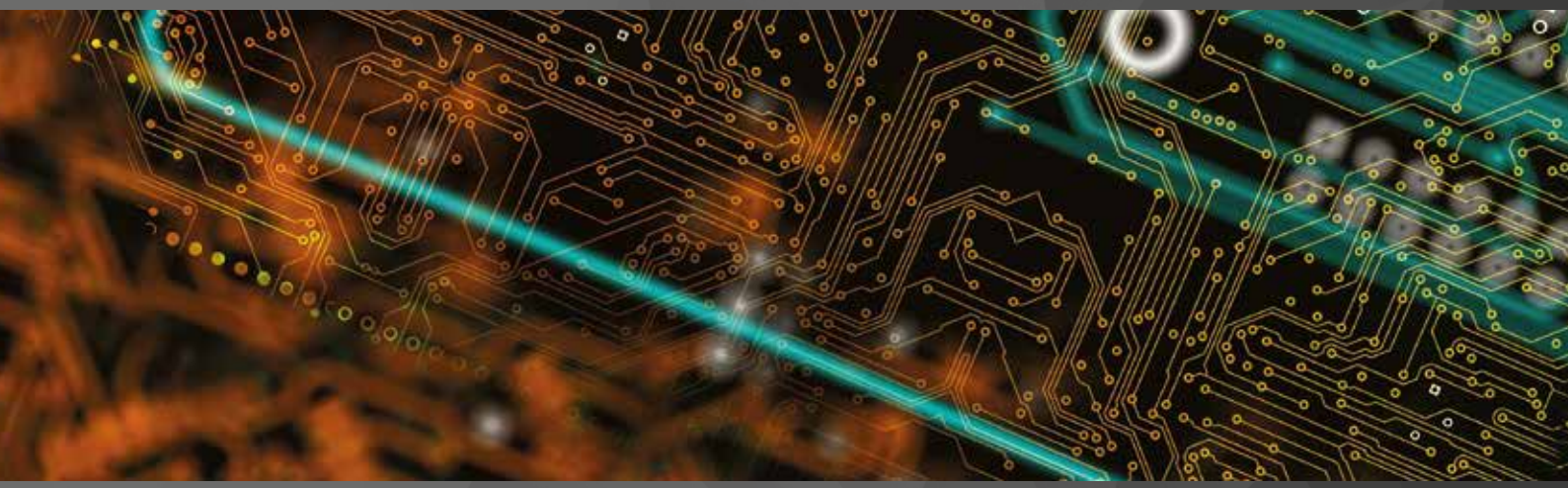
International Comparative Legal Guides



Cybersecurity 2021

A practical cross-border insight into cybersecurity law

Fourth Edition

Featuring contributions from:

Alburhan
Allen & Overy LLP
Ankura Consulting Group
Creel, García-Cuéllar, Aiza y Enríquez
Drew & Napier LLC
Eversheds Sutherland (Germany) LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Ince
Iwata Godo
Kellerhals Carrard
King & Wood Mallesons
Kluge Advokatfirma AS
Lee & Ko
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan LLP
Mori Hamada & Matsumoto
Nikolinakos & Partners Law Firm
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Ropes & Gray LLP
Rothwell Figg
Rubino Avvocati
Schönherr Rechtsanwälte GmbH
Simion & Baciu
Sirius Legal
Stehlin & Associés
TIME DANOWSKY Advokatbyrå AB

ICLG.com

Expert Chapters

Q&A Chapters

Singapore


Lim Chong Kin


David N. Alfred


Albert Pichlmaier

Drew & Napier LLC

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Under section 3(1) of the Computer Misuse Act (Cap. 50A) ("**CMA**"), it is an offence for any person to knowingly cause a computer to perform any function for the purpose of securing access without authority, to any program or data held in any computer. Upon conviction, an offender shall be liable for: a fine of up to $5,000; imprisonment for a term of up to two years; or both for the first offence.

In *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1999] 3 SLR(R) 653, the accused was found to have, *inter alia*, exploited certain vulnerabilities to hack into some of the servers of the victim, in order to gain unauthorised access to the computer files contained on the victim's server. The accused was sentenced to two months' imprisonment for the charge under section 3(1) of the CMA.

In *Tan Chye Guan Charles v Public Prosecutor* [2009] 4 SLR(R) 5, the accused was found to have accessed files on a laptop without authorisation, by copying them onto his thumbdrive when the laptop's owner left his laptop unattended to answer a phone call. The accused was sentenced to three weeks' imprisonment and fined $5,000.

Denial-of-service attacks

Yes. A denial-of-service ("**DOS**") attack is a cyber-attack meant to shut down a machine or network, thus making it inaccessible to its intended users.

Under section 7(1) of the CMA, any person who, knowingly and without authority or lawful excuse (a) interferes with, or interrupts or obstructs the lawful use of, a computer, or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, shall be guilty of an offence. Upon conviction, an offender shall be liable for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for the first offence.

There have not been any published judgments by the Singapore courts involving an offence involving a DOS attack.

Phishing

Possibly. Whilst phishing itself may not be an offence, a number of provisions criminalise actions which could include phishing.

Under section 3 of the CMA, it is an offence for any person to cause a computer to perform any function for the purpose of securing access without authority to any data held in any computer. It is possible, depending on the exact circumstances, for this to include phishing. An offender who is convicted under this section shall be liable for: a fine of up to $5,000; imprisonment for a term of up to two years; or both for a first offence.

In *Public Prosecutor v Lim Yi Jie* [2019] SGDC 128, the Court found the accused to have facilitated a phishing scam involving the use of a phishing website, causing a victim to divulge her 2-factor-authentication and time-sensitive PIN number to the accused, as the victim assumed that the phishing website was an official bank website. Although the accused was not responsible for the execution of the phishing scam (which, in the Court's view, could be an offence under section 3(1) of the CMA, then named as the Computer Misuse and Cybersecurity Act), the accused had attempted to cash two cheques that were the criminal proceeds of the phishing scam. The accused was thus charged and convicted of an offence under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A).

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Under section 5 of the CMA, it is an offence for any person who commits any act which he knows will cause an unauthorised modification of the contents of any computer. As the infection of IT systems with malware would cause an unauthorised modification of the contents of the infected computer, this could be an offence under section 5 of the CMA.

Upon conviction, the offender shall be liable for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving an offence under the CMA for the infection of IT systems with malware.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Yes. Under section 8B(1)(b) of the CMA, a person shall be guilty of an offence if that person makes, supplies, offers to supply or makes available, by any means, any of the following items, intending it to be used to commit or facilitate the commission of an offence under section 3, 4, 5, 6 or 7 of the CMA:

(a) any device, including a computer program, that is primarily designed, adapted, or capable of being used for the purpose of committing an offence under section 3, 4, 5, 6 or 7; and
(b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

A person found guilty of this offence shall be liable on conviction for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving the distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime.

Possession or use of hardware, software or other tools used to commit cybercrime

Yes. Under section 8B(1)(a) of the CMA, it is an offence if a person obtains or retains certain items (as detailed in the following paragraph) and (i) intends to use it to commit or facilitate the commission of an offence under section 3, 4, 5, 6 or 7 of the CMA, or (ii) does so with a view to it being supplied or made available, by any means, for use in committing or in facilitating the commission of any of those offences.

The items in question are:

(a) any device, including a computer program, that is primarily designed, adapted or is capable of being used for the purpose of committing an offence under section 3, 4, 5, 6 or 7; and
(b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

A person found guilty of this offence shall be liable on conviction for: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

There are presently no published judgments by the Singapore courts involving the possession or use of hardware, software or other tools used to commit cybercrime.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Under section 4 of the CMA, it is an offence for a person to cause a computer to perform any function for the purposes of securing access to any program or data held in any computer, with the intent to commit a number of offences, including certain offences involving fraud or dishonesty. A person convicted of such an offence is liable for: a fine not exceeding $50,000; imprisonment for a term not exceeding 10 years; or both.

Penalties for identity theft and identity fraud are also set out in the Penal Code (Cap. 224) ("**Penal Code**"). Under section 419 read with section 416 of the Penal Code, a person who cheats by personation (i.e., if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is), is guilty of an offence and, upon conviction, liable for: imprisonment for a term of up to five years; a fine; or both. Whilst this offence is of general application, it could also extend to the cyber context.

Separately, section 170 of the Penal Code criminalises the offence of personating a public servant. Any person who is convicted of this offence shall be liable upon conviction for: imprisonment for a term which may extend to two years; a fine; or both.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Under section 8A(1) of the CMA, it is an offence for a person who, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 of the CMA:

(a) obtains or retains the personal information; or
(b) supplies, offers to supply, transmits or makes available, by any means the personal information.

Upon conviction, an offender may be sentenced to: a fine of up to $10,000; imprisonment for a term of up to three years; or both for a first offence.

Additionally, it is also an offence under section 136(1) of the Copyright Act (Cap. 63) ("**Copyright Act**") for a person who (a) makes for sale or hire, (b) sells or lets for hire, or by way of trade offers or exposes for sale or hire, or (c) by way of trade exhibits in public, any article which he knows or ought reasonably to know to be an infringing copy of the work. Upon conviction, an offender may be liable for a fine of up to: $10,000 for the article or for each article in respect of which the offence was committed, or $100,000 (whichever is the lower); imprisonment for a term of up to five years; or both.

In addition, it is also an offence under section 136(3) of the Copyright Act for any person who, at the time when copyright subsists in a work, distributes, for either (a) the purposes of trade, or (b) other purposes (but to such an extent as to affect prejudicially the owner of the copyright), articles which he knows to be infringing copies of the work. Upon conviction, an offender may be liable for: a fine of up to $50,000; imprisonment for a term of up to three years; or both.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Yes. Under section 3(1) of the CMA, any person who knowingly causes a computer to perform any function for the purpose of securing access without authority, to any program or data held in any computer, shall be guilty of an offence. Upon the first conviction, the offender shall be liable for a fine of up to $5,000; imprisonment for a term of up to two years; or both.

Given that penetration testing would necessarily involve gaining access to a computer system, it is possible that such unsolicited penetration testing (i.e., penetration testing done without any authorisation from the owner of the computer system) would constitute an offence under section 3(1) of the CMA.

Even if the penetration testing is unsuccessful, such an act may still be an offence. Under section 10 of the CMA, any person who attempts to commit an offence or does any act preparatory to an offence under the CMA shall be guilty of that offence and shall be liable on conviction for the punishment provided for the offence.

In *Public Prosecutor v James Raj s/o Arokiasamy* [2015] SGDC 36, the accused pleaded guilty and was convicted of the unauthorised hacking of a number of websites, including the websites of a well-known church in Singapore, the blog of a journalist, and a political party's website, as well as the unsolicited scanning and penetration testing of various government servers. The accused was sentenced to six months' imprisonment for the charges pertaining to the unsolicited scanning and penetration testing of various government servers under section 3(1) read with section 10 of the CMA.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Yes. The offences listed under Part II (i.e., sections 3 to 10) of the CMA are generally broad enough to address activities that adversely affect or threaten the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

For example, unauthorised modification of computer material (i.e., adversely affecting or threatening the integrity of computer material) is an offence under section 5 of the CMA, and unauthorised obstruction of use of computer (i.e., adversely affecting or threatening the availability of a computer system) is an offence under section 7 of the CMA.

Additionally, under section 10 of the CMA, abetments and attempts of the offences under Part II of the CMA are also treated as offences, and a person who abets or attempts to do any act preparatory to or in furtherance of the commission of any offence shall be guilty of that offence.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the above offences have extraterritorial application.

In respect of the CMA, section 11 of the CMA provides that the provisions of the CMA shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore. Where an offence is committed outside Singapore, the offender may be dealt with as if the offence had been committed within Singapore, if:

(a) for the offence in question, the accused was in Singapore at the material time;
(b) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8 of the CMA), the computer, program or data was in Singapore at the material time; or
(c) the offence causes, or creates a significant risk of, serious harm in Singapore.

Thus, where a person commits an offence under the CMA from a location outside Singapore, the person in question may nonetheless be prosecuted under the CMA as if the person had committed the offence within Singapore.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

Not necessarily. The offences under the CMA do not set out any general exceptions or factors that must be considered by a court in mitigation.

Nonetheless, there are factors that may be taken into account by the court in determining the appropriate sentence. For example, the fact that an offender had no intention to make a financial gain through his actions, and did not, in fact, make any financial gain, may have some impact in mitigating the length of a sentence, or the quantum of a fine.

2 Cybersecurity Laws

2.1 *Applicable Law*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

There are a number of applicable laws in Singapore relating to cybersecurity. Some of these laws are:

Cybersecurity Act 2018 ("Cybersecurity Act")

The Cybersecurity Act sets out a framework for the monitoring of Critical Information Infrastructures ("**CIIs**"), including imposing obligations on owners of CIIs to report cybersecurity incidents, and provides for the appointment of a Commissioner of Cybersecurity to, amongst others, oversee and promote the cybersecurity of computers and computer systems in Singapore.

In addition, the Commissioner of Cybersecurity is also empowered under the Cybersecurity Act to issue or approve one or more codes of practice of standards of performance for the regulation of owners of CIIs with respect to measures to be taken by them to ensure the cybersecurity of the CII. However, these codes of practice are meant for guidance, and do not have legislative effect.

As of the time of writing, the Commissioner of Cybersecurity has issued one such code: the Cybersecurity Code of Practice for Critical Information Infrastructure.

Personal Data Protection Act 2012 ("PDPA")

The PDPA imposes a number of data protection obligations on organisations, in respect of personal data. Importantly, section 24 of the PDPA requires organisations to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Computer Misuse Act (Cap. 50A)

As mentioned above, the CMA covers a number of cyber offences, including, but not limited to, offences such as the exploiting of computer vulnerabilities to gain unauthorised access to a computer system (section 3 of the CMA).

Copyright Act (Cap. 63)

The Copyright Act criminalises copyright infringement. Specifically, it is an offence for a person to, at a time when copyright subsists in a work, (a) make for sale or hire, (b) sell or let for hire, or, by way of trade, offer or expose for sale or hire, or (c) by way of trade, exhibit in public, any article which he knows, or ought reasonably to know, to be an infringing copy of the work.

Strategic Goods (Control) Act (Cap. 300)

The Strategic Goods (Control) Act sets out provisions relating to the transfer and brokering of strategic goods and strategic goods technology. The list of items that have been prescribed by the Minister as strategic goods and strategic goods technology includes "information security" systems, equipment and components (i.e., systems, equipment and components designed or modified to use "cryptography for data confidentiality" having "in excess of 56 bits of symmetric key length, or equivalent").

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes. Under the Cybersecurity Act, the Commissioner of Cybersecurity may designate a computer or computer system as a CII under the Cybersecurity Act, if he is satisfied that (a) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore, and (b) the computer or computer system is located wholly or partly in Singapore.

The list of essential services are set out in the First Schedule to the Cybersecurity Act, which consists of services in the following industries: energy; info-communications; water; healthcare; banking and finance; security and emergency services; aviation; land transport; maritime; services relating to the functioning of Government; and media.

The obligations placed on owners of CIIs include having to report cybersecurity incidents to the Commissioner of Cybersecurity (section 14 of the Cybersecurity Act), conducting regular cybersecurity audits and risk assessments of CII (section 15 of the Cybersecurity Act) and furnishing information on, amongst others, the design, configuration and security of the CII to the Commissioner of Cybersecurity upon the Commissioner of Cybersecurity's written notice to do so (section 10 of the Cybersecurity Act).

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Under section 14(2) of the Cybersecurity Act, the owner of a CII must establish mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the CII, as set out in any applicable code of practice.

Separately, the Protection Obligation under the PDPA requires organisations to put in place reasonable security measures to protect personal data under its possession and/or control. However, the PDPA does not specify the specific measures that organisations should take.

In its Guide to Managing Data Breaches 2.0 (the "**Data Breach Guide**"), the Personal Data Protection Commission ("**PDPC**") sets out what organisations should do to prevent data breaches. First, it states that organisations should implement monitoring measures and tools to provide early detection and warning to organisations. Examples include:

(a) monitoring of inbound and outbound traffic for websites and databases for abnormal network activities;
(b) usage of real-time intrusion detection software designed to detect unauthorised user activities, attacks, and network compromises; and
(c) usage of security cameras for monitoring of internal and external perimeters of secure areas such as data centres and server rooms.

The Data Breach Guide also encourages organisations to put in place a data breach management plan, which would include the following information:

(a) a clear explanation of what constitutes a data breach (both suspected and confirmed);
(b) how to report a data breach internally;
(c) how to respond to a data breach; and
(d) responsibilities of the data breach management team.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. In respect of data protection, the PDPC encourages organisations to report information related to Incidents or potential Incidents. In respect of the Cybersecurity Act, owners of CIIs are statutorily obligated to report Incidents.

Personal Data Protection Act 2012

At present, the PDPA does not require organisations to make any reports to the PDPC.

However, in the Data Breach Guide, the PDPC encourages organisations to notify the PDPC and/or affected individuals of a data breach that is: (a) likely to result in significant harm or impact to the individuals to whom the information relates; or (b) of a significant scale (i.e., involves personal data of 500 or more individuals). The guide also states that organisations should inform the relevant parties as soon as practicable and, in the case of the PDPC, no later than 72 hours after assessing that the data breach has met one of the requirements for notification to the PDPC.

The organisation should inform the PDPC of the following:

- the extent of the data breach;
- the type(s) and volume of personal data involved;
- the cause or suspected cause of the breach;
- whether the breach has been rectified;
- the measures and processes that the organisation had put in place at the time of the breach;
- information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so; and
- the contact details of person(s) whom the PDPC could contact for further information or clarification.

In general, there are no express defences or exemptions which organisations may rely on to prevent publication of that information. The PDPC is empowered, under regulations 16 to 20 of the Personal Data Protection (Enforcement) Regulations 2014, to publish a decision or direction ("**Decision**"), or a summary of the decision or direction ("**Summary**"). However, where a Decision contains personal data or information that is treated as confidential under the PDPA, the PDPC may either redact such data and information from the published Decision or publish a Summary that excludes such data and information. Persons providing information to PDPC may identify any such information which is confidential and provide a written statement giving reasons why the information is confidential (section 59 (3) and (4) of the PDPA). In considering whether to publish a Decision or Summary, the PDPC has stated that it will generally publish a Decision relating to an organisation that is found to have contravened its obligations under the PDPA. Amongst other reasons, this is for transparency, and so that other organisations may take note of the manner in which the Commission has applied the PDPA in specific cases and take preventive measures to avoid similar occurrences.

Additionally, as of this time of writing, the PDPC has published the draft Personal Data Protection (Amendment) Bill 2020, which will introduce, *inter alia*, a mandatory breach notification obligation. This proposed mandatory breach notification obligation is in line with the existing guidelines under the Data Breach Guide (i.e., notification should be made if it is likely to result in significant harm or is of a significant scale). As of the time of writing, the Personal Data Protection (Amendment) Bill 2020 has yet to be passed.

Cybersecurity Act

Under section 14(1) of the Cybersecurity Act, the owner of a CII must notify the Commissioner of Cybersecurity of the occurrence of any of the following:

(a) a prescribed cybersecurity incident in respect of the critical information infrastructure;
(b) a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure; and/or
(c) any other type of cybersecurity incident in respect of the critical information infrastructure that the Commissioner has specified by written direction to the owner.

In particular, the owner of the CII is required to notify the Commissioner of Cybersecurity, within two hours after a cybersecurity incident, of the following:

(i) the critical information infrastructure affected;
(ii) the name and contact number of the owner of the critical information infrastructure;
(iii) the nature of the cybersecurity incident, whether it was in respect of the critical information infrastructure or an interconnected computer or computer system, and when and how it occurred;
(iv) the resulting effect that has been observed, including how the critical information infrastructure or any interconnected computer or computer system has been affected; and
(v) the name, designation, organisation and contact number of the individual submitting the notification.

The owner of the CII is then required to provide the following supplementary details within 14 days via the Cyber Security Agency of Singapore's website:

(i) the cause of the cybersecurity incident;
(ii) its impact on the critical information infrastructure, or any interconnected computer or computer system; and
(iii) what remedial measures have been taken.

The Cybersecurity Act also generally empowers the Commissioner of Cybersecurity to investigate and prevent cybersecurity incidents (not limited to those involving CIIs), including but not limited to requiring any person to answer any question or to produce any physical or electronic record that is in possession of that person to the incident response officer, which the incident response officer considers to be related to any matter relevant to the investigation.

Under section 43 of the Cybersecurity Act, every person must preserve, and aid in preserving, *inter alia*, all matters relating to a computer or computer system of any person that may have come to the Commissioner of Cybersecurity's and/or incident response officer's knowledge in the performance of his or her functions or the discharge of his or her duties under the Act. For this reason (amongst others), any information furnished would not likely be published.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

As stated above, the PDPC, in its Data Breach Guide, encourages organisations to notify the PDPC and/or affected individuals of a data breach that is: (a) likely to result in significant harm or impact to the individuals to whom the information relates; or (b) of a significant scale (involves personal data of 500 or more individuals). In respect of the affected individuals, the guide states that organisations should inform these affected individuals as soon as practicable.

The information that should be given to the affected individuals include:

- how and when the data breach occurred;
- types of personal data involved in the data breach;
- what the organisation has done or will be doing in response to the risks brought about by the data breach;
- specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- contact details and how affected individuals can reach the organisation for further information or assistance (e.g., helpline numbers, e-mail addresses or websites); and/or
- where applicable, what type of harm/impact the individual may suffer from the compromised data.

In addition, the PDPC has published the draft Personal Data Protection (Amendment) Bill 2020, which will introduce, *inter alia*, a mandatory breach notification obligation that would require organisations to inform affected individuals of a breach. This has yet to take effect.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

There are different regulators responsible for enforcing the above requirements.

The PDPC, which is a division within the Infocomm Media Development Authority ("**IMDA**"), is the regulator responsible for enforcing the provisions under the PDPA.

The Commissioner of Cybersecurity, working together with his team at the Cyber Security Agency of Singapore ("**CSA**"), is responsible for the enforcement of the provisions under the Cybersecurity Act.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

There are a range of potential penalties, depending on the exact requirements that have not been complied with.

Under the PDPA, the PDPC is empowered to issue directions to ensure that organisations comply with the PDPA, including imposing a financial penalty of up to $1 million. It should be noted that, with the upcoming changes in the Personal Data Protection (Amendment) Bill 2020, the financial penalty that may be imposed will be increased to the higher of (a) 10% of an organisation's annual turnover, or (b) $1 million. However, as of the time of writing, this has yet to be passed.

Under the Cybersecurity Act, the failure of a CII owner to report a cybersecurity incident in respect of a CII, without reasonable excuse, is an offence and the owner shall be liable on conviction to a fine of up to $100,000; imprisonment for a term of up to two years; or both.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In respect of non-compliance with the PDPA, the PDPC has published a number of its enforcement decisions.

One of the more notable enforcement cases is *Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDPC 3. In that case, the PDPC took enforcement action against (1) Singapore Health Services Pte. Ltd. ("**SingHealth**"), and (2) Integrated Health information Systems Pte. Ltd. ("**IHiS**"), for failing to put in place reasonable security measures to protect personal data under its possession and control, leading to a data breach wherein the medical records of 1.5 million patients were leaked. The PDPC imposed a financial penalty of $250,000 on SingHealth and $750,000 on IHiS.

There are no published enforcement actions that have been taken against owners of CIIs under the Cybersecurity Act.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)

There are likely to be no restrictions on the usage of beacons for protection purposes, *unless* the data collected by such beacons constitutes personal data under the PDPA.

Under the Consent Obligation of the PDPA, organisations are required to obtain consent (or deemed consent) from individuals before the collection, use and disclosure of that individual's personal data. Thus, beacons would not be permissible if they collect personal data without the consent (or deemed consent) of the individuals in question, unless an exception to the Consent Obligation applies under the PDPA.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)

There are likely to be no restrictions on the usage of honeypots for the purpose of protection of IT systems. Neither the Cybersecurity Act nor the PDPA restrict the usage of honeypots as a way of protecting IT systems.

In fact, the relevant regulators have addressed the use of honeypots, and do not appear to object to their usage. In an article published by the CSA in 2019, it explained honeypots and their role in cyber defence. Additionally, the PDPC's Guide to Securing Personal Data in Electronic Medium encourages the use of "*defences that may be used to improve the security of networks*".

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)

There are likely to be no restrictions on the usage of sinkholes for the purpose of protection of IT systems. As is the case for honeypots, neither the Cybersecurity Act nor the PDPA restrict the usage of sinkholes for the purpose of protecting IT systems.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber-attacks?

Yes, organisations are permitted to monitor or intercept electronic communications on their networks in order to prevent or mitigate the impact of cyber-attacks.

There is no law prohibiting an organisation from monitoring or intercepting electronic communications on their *own* networks. However, if such data falls within the definition of personal data, then the organisation may be required to obtain consent from the relevant individuals.

We note that, under the Protection Obligation of the PDPA, organisations are required to put in place reasonable security measures to protect personal data under its possession or control. Depending on a number of factors, the monitoring or intercepting of electronic communications on an organisation's networks may be considered to be one such reasonable security measure.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber-attacks?

Yes. Under the Strategic Goods (Control) Act, the import and export of certain types of strategic goods and strategic goods technology is controlled, including "information security" systems, equipment and components (i.e., systems, equipment and components designed or modified to use "cryptography for data confidentiality" having "in excess of 56 bits of symmetric key length, or equivalent").

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes. The PDPA sets out the baseline standards that all organisations must meet, in respect of the protection of personal data. However, certain sectoral regulators may impose higher standards on a particular industry, especially where the personal data commonly collected, used and disclosed in these industries are sensitive in nature.

4.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Financial Services Sector

In respect of the Financial Services Sector, the Monetary Authority of Singapore ("**MAS**") has set out, in its published Guidelines on Technology Risk Management ("**MAS TRM Guidelines**"), risk management principles and best practice standards to guide financial institutions in (a) establishing a sound and robust technology risk management framework, (b)

strengthening system security, reliability, resiliency, and recoverability, and (c) deploying strong authentication processes to protect customer data, transactions and systems. These include (non-exhaustively) requiring financial institutions to establish a technology risk management framework with oversight by the board and senior management to identify, assess, monitor, report and treat technology risks.

Additionally, the MAS has also issued a Notice on Cyber Hygiene, which requires banks to, amongst others, ensure that security patches are applied to address vulnerabilities in their computer systems.

Healthcare Sector

In the healthcare sector, the Ministry of Health has issued a Cybersecurity Advisory 1/2019 in the wake of the SingHealth data breach in 2018 (*Re Singapore Health Services Pte. Ltd. & Ors.* [2019] SGPDPC 3), which involved the medical personal data of 1.5 million individuals being leaked.

In this Cybersecurity Advisory, all licensees (i.e., hospitals, clinics, etc.) are strongly encouraged to review the Committee of Inquiry's recommendations and cybersecurity best practices, and to implement relevant measures, where appropriate.

Telecommunications Sector

The IMDA has published the Telecommunication Cybersecurity Codes of Practice, which are currently imposed on major Internet Service Providers (ISPs) in Singapore for mandatory compliance. Apart from security incident management requirements, the Codes include requirements to prevent, protect, detect and respond to cybersecurity threats. The Codes were formulated using international standards and best practices including the ISO/IEC 27011 and IETF Best Current Practices.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Under section 157 of the Companies Act, directors of a company are required to, amongst others, act honestly and use reasonable diligence in the discharge of the duties of their office. In addition, under the common law, directors are also required to carry out their duties with skill, care and diligence.

Thus, if a company fails to prevent, mitigate, manage or respond to an Incident due to a lack of honesty, or a lack of the requisite skill, care and diligence on the part of its directors, this may constitute a breach of directors' duties.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

(a) There is no present requirement for companies to designate a CISO under the relevant cybersecurity laws. The provisions of the Cybersecurity Act generally apply to owners of CIIs.

In respect of the PDPA, companies are required to appoint a Data Protection Officer ("**DPO**") under section 11(3) of the PDPA, whose duties include, amongst others, to:

- ensure compliance of PDPA when developing and implementing policies and processes for handling personal data;
- foster a data protection culture among employees and communicate data protection policies to stakeholders;
- manage data protection-related queries and complaints;
- alert management to any risks that might arise with regard to personal data; and
- liaise with the PDPC on data protection matters, if necessary.

(b) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to establish a written Incident response plan or policy in respect of that CII.

In respect of the PDPA, there is no specific requirement to establish a written Incident response plan or policy. However, section 12 of the PDPA requires organisations to, amongst others, develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA. This would likely include developing a policy relating to the handling of security incidents and data breaches.

Related to the above, the PDPC has recommended in its Data Breach Guide that organisations put in place a data breach management plan, which should set out, amongst others, how the organisation should respond to a data breach.

(c) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to conduct periodic cyber risk assessments.

There is no specific requirement under the PDPA for companies to conduct periodic cyber risk assessments, including for third-party vendors. However, in its Advisory Guidelines on Key Concepts in the PDPA, the PDPC has stated that organisations should take steps to ensure, amongst others, that its computer networks are secure, and that its IT service providers are able to provide the requisite standard of IT security.

(d) Under the Cybersecurity Act and the Cybersecurity Code of Practice for Critical Information Infrastructure, owners of a CII may be required to conduct periodic cyber risk assessments, which may include penetration testing and vulnerability assessments.

There is no specific requirement for companies to perform penetration tests or vulnerability assessments under the PDPA. However, as above, the PDPC has stated in its Guide to Data Protection Impact Assessments that organisations may conduct penetration tests as part of their reasonable security arrangements to protect personal data.

We further highlight that certain sectoral regulators in Singapore impose more stringent requirements on organisations within that sector. For example, the MAS imposes certain requirements in respect of cybersecurity on its licensees, including requiring its licensees to implement robust security measures to ensure that their systems and customer data are well protected against any breach or loss.

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, companies are not subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents, other than

those already mentioned above (i.e., to the relevant regulatory bodies).

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

If an Incident gives rise to a private actionable claim, the affected individual may have recourse against the organisation that caused the Incident.

Section 32 of the PDPA provides for a right of private action. Under this section, any person who suffers loss or damage directly as a result of a contravention of the organisation's obligations under Parts IV, V or VI of the PDPA (which set out organisations' obligations to protect individuals personal data) shall have a right of action for relief in civil proceedings in a court. This includes a breach of section 24 of the PDPA, which requires organisations to protect personal data which is in its possession or under its control (as outlined further above).

Under the CMA, a court may order an offender to pay a compensation amount to a victim of the offence. The victim may also pursue a civil remedy against the offender separately, as the order for payment of compensation does not prejudice the right of the victim to recover more than was compensated to him under the compensation order.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

In *IP Investment Management Pte Ltd and others v Alex Bellingham* [2019] SGDC 207, the third plaintiff (a natural person) successfully obtained an order enjoining the defendant, a former employee of the first and second plaintiffs (which were corporate entities engaged in a fund management business), from using, disclosing or communicating his personal data, and also obtained an order for the defendant to deliver up any copies of his personal data.

Finding the case in favour of the third plaintiff, the court held that the defendant had breached his obligations under the PDPA; in particular, the Consent Obligation and Purpose Limitation Obligation. The court also found that the third plaintiff had suffered loss as a result of the defendant's breach of the Consent Obligation and Purpose Limitation Obligation.

It is worth noting that the court found that the first and second plaintiffs had no legal standing to bring the claim under section 32 of the PDPA, as it held that section 32 of the PDPA did not extend to corporate entities. Thus, as the first and second plaintiffs were corporate entities, their applications were disallowed by the court.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes. Depending on the circumstances of the Incident, it is possible that one or more causes of action in tort may be applicable. For example, if an organisation had breached its duty of care under the tort of negligence, by failing to put in place measures to prevent an Incident, the organisation may be found liable under this tort.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents in Singapore.

As of the date of writing, a number of insurance providers in Singapore provide cyber insurance, which covers, amongst others, data protection/personal data liability and corporate data liability.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

No, there are presently no regulatory limitations to insurance coverage against specific types of loss in respect of cyber insurance.

However, it bears noting that as insurance contracts are ultimately contracts, they are also subject to contractual law principles. These principles include, amongst others, that such a contract will be enforceable only if it is not tainted by illegality or is contrary to public policy.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

There are a number of laws that would provide investigatory powers to the relevant regulators/law enforcement personnel.

Generally, the Singapore law enforcement authorities have fairly broad powers under the Criminal Procedure Code (Cap. 68) ("**CPC**") to access, inspect and check the operation of any computer that they suspect is or has been used in connection with, or contains or contained evidence relating to, an arrestable offence. This may include offences under the CMA.

In relation to the PDPA, section 50 of the PDPA empowers the PDPC with powers of investigation to investigate whether organisations are in compliance with the PDPA. The powers are set out in the Ninth Schedule of the PDPA, which includes, amongst others, the power to require documents or information to be produced by the organisation to the PDPC, as well as the power to enter premises (both without and with a warrant), subject to certain conditions being satisfied.

In relation to the Cybersecurity Act, the Commissioner of Cybersecurity is empowered under sections 19 and 20 to investigate and prevent cybersecurity incidents. These powers include requiring, by written notice, any person to produce to the incident response officer appointed by the Commissioner of Cybersecurity, any physical or electronic record, or document that is in the possession of that person.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

No, there are no requirements for organisations to implement backdoors in their IT systems for law enforcement authorities. However, there is a requirement (under certain circumstances) to provide law enforcement authorities with encryption keys.

Under section 40 of the CPC, for the purposes of investigating an arrestable offence, an authorised police officer or other authorised person can require any person whom he reasonably suspects to be in possession of any decryption information, to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.

Lim Chong Kin heads Drew & Napier's Technology, Media and Telecommunications Practice Group, and is co-head of the firm's Data Protection, Privacy & Cybersecurity Practice.
Under Chong Kin's leadership, these Practices are consistently ranked as the leading practices in Singapore. His clients include the telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers.
Chong Kin has been an external legal and regulatory advisor for the Personal Data Protection Commission of Singapore since 2013, and he played a key role in the liberalisation of Singapore's telecoms, media and postal sectors, where he drafted the competition frameworks.
Chong Kin is highly regarded by his peers, clients and rivals alike for his expertise, and is consistently recommended as a leading lawyer by major international legal publications such as *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Who's Who Legal*, *The Guide to the World's Leading Competition & Antitrust Lawyers/Economists*, *Global Competition Review*, *Practical Law Company – Which Lawyer?*, *Asialaw Profiles* and *Best Lawyers*.

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 65314110
Fax: +65 65354864
Email: chongkin.law@drewnapier.com
URL: www.drewnapier.com

David N. Alfred is a director of Drew & Napier LLC and co-head of the firm's Data Protection, Privacy and Cybersecurity Practice. He is concurrently co-head and programme director of the Drew Data Protection & Cybersecurity Academy. David is a data protection, cybersecurity and technology lawyer with over 20 years' experience advising on a broad range of matters relating to digital technology, telecommunications and the internet.
David's practice over the last 10 years has focused on data protection and cybersecurity. He has substantial experience advising on data protection compliance, public policy and legislation, regulatory enforcement, data breaches and international aspects of data protection.
Prior to joining the firm, David was the first Chief Counsel to Singapore's data protection authority, the Personal Data Protection Commission. He has also worked in other in-house roles including with Singapore's media and telecom regulator, the Info-communications Media Development Authority.

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 65312342
Fax: +65 65354864
Email: david.alfred@drewnapier.com
URL: www.drewnapier.com

Albert Pichlmaier is a senior cybersecurity engineer with Drew & Napier LLC and concurrently course director (cybersecurity) with the Drew Data Protection & Cybersecurity Academy. Albert is an IT professional with 30 years of international experience in the private and public sectors. He has worked in a wide range of IT and security domains, from smart card firmware development and test automation, to artificial intelligence and blockchain development. Albert holds a degree in computer science and the CISSP and CDPSE certifications.
Prior to joining the firm, Albert worked for over 10 years in the public sector in Singapore. Most recently, he worked with Singapore's data protection authority, the Personal Data Protection Commission, where he was involved in technology and cybersecurity assessments for data protection compliance and enforcement cases. Prior to that, he was the technical manager for common criteria certifications with the Info-communications Development Authority of Singapore.

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 65314108
Fax: +65 65354864
Email: albert.pichlmaier@drewnapier.com
URL: www.drewnapier.com

Drew & Napier LLC has provided exceptional legal advice and representation to discerning clients since 1889 and is one of the leading and largest law firms in Singapore.
The firm's work in data protection, privacy and cybersecurity precedes the advent of Singapore's Personal Data Protection Act 2012 and Cybersecurity Act 2018. Over the last decade, Drew & Napier has been one of the leading Singapore practices in the fields of data protection, privacy and cybersecurity. The firm has advised and acted for a wide range of clients on a variety of matters which run the full gamut. These include implementation of group-wide data protection compliance programmes, localisation of global data privacy policies, data protection training programmes, requirements of Singapore's Cybersecurity Act 2018, developing a data breach management plan, dealing with data breaches and cybersecurity incidents (whether involving hacking, malware or accidental disclosure), data breach reporting requirements, conducting data protection and regulatory risk audits and addressing *ad hoc* legal queries.

www.drewnapier.com

DREW & NAPIER

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by: global legal group