ICLG

The International Comparative Legal Guide to:

Cybersecurity 2018

1st Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Allen & Overy
Angara Abello Concepcion Regala & Cruz Law Offices
Baker McKenzie
Boga & Associates
BTG Legal
Christopher & Lee Ong
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
ENSafrica
Erkelens Law
Eversheds Sutherland
Holland & Hart LLP
JIPYONG
Josh and Mak International
King & Wood Mallesons
Lee, Tsai & Partners Attorneys-at-Law
Maples and Calder
MinterEllison
Mori Hamada & Matsumoto
Niederer Kraft & Frey Ltd.
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Shibolet & Co.
Simmons & Simmons LLP
Udo Udoma & Belo-Osagie

glg
global legal group

global legal group

Contributing Editors
Nigel Parker & Alex Shandro, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2017

ISBN 978-1-911367-77-2
ISSN 2515-4206

Strategic Partners

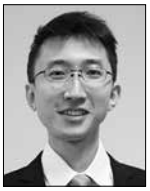
General Chapters:

Country Question and Answer Chapters:

Chapter 23

Singapore


Rajesh Sreenivasan


Michael Chen

Rajah & Tann Singapore LLP

1 Criminal Activity

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

According to the applicable legislation specified below, the following activities would constitute criminal offences in Singapore.

Hacking (i.e. unauthorised access)

Yes. Under section 3 of the CMCA, any person who knowingly causes a computer to perform any function for the purposes of securing access without authority to any program or data held in any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years or to both.

In *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1999] 3 SLR(R) 653, the accused relied on an exploit, instead of sophisticated software, to perform unauthorised access to an internet service provider server, among others. In *Lim Siong Khee v Public Prosecutor* [2001] 1 SLR(R) 631, the accused hacked the victim's email account by answering correctly the hint question to successfully retrieve passwords and to gain unauthorised access. He was sentenced to 12 months' imprisonment.

Denial-of-service attacks

Yes. Under section 7 of the CMCA, any person who knowingly and without authority or lawful excuse, (a) interferes with, 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 computer, shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years or to both.

There have been no prosecutions for denial-of-service attacks as yet. Nevertheless, such attacks are recognised as threats under Singapore's Cybersecurity Strategy.

Phishing

There is no specific provision that deals with phishing. However, under section 3 of the CMCA, any person who knowingly causes a computer to perform any function for the purposes of securing access without authority to any program or data held in any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding two years or to both.

There have been no prosecutions relating to phishing activities as yet. Nonetheless, as with denial-of-service attacks, phishing is also recognised as a threat in Singapore's Cybersecurity Strategy.

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

Yes. Under section 5 of the CMCA, a person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years or to both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Yes. Under section 8B of the CMCA, it is an offence for a person to obtain or retain any item (which includes hacking tools, among others) with the intent to use it to commit or facilitate commission of an offence under the CMCA.

A person found guilty of this offence shall be liable on conviction to a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years or to both.

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

Yes. Under section 4 of the CMCA, it is an offence to secure unauthorised access to any computer program or data, with the intent to commit an offence involving property, fraud or dishonesty. This offence is punishable on conviction by a fine not exceeding S$50,000 or imprisonment for a term not exceeding 10 years or to both.

In *Public Prosecutor v S Kalai Magal Naidu* [2006] SGDC 226, the accused was convicted under section 4 for conducting searches on her bank employer's computer systems to effect cash withdrawals from the victim's bank account. She was sentenced to four months' imprisonment for each charge under section 4.

Also, under section 5 of the CMCA, an accused may be charged for unauthorised modification of computer material. This may be seen in *Public Prosecuctor v Tan Hock Keong Benjamin* [2014] SGDC 16, where the accused used the victim's debit card that he found to make a purchase on eBay. It was held that he knew that by doing so, he would cause unauthorised modification to the contents of a computer, namely the data stored in the bank's servers, such that the online purchase would be approved.

In addition, the Penal Code contains provisions on cheating by personation. Although not cyber-specific, section 416 of the Penal

Code (cheating by personation) may apply to identity theft. It is an offence for anyone to cheat 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. The punishment is imprisonment for a term which may extend to five years or a fine or both.

Under section 170 of the Penal Code, it is an offence to personate a public servant. The punishment is imprisonment for a term which may extend to two years or 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 of the CMCA, it is an offence for a person to obtain or retain personal information, or to supply, offer to supply, transmit or make available the personal information, if the person knows or has reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of the CMCA. This offence is punishable on conviction by a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years or to both.

The theft of personal data could constitute an offence under the PDPA. Under section 51 of the PDPA, it is an offence for an organisation or individual to dispose of, alter, falsify, conceal or destroy personal data. The punishment for this offence is a fine of up to S$5,000 in the case of an individual, and up to S$50,000 in any other case.

Under section 136 of the Copyright Act, the following instances of copyright infringement are criminal offences, where the infringing party knows or ought reasonably to know that the copies are infringing ones: make for sale or hire infringing copies; sell or let for hire infringing copies; possess or import infringing copies for commercial purposes; and distribute infringing copies for commercial purposes.

There is also criminal liability if the copyright infringement is wilful and either or both of certain situations apply: (i) the extent of the infringement is significant; and/or (ii) the person does the act to obtain a commercial advantage.

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

Under the CMCA, it is an offence to perform unauthorised use or interception of a computer service (section 6), and for unauthorised disclosure of access code (section 8). Attempts are also caught under section 10 of the CMCA, whereby anyone who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under the CMCA shall be guilty of an offence. Therefore, any forms of attempts to gain unauthorised access, or to commit any other offences under the CMCA, will constitute offences as well.

Failure by an organisation to implement cybersecurity measures

The PDPA requires organisations to protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. If the organisation does not comply with this requirement, the Personal Data Protection Commission (the "**PDPC**") can give the organisation directions to ensure compliance; for example, directing the organisation to pay a financial penalty of up to S$1 million.

The Cybersecurity Bill proposes to require owners of CII to establish mechanisms and processes as may be necessary in order to detect any cybersecurity threat in respect of its critical information infrastructure. Please note that the draft Cybersecurity Bill is still undergoing review at the time of writing and has yet to take effect.

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

The CMCA, PDPA and Penal Code have extraterritorial application. Section 11 of the CMCA specifies that the CMCA provisions have effect against any person, irrespective of nationality or citizenship, and even if the person is outside or within Singapore, if:

(a) the accused was in Singapore at the material time of the offence;

(b) the computer, program or data was in Singapore at the material time of the offence; or

(c) the offence causes or creates significant risk of serious harm in Singapore.

The above captures anyone who commits an offence under the CMCA for which the person targets a computer, program or data located in Singapore, or if the person was located in Singapore when the offence happened. Also, if the offence causes significant risk of serious harm in Singapore, then the extraterritorial provision may apply. Examples of serious harm include the disruption of or serious diminution of public confidence in essential services such as communications and transport infrastructure or public utilities.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The legislation does not specify mitigating factors to the above offences. Nevertheless, cooperation with the relevant regulators or enforcement authorities, or active steps taken to mitigate the loss or damage caused by any of the offences, could be viewed by a court as mitigating factors.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

In addition to legislation specifically targeted at cybercrime, the existing criminal offences as set out in the Penal Code and Sedition Act (Cap. 290), among others, may be able to encompass offences relating to cybersecurity. It is generally an offence (even though not specific to cybersecurity) to commit or facilitate terrorism activities, e.g. where there is financing of terrorism.

The Protection from Harassment Act (Cap. 256A) (the "**POHA**") establishes that it is an offence to intentionally cause harassment, alarm or distress, and to commit unlawful stalking. For example, unlawful stalking includes keeping the victim or a related person under surveillance.

2 Applicable Laws

2.1 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, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import / export controls, among others.

The Ministry of Communications and Information ("**MCI**") and

the Cyber Security Agency of Singapore ("**CSA**") issued a public consultation on the proposed Cybersecurity Bill, over the period from 10 July 2017 to 24 August 2017. At the time of writing, the MCI and CSA were still reviewing the feedback received during the public consultation. The draft Cybersecurity Bill is intended to establish a framework for the oversight and maintenance of national cybersecurity in Singapore. As described subsequently, the Cybersecurity Bill will impose duties and obligations on owners who own CII.

Notwithstanding the above, the current laws which relate to cybersecurity in Singapore include:

Computer Misuse and Cybersecurity Act (Cap. 50A) (CMCA)

The CMCA sets out penalties for various cybersecurity offences, as described in section 1 above. Depending on the offence, the maximum quantum of the fine ranges from between S$5,000 to S$50,000, and the maximum imprisonment term ranges from between two years to 10 years. The penalties may be enhanced in specific circumstances. For example, the maximum fine quantum and imprisonment term are increased in the case of second or subsequent conviction.

Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA)

The PDPA imposes data protection obligations on private organisations when they perform activities involving the collection, use and disclosure of personal data. The PDPC has powers to bring enforcement actions against organisations which fail to comply with these PDPA obligations.

Penal Code (Cap. 224)

As described in section 1 above, the Penal Code sets out offences relating to personation, among others.

Copyright Act (Cap. 63)

As described in section 1 above, the Copyright Act establishes that certain acts of copyright infringement constitute offences.

Strategic Goods (Control) Act (Cap. 300)

The Strategic Goods (Control) Act controls the transfer and brokering of strategic goods and strategic goods technology (including specified information security and cryptographic systems), among others.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, how (and according to what timetable) is your jurisdiction expected to implement the Network and Information Systems Directive? Please include details of any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Section 15A of the CMCA sets out the Minister for Communications and Information's powers to issue directions to any person or organisation to take such measures or comply with such requirements as may be necessary to prevent, detect or counter cyber threats to national security, essential services, defence, or foreign relations of Singapore. Under the CMCA, "essential services" means services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure; or emergency services such as police, civil defence or health services.

Section 9 of the CMCA enhances the punishment for certain offences that are committed on protected computers (including computers used for defence, communications, public utilities, and banking, among others). The applicable punishment is enhanced to a maximum fine of up to S$100,000, and/or imprisonment for a term not exceeding 20 years.

In the proposed Cybersecurity Bill ("**Bill**"), there are cybersecurity requirements that impose duties on owners of CII. Per the Bill, a CII means: 'a computer or computer system that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will lead to a debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore'. The Commissioner will have the power to designate a computer or computer system as a CII – such designation of a computer or computer system as a CII will be an official secret under the Official Secrets Act, and shall not be divulged to the public.

'Essential services' are specified in the First Schedule of the Bill. The First Schedule details 44 types of services which may be considered as 'essential services', under the broad categories of energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, Government, and media.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Under the Protection Obligation imposed by the PDPA, an organisation is required 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.

Under the draft Cybersecurity Bill, CII owners will be required to: comply with such codes of practice or directions in relation to the CII as may be issued by the Commissioner; carry out regular risk assessments; and participate in cybersecurity exercises as required by the Commissioner. Please note that the draft Cybersecurity Bill is still undergoing review at the time of writing and has yet to take effect.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import / export controls of encryption software and hardware.

No such issues have been reported to arise thus far in Singapore.

2.5 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 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 (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Section 15A of the CMCA sets out the Minister for Communications and Information's powers to issue directions to any person or

organisation to take such measures or comply with such requirements as may be necessary to prevent, detect or counter cyber threats to national security, essential services, defence, or foreign relations of Singapore. Such measures include providing any information that is necessary to identify, detect or counter any such threat, and/or a report of a breach or an attempted breach of security.

The PDPA does not contain a mandatory reporting obligation. However, the PDPC has issued non-binding guidelines recommending organisations to voluntarily notify the PDPC as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals.

The PDPC is currently reviewing the PDPA, and has issued a public consultation (from 27 July 2017 to 21 September 2017) seeking feedback on its proposed amendments. One amendment relates to mandatory data breach notification. It is proposed that organisations must notify the affected individuals and PDPC if a data breach has risks of impacting or harming the affected individuals, or to notify the PDPC if there is a significant scale of breach (involving 500 or more individuals). As the public consultation is still underway at the time of writing, there are no guidelines on the nature and scope of information needed to be reported. It is proposed that certain exemptions should apply to the reporting requirement; for example, if the organisation is acting on behalf of a public agency, or where other written law prohibit notification.

The draft Cybersecurity Bill proposes to impose a duty to report cybersecurity Incidents to the Commissioner of Cybersecurity if these Incidents involve CII or systems interconnected with CII. The information required for reporting will be prescribed by the Commissioner.

The draft Cybersecurity Bill also proposes to grant the Commissioner with powers to investigate all cybersecurity threats and Incidents (not only those involving CIIs); for example, to obtain information (such as technical logs), and, in the event of serious cybersecurity threats and Incidents, to enter premises where relevant computers and computer systems are located, access such computers, and scan computers for cybersecurity vulnerabilities. In addition, the Commissioner will be empowered to direct any person or organisation to take emergency measures and requirements to prevent, detect, counter any threat to a computer or computer service. Please note that the draft Cybersecurity Bill is still undergoing review at the time of writing and has yet to take effect.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

While there are no general restrictions with regards to voluntary sharing of information pertaining to an Incident, this is subject to sector-specific regulations and regulatory oversight which may constrain an organisation from sharing such information. If the information pertains to personal data, the organisation must comply with the PDPA in sharing such information. Additionally, organisations should not share information protected on the grounds of national secret or which is prejudicial to national security, under the Official Secrets Act and Internal Security Act, respectively.

2.7 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.

The PDPA does not contain a mandatory notification obligation. However, the PDPC has issued non-binding guidelines recommending organisations to voluntarily notify affected individuals immediately if a data breach involves sensitive personal data. Note that "sensitive personal data" is not defined under the PDPA, only "personal data".

The PDPC is currently reviewing the PDPA, and has issued a public consultation (from 27 July 2017 to 21 September 2017) seeking feedback on its proposed amendments. One amendment relates to mandatory data breach notification. It is proposed that organisations must notify the affected individuals and PDPC if a data breach has risks of impacting or harming the affected individuals, or to notify the PDPC if there is a significant scale of breach (involving 500 or more individuals). As the public consultation is still underway at the time of writing, there are no guidelines on the nature and scope of information needed to be reported. It is proposed that certain exemptions should apply to the notification requirement to affected individuals; for example, if notification is likely to impede law enforcement investigations, or where the breached personal data is encrypted to a reasonable standard.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses do not change, provided that any PDPA requirements are complied with if the information includes personal data.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

Regulators responsible for enforcing requirements are generally either sector-specific or subject-matter specific, including but not limited to:

Sector/Subject Matter	Relevant Statute/ Regulations	Regulators
Cybersecurity	CMCA	MCI, CSA
Personal Data	PDPA	PDPC
Penal Offences	Penal Code	Singapore Police Force ("**SPF**")
Sector-Specific Regulations	Banking and Financial Sector Laws/Notices/ Guidelines	Monetary Authority of Singapore ("**MAS**")
	Telecommunications Act	Infocomm Media Development Authority ("**IMDA**")

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Penalties for failure to comply with any of the abovementioned requirements are dependent upon the respective statutes, regulations or guidelines, for example:

- The PDPC has powers to issue directions and bring enforcement actions to ensure compliance with the PDPA. For example, the PDPC can impose a financial penalty of up to S$1 million.
- Under section 15A of the CMCA, a person who fails to take any measure or comply with any requirement directed by the Minister shall be guilty of an offence and shall 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.

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

The PDPC has taken an active role in ensuring action be taken against organisations which breach the PDPA. By way of example, on 21 April 2016, the PDPC imposed financial penalties of S$50,000 and S$10,000 on K Box Entertainment Group ("**K Box**") and its data intermediary, Finantech Holdings, for failing to implement proper and adequate protective measures to secure its IT system, resulting in unauthorised disclosure of the personal data of 317,000 K Box members. K Box was also issued directions and penalised for the absence of a Data Protection Officer.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Apart from the PDPA requirement for all organisations to make reasonable security arrangements to protect personal data, other cybersecurity obligations and requirements are imposed in sector-specific legislation, codes of practice, and guidelines, such that information security measures vary depending on business sector.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Financial Services Sector:

Under the Technology Risk Management Notices, regulated financial institutions are required to notify the MAS as soon as possible, but not later than one hour, upon the discovery of a relevant Incident. Regulated financial institutions are required to submit a root cause and impact analysis report to the MAS, within 14 days or such longer period as the MAS may allow, from the discovery of the relevant Incident.

A "relevant incident" refers to a system malfunction or IT security Incident, which has a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers.

The MAS has also issued guidelines for financial institutions to mitigate cybersecurity risks, such as the Technology Risk Management Guidelines, Outsourcing Guidelines, Business Continuity Management Guidelines, and Bring-Your-Own-Device ("**BYOD**") Circular.

Telecommunications Sector:

The IMDA has formulated the Telecommunication Cybersecurity Code of Practice to enhance the cybersecurity preparedness for designated licensees. Besides security Incident management requirements, the Code includes requirements to prevent, protect, detect and respond to cybersecurity threats.

4 Corporate Governance

4.1 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' duties in your jurisdiction?

Failure by a company to prevent, mitigate, manage or respond to an Incident could amount to breach of directors' duties; for example, if the failure results from a director's breach of their duty to act honestly and use reasonable diligence in the discharge of the duties of their office.

While not mandatory, the Code of Corporate Governance ("**Code**") sets out best practices in relation to corporate governance principles. The Code of Corporate Governance is issued by the MAS, on recommendation by the Corporate Governance Council, and was last revised on 2 May 2012. Under Principle 11 "Risk Management and Internal Controls", the board of directors should determine the company's levels of risk tolerance and risk policies, and oversee management in the design, implementation and monitoring of the risk management and internal control systems (including financial, operational, compliance and information technology controls).

In relation to financial institutions, the MAS has issued the Technology Risk Management Guidelines, which set out technology risk management best practices and recommend that, in view of the importance of the IT function in supporting a financial institution's business, the board of directors and senior management should have oversight of technology risks and ensure that the organisation's IT function is capable of supporting its business strategies and objectives. The board of directors and senior management should ensure that a sound and robust technology risk management framework is established and maintained. They should also be fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (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?

There is currently no general requirement under Applicable Laws for all companies to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments; and (d) perform penetration tests or vulnerability assessments.

Nevertheless, there are sector-specific cybersecurity requirements. For example, in relation to financial institutions, the MAS Technology

Risk Management Guidelines recommend that financial institutions devise an Incident response framework, perform risk assessments, as well as penetration tests and vulnerability assessments. The MAS Outsourcing Guidelines recommend that financial institutions conduct periodic risk assessments on outsourced service providers, and review and monitor the security practices and control processes of the outsourced service providers on a regular basis.

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

Companies are currently not subject to specific disclosure requirements in relation to cybersecurity risks or Incidents (whether to listing authorities, the market or otherwise in their annual reports).

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

Companies may be subject to specific cybersecurity requirements under sector-specific codes or guidelines, such as those set out in section 3 above.

5 Litigation

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

An Incident could give rise to claims in contract (for breach of contract) or tort (as set out under question 5.3 below).

The PDPA provides for a right of private action, whereby any person who suffers loss or damage directly as a result of a contravention of certain Data Protection Provisions by an organisation shall have a right of action for relief in civil proceedings in a court. In such a private action, the court may grant the plaintiff all or any of the following: (a) relief by way of injunction or declaration; (b) damages; and/or (c) such other relief as the court thinks fit.

Under the CMCA, the court may order a person convicted of a CMCA offence to pay compensation to any victim of the offence. This order will not prejudice the victim's right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

There have not been reported cases directly relating to civil actions brought in relation to Incidents.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A party may face potential liability in tort in relation to an Incident; for example: if the Incident results from the party's negligence; there is a breach of confidence; or there is a breach of statutory duties.

6 Insurance

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

Yes. Organisations are permitted to take out insurance against Incidents. Often known as 'cyber insurance', such insurance may cover business interruption loss due to network security failure or attack, human errors, or programming errors, among others.

As this type of insurance is relatively novel in Singapore, it has been reported that the MAS and CSA have been working with industry partners and a Singapore university to research on cyber risk, security and insurance, so as to develop insurance schemes to protect citizens and businesses against cyber attacks.

6.2 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?

Currently, there are no regulatory limitations to insurance coverage against the specified losses, such as business interruption, system failures, cyber extortion or digital asset restoration.

Notwithstanding the above, the general rule of *ex turpi causa non oritur actio* applies to insurance contracts as it applies to contractual illegality. A person cannot rely on his own illegal act to make a claim against his insurance policy, nor benefit from his own criminal conduct. This is also contrary to public policy, since allowing the indemnification of such risks would be to encourage the commission of crimes, which would be wholly against public policy.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

(a) Generally, the Applicable Law does not impose specific requirements on employers to monitor employees for the purposes of preventing, detecting, mitigating and responding to Incidents.

In relation to financial institutions, the MAS Technology Risk Management Guidelines recommend that, for accountability and identification of unauthorised access, financial institutions should ensure that records of user access are uniquely identified and logged for audit and review purposes. The MAS recommends that financial institutions should closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures.

In the non-binding Advisory Guidelines issued by the PDPC, which provide examples of security arrangements to protect personal data, the PDPC recommends restricting employee access to confidential documents on a need-to-know basis.

(b) There are no requirements under Applicable Law regarding the reporting of Incidents or potential Incidents by employees to their employers. However, it is to be noted that under

the employment contracts or internal company policies, there may be such notification requirements imposed upon employees.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

There are currently no Applicable Laws which may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee.

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.

CMCA: computer misuse offences are investigated by the SPF. More specifically, within SPF's Criminal Investigation Department, the Technology Crime Division conducts investigation and forensic examination into technology-related offences committed under the CMCA. The SPF's powers of investigation are set out under the Criminal Procedure Code (Cap. 63) ("**CPC**").

PDPA: the PDPC can initiate investigations upon complaint or its own motion. It has the power to require relevant documents or information, and the power to enter premises without warrant as well as under warrant.

Internal Security Act ("**ISA**"): in the interest of Singapore's national security, the ISA provides for the Government's power to order preventive detention, and the power of police to search and seize subversive documents, among other powers.

Cybersecurity Bill: the draft Bill proposes to provide investigative powers to the Cybersecurity Commissioner (or any other cybersecurity officer upon his authorisation), and to exercise powers necessary to determine the impact or potential impact of the cybersecurity threat or Incident.

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?

Under section 40(2) of the CPC, for the purposes of investigating an arrestable offence, the Public Prosecutor may by order authorise a police officer or an authorised person to 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. Failure to comply is an offence punishable by a fine not exceeding S$10,000 or to imprisonment for a term not exceeding three years or to both.

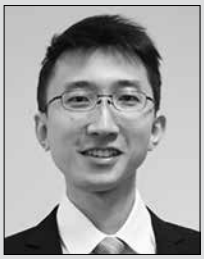
Under section 15A of the CMCA, the Minister for Communications and Information has the power to issue directions to any person or organisation to take such measures, such as the exercise of powers referred to under section 40(2) of the CPC to require decryption information, as may be necessary to prevent, detect or counter cyber threats to national security, essential services, defence, or foreign relations of Singapore.

Rajesh Sreenivasan
Rajah & Tann Singapore LLP
9 Battery Road #25-01
Singapore 049910
Singapore

Tel: +65 6232 0751
Email: rajesh@rajahtann.com
URL: sg.rajahtannasia.com

Rajesh Sreenivasan heads the Technology Media and Telecommunications Practice at Rajah & Tann Singapore LLP. He has been advising clients on matters relating to cybersecurity, data protection, telecommunications, electronic commerce, IT contracts, digital forensics and digital media for over 20 years.

His clients include financial institutions, state governments, multinational corporations in the telecoms, computer hardware and software sectors, government-linked companies and statutory boards. On the regional front, Rajesh has been engaged by the ASEAN Secretariat to facilitate a pan-ASEAN forum on legislative and regulatory reforms to collectively address convergence of IT, telecoms and broadcasting across all 10 member countries, and by the Commonwealth Secretariat to co-lead an e-government capacity building exercise involving all member Caribbean nations. Rajesh is also the contributing author for the Singapore chapter of Sweet & Maxwell's *Data Protection Laws of the World* since 2010. Rajesh has been cited as a leading TMT lawyer by all major legal ranking directories.



Michael Chen
Rajah & Tann Singapore LLP
9 Battery Road #25-01
Singapore 049910
Singapore

Tel: +65 6232 0780
Email: michael.chen@rajahtann.com
URL: sg.rajahtannasia.com

Michael Chen is an Associate in the Technology Media and Telecommunications Practice at Rajah & Tann Singapore LLP. He has assisted in an extensive range of intellectual property, technology, media, and data protection matters. He actively advises on a wide range of technology contracts.

He graduated from the University of Melbourne Law School and is admitted in both Singapore and Australia. Michael has a keen interest in computers and technology, and also holds a degree in electrical and computer engineering from Cornell University.

Rajah & Tann Singapore LLP has grown to be one of the largest full-service law firms in Singapore, providing full service and high-quality advice to an impressive list of clients. We have more than 300 lawyers, many ranked among the very best in their specialist practice areas.

Our Technology, Media and Telecommunications ("**TMT**") Practice is at the forefront of the TMT sector as thought leaders and trusted legal advisors for major TMT organisations and regulatory bodies in the Asia Pacific region and beyond. Led by a team of Partners who have been universally commended as the best of breed in TMT and ably supported by a team of specialist Associates, we are ready to help our clients navigate through this dynamic and constantly evolving area of practice.

Cybersecurity is a key area of concern for all clients, and safeguarding clients' trust and ensuring confidentiality of sensitive data is a vital task for many of our clients. In this respect, our broad suite of cybersecurity services, which includes multi-disciplinary data breach services and 24-hour emergency response teams, stand ready to assist our clients as may be required.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com