ICLG

The International Comparative Legal Guide to:

# Cybersecurity 2019

## 2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

**Contributing Editors**
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

**Sales Director**
Florjan Osmani

**Account Director**
Oliver Smith

**Sales Support Manager**
Toni Hayward

**Editor**
Sam Friend

**Senior Editors**
Suzie Levy
Caroline Collingwood

**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 2018



**ISBN** 978-1-912509-38-6
**ISSN** 2515-4206

**Strategic Partners**

## General Chapters:



## Country Question and Answer Chapters:

# Malaysia

Deepak Pillai

Christopher & Lee Ong

Yong Shih Han

## 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:**

**Hacking (i.e. unauthorised access)**

Yes. Under section 3 of the Computer Crimes Act 1997 ("**CCA**"), it is an offence if a person knowingly and intentionally accesses a computer without authorisation and causes a computer to perform any function with the intent to secure access to any program or data held in any computer.

A person found guilty of an offence under section 3 is liable to a fine not exceeding RM50,000 or imprisonment not exceeding five years or both.

In *PP v Vishnu Devarajan* [2016] 1 LNS 1066, the accused was charged under section 3 of the CCA for accessing without authorisation the servers of a broadcast centre and the server database of a Malaysian radio network company. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

Section 4 of the CCA creates a further offence against persons who commit a hacking offence under section 3 with the intent to: (i) commit an offence involving fraud or dishonesty which causes injury under the Malaysian Penal Code (the main penal statute in Malaysia) (the "**Penal Code**"); or (ii) facilitate the commission of such an offence whether by himself or any other person. A person found guilty under section 4 is liable to a fine not exceeding RM150,000, or imprisonment not exceeding 10 years, or both.

In *Basheer Ahmad Maula Sahul Hameed v PP* [2016] 6 CLJ 422, the two accused persons, who were husband and wife, where the wife worked in a bank, were convicted under section 4(1) of the CCA for using a debit card belonging to an airplane accident victim to withdraw cash from an ATM machine and for transferring money from several other victims' online banking accounts without authorisation.

**Denial-of-service attacks**

There is no specific provision which provides for denial-of-service attacks. However, under section 233(1)(b) of the Communications and Multimedia Act 1998 ("**CMA**"), a person who continuously, repeatedly or otherwise initiates a communication using any applications services with the intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence, regardless of whether the communication ensued and whether or not the person initiating such communication disclosed their identity.

A person found guilty of an offence under section 233(1)(b) is liable to a fine not exceeding RM50,000, or imprisonment not exceeding one year, or both, and shall also be liable to a further fine of RM1,000 for every day that the offence is continued after conviction.

To date, there have been no reported cases under section 233(1)(b) of the CMA.

**Phishing**

There are no specific offences with regard to phishing. However, other statutory provisions may be applicable in tackling phishing offences.

Under section 416 of the Malaysian Penal Code, any person is said to "cheat by personation", 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. The offence of cheating by personation is punishable with imprisonment for a term which may extend to seven years and/or a fine.

To date, there are no reported cases specifically in relation to phishing.

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

Infection of IT systems with malware is an offence punishable under the CCA. Under section 5 of the CCA, it is an offence for a person to do any act which he knows will cause unauthorised modification of the contents of any computer.

A person found guilty of an offence under section 5 is liable to a fine not exceeding RM100,000 or imprisonment not exceeding 10 years, or both if the act was done with the intention of causing injury.

In *PP v Roslan and Anor* [2016] 1 LNS 651, the accused who worked as a Systems Analyst in the IT Department of the Malaysian Hajj Pilgrims Fund Board, was convicted under section 5(1) of the CCA for modifying pilgrims' records in the organisation's database without authorisation.

In *PP v Vishnu Devarajan* [2016] 1 LNS 1066, the accused was charged under section 5 of the CCA for, amongst others, carrying out the following without authorisation: downloading and launching software; running and stopping certain processes on servers; and running certain programs on the database server of a broadcast centre. However, all charges were dropped due to technical and procedural errors in the prosecution of the case.

In *Kangaie Agilan Jammany v PP* [2017] 1 LNS 1640, the accused, an employee of AirAsia, a low-cost airline carrier company, was charged under section 5 of the CCA where he used the Air Asia reservation system without authorisation to modify passenger flight

schedules, in order to help family members and friends obtain airline tickets at lower rates.

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

Under section 236 of the CMA, it is an offence for a person to possess or use any counterfeit access devices, unauthorised access devices (e.g. lost, stolen, expired, or obtained with the intention to defraud), any device-making equipment intended to make counterfeit access devices, or any other equipment or device modified or altered or intended to alter or modify such other equipment or device in order to obtain unauthorised access to any network services, etc.

Possession or use of the above is an offence and the offender would be liable to a fine not exceeding RM500,000 or to imprisonment not exceeding five years, or both.

Under section 240 of the CMA, it is an offence to distribute or advertise any communications equipment or device for interception of communication. An offence under this section would render the offender liable to a fine not exceeding RM100,000 or to imprisonment not exceeding two years, or both.

To date, there have been no reported cases under either section 236 or section 240 of the CMA.

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

The Penal Code contains provisions on cheating by personation. Although not cyber-specific, section 416 of the Penal Code (as discussed above) may apply to identity theft. Under section 416 of the Penal Code, it is an offence to "cheat by personation", i.e. where a person 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 person really is.

To date, while there has been news of individuals committing identity theft or fraud, such cases have, however, usually been tried on the basis of contravening national registration regulations (in relation to impersonating or theft of identification cards). There have been no reported cases for actions on identity theft or identity fraud specifically in the context of cybersecurity or cybercrimes.

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

Under Malaysian law, the right to bring an action for breach of confidence stems from common law, or pursuant to the contracts of employment, which generally contain confidentiality clauses and as such would not constitute a criminal offence.

Copyright owners have the right to bring an action for copyright infringement either as a civil or criminal offence. Section 41 of the Copyright Act 1987 sets out a range of offences for copyright infringement, which include making for sale or hire, distributing, and exhibiting in public any infringing copy during the subsistence of copyright in a work or performers' right.

In *Chuah Gim Seng & More Again v. SO* [2009] 10 CLJ 65, the appellants were found guilty and convicted for the sale of pirated copy films. The penalty imposed was RM2,000 for the sale of each copy and in default a four-month jail term for failure to pay each charge.

In *PP v. Haw Swee Po* [2011] 5 LNS 23, the accused was tried for possession and use (other than for private and domestic use) of 3,300 copies of seven films in DVD format. The court sentenced the accused to 14 months' imprisonment.

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

Activities which adversely affect or threaten security, confidentiality, integrity or availability of IT systems, infrastructures, etc. are prohibited or regulated under the CMA. For example, it is an offence to: use any apparatus or device with the intent to obtain information regarding the contents, sender or addressee of any communication without an approval by a registered certifying agency (section 231 of the CMA); possess or create a system designed to fraudulently use or obtain any network facilities, network service, applications service or content applications service (section 232(2) of the CMA); intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept, any communications (section 234 of the CMA); and extend, tamper with, adjust, alter, remove, destroy or damage any network facilities or any part thereof (section 235 of the CMA).

A person who is found liable for any of the above offences under CMA may, upon conviction, be held liable to a maximum fine ranging from RM50,000 to RM300,000 or imprisonment not exceeding two to three years, or both.

In relation to personal data, organisations are required to ensure the security of individuals' personal data (section 9 of the Personal Data Protection Act 2010, the "**PDPA**"), and in this regard are required to comply with the minimum security standards prescribed by the Personal Data Protection Standards 2015 (the "**PDP Standards**"). Non-compliance with section 9 of the PDPA may hold the offender liable to a fine not exceeding RM100,000 or imprisonment not exceeding two years, or both, whereas non-compliance with any of the security standards under the PDP Standards may result in the offender being held liable to a fine not exceeding RM250,000 or imprisonment not exceeding two years, or both.

To date, there have been no reported cases prosecuted under any of the abovementioned provisions of the CMA or PDPA.

**Failure by an organisation to implement cybersecurity measures**

There is currently no legislation which imposes a blanket requirement in respect of implementing cybersecurity measures. The closest is the PDPA, which only applies to organisations involved in commercial transactions and expressly excludes the Government of Malaysia.

Organisations that are involved in processing personal data are required to implement minimum security standards as prescribed by the PDP Standards, or such other standards as prescribed by the Personal Data Protection Commissioner (the "**PDP Commissioner**") from time to time.

Certain sectors are additionally subject to the guidelines requiring the implementation of certain cybersecurity measures, for example:

(a) in the capital market industry, capital market entities are subject to cybersecurity requirements as set out in the *Guidelines on Management of Cyber Risk* issued by the Securities Commission of Malaysia ("**SC**"); and

(b) in the banking and financial sector, banks and financial institutions are subject to the requirements as set out in the *Guidelines on Management of IT Environment (GPIS 1)* issued by the Central Bank of Malaysia or Bank Negara Malaysia ("**BNM**").

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

Yes. The CCA, CMA, and to a certain extent, the Penal Code (in relation to terrorism and offences against the state) have extraterritorial application.

### 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?

For organisations that are subject to cybersecurity obligations or requirements (e.g. PDPA, sector-specific cybersecurity requirements),

there are no specific actions specified in the statutes or guidelines which might mitigate the penalty which would otherwise be incurred by reason of any breach or non-compliance by the organisation. However, it is reasonable to infer that cooperation with the relevant regulators or enforcement authorities, or active steps taken to mitigate the loss or damage caused by any of the offences, may serve to mitigate the severity of the penalty to be imposed by the regulators or enforcement authorities.

**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.**

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, or participation or indication of support to terrorist groups or activities (section 130J of the Penal Code).

In the context of cyberterrorism, sub-section (2)(k) of section 130J specifically provides that "support" to a terrorist group extends to the act of "using social media or any other means to:

(i) advocate for or to promote a terrorist group, support for a terrorist group or the commission of a terrorist act; or

(ii) further or facilitate the activities of a terrorist group".

While Malaysian enforcement authorities have regularly taken steps to block or remove known terrorist websites, there have been no reported cases in respect of cyberterrorism under the abovementioned section 130J(2)(k) of the Penal Code.

## 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.**

As at the time of writing, there is no single piece of legislation in Malaysia in respect of cybersecurity. In June 2017, the then Malaysian Home Minister, Ahmad Zahid Hamidi, announced that a new cybersecurity bill will be drafted and tabled in Parliament, in order to combat cybercrimes, including recruitment and financial sourcing by terrorist groups, money laundering and online gambling. However, the cybersecurity bill has not been tabled in Parliament to date.

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

**Communications and Multimedia Act 1998 (CMA)**

The CMA provides for and regulates the converging areas of communications and multimedia. In particular, the CMA regulates various activities carried out by licensees (i.e. network facilities providers, network service providers, applications service providers and content applications service providers) as well as those utilising the services provided by the licensees. One of the objects of the CMA is to ensure information security and network reliability and integrity in Malaysia. The CMA: requires licensees to use their best endeavours to prevent network facilities or network services from being used for the commission of any offence under Malaysian laws; prohibits fraudulent or improper use of network facilities or network services; prohibits the use and possession of counterfeit access devices; prohibits use of equipment or device in order to obtain unauthorised access to any network services; and prohibits interception of any communications unless with lawful authority.

**Computer Crimes Act 1997 (CCA)**

The CCA criminalises: the act of gaining unauthorised access into computers or networks; spreading malicious codes (e.g. viruses, worms and Trojan horses); unauthorised modification of any program or data on a computer; as well as wrongful communication of any means of access to a computer to an unauthorised person. Depending on the type of offence committed, the fine for a convicted offence ranges from RM25,000 to RM150,000 or imprisonment of three to 10 years or both. The case *Basheer Ahmad Maula Sahul Hameed v PP* [2016] 6 CLJ 422 (as discussed in 'Hacking' in question 1.1 above) is an example of an offence under CCA.

**Penal Code**

In cases where computer-/Internet-related crime activities are involved, but do not specifically fall within the ambit of any of the aforementioned statutes (for example, online fraud, cheating, criminal defamation, intimidation, gambling, pornography, etc.), such offences may be charged under the Penal Code, which is the main statute that deals with a wide range of criminal offences and procedures in Malaysia.

**Personal Data Protection Act 2010 (PDPA)**

The PDPA regulates the processing of personal data in commercial transactions and applies to anyone who processes and has control over or authorises the processing of any personal data in respect of commercial transactions.

The most relevant PDPA principle in the context of cybersecurity would be the Security Principle, i.e. appropriate technical and organisational security measures must be taken to prevent unauthorised or unlawful processing of personal data and accidental loss, misuse, modification or unauthorised disclosure of personal data.

The PDP Commissioner has also issued subsidiary legislation pursuant to the PDPA, among which are the Personal Data Protection Regulations 2013 (the "**Regulations**") and the Personal Data Protection Standard 2015 (the PDP Standards), which provide specific requirements regarding security standards expected of data users.

**Copyright Act 1987 ("Copyright Act")**

The Copyright Act generally protects copyrights, including trade secrets, intellectual property in devices or data, etc. Where any technological protection measure is applied to any copyright, it is an offence under the Copyright Act to circumvent such technological protection measures (section 36A of the Copyright Act). No person shall offer such technology or device which allows for circumvention of such technological protection measures, and non-compliance with the provision would be an offence and the person guilty of the offence may be held liable to a fine not exceeding RM 250,000 or to imprisonment for a term not exceeding five years, or to both; and for any subsequent offence, to a fine not exceeding RM 500,000 or to imprisonment for a term not exceeding 10 years, or to both.

**Strategic Trade Act 2010 ("Strategic Trade Act")**

The Strategic Trade Act 2010 is the legislation that controls the export, trans-shipment, transit and brokering of strategic items and technology, as well as activities that will or may facilitate the design, development, production and delivery of weapons of mass destruction. The Strategic Trade Act, which is consistent with Malaysia's international obligations on national security, prohibits the import or export of strategic items, including items deemed as 'strategic technology' (i.e. controlled items as determined by the Minister of International Trade and Industry in Malaysia, such as encryption technology) (section 9 of the Strategic Trade Act).

**2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.**

The Malaysian Government, under the National Cyber Security Policy ("**NCSP**") has identified 10 critical sectors in Malaysia, known as the Critical National Information Infrastructure ("**CNII**"), which are required to be protected to a level commensurate with the risks faced. These CNII sectors are:

(1) National Defence and Security.
(2) Banking and Finance.
(3) Information and Communications.
(4) Energy.
(5) Transportation.
(6) Water.
(7) Health Services.
(8) Government.
(9) Emergency Services.
(10) Food and Agriculture.

While there are no minimum protective measures in general and across sectors to protect data and information technology systems from Incidents (save for security requirements in relation to personal data under the PDPA), the government of Malaysia has stipulated *ISO/IEC 27001 Information Security Management Systems* ("**ISMS**") as the baseline standard for information security and has proposed for all CNII sectors (as listed above) to be ISMS-certified. Such standards have been incorporated in certain sector-specific guidelines/handbooks. Penalties for failure to undertake such protective measures would be as prescribed by the respective standards/guidelines.

**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.**

The PDPA regulates processing of personal data in the context of commercial transactions, including for the purpose of ensuring security of such data. Under the Regulations, organisations that process personal data (i.e. data users under the PDPA) are required to develop a security policy to ensure that personal data is protected from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Further to the above, the PDP Standards prescribe a list of minimum security standards to be complied with by the data users (e.g. prohibition of the use of removable media devices or cloud computing services for transfer or storage of personal data, unless with written authorisation from the top management of the organisation; ensuring the organisation's backup/recovery system and anti-virus software are regularly updated to protect personal data from data intrusion or security breach; contractually binding third-party data processors in respect of data processing activities, etc.).

From the perspective of the CMA in turn, section 263 requires all network facilities or network service providers to use their best endeavours to prevent network facilities or network services, applications services or content applications services from being used in, or in relation to, the commission of any offence under any law of Malaysia.

Apart from the above, several sector-specific standards and guidelines also require organisations to apply security measures. Some examples of these are *Guidelines on Internet Insurance for the Insurance Sector*, *BNM Guidelines on the Provision of Electronic Banking (e-banking) Services*, the *BNM Guidelines on Data Management and Management Information System (MIS) Framework for the Banking Sector* and the Securities Commission Malaysia's *Guidelines on Management of Cyber Risk*. These standards and guidelines will be further discussed below.

**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 arisen thus far in Malaysia.

**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.**

There are currently no applicable laws in Malaysia that generally require organisations to report information related to Incidents or potential Incidents to a regulatory or other authority.

However, in August 2018, the PDP Commissioner published the Public Consultation Paper (No. 1/2018) entitled "The Implementation of Data Breach Notification" (the "**DBN Public Consultation Paper**") which would be applicable to organisations who are required to register under the PDPA and who process personal data or have control over or authorise the processing of any personal data (i.e. registered data users under the PDPA).

Pursuant to the DBN Public Consultation Paper, the PDP Commissioner intends to implement a data breach notification mechanism ("**DBN**") in Malaysia, where data users are required to notify and inform the relevant authorities and affected parties when a data breach has occurred within the organisation. Organisations will be required to report on:

(i) details about the Incident, (i.e. summary of the event and circumstances, type and amount of personal data involved in the Incident and the estimated number of affected individuals);
(ii) the organisation's containment or control measures (i.e. details of actions/measures taken or to be taken to contain the breach and the potential harm of the breach, especially to the affected individuals);
(iii) details and requirements with regards to notification (i.e. identification of the persons who have been notified about the breach, details whether any regulatory bodies/law enforcement agencies have been notified about the breach, the method(s) used by the organisation to notify the affected individual about the Incident, any advice given to the affected individual, the requirement for the PDP Commissioner to be notified no later than 72 hours after having become aware of the breach); and

(iv) details on the organisations' training and guidance in relation to data protection (i.e. whether the organisation had provided training/awareness programmes to staff members prior to the Incident, whether the staff members involved in the Incident had received training in the last 24 months and whether the organisation had provided any detailed guidance to staff on the handling of personal data in relation to the reported Incident).

The DBN Public Consultation Paper in its current draft form merely provides that data users are to report to the authority and the affected/relevant parties where a breach has occurred in an organisation. However, the PDP Commissioner has not clarified the scope of such "breach" nor identified the events which would trigger reporting obligations, and whether any defences or exemptions exist by which the data subject might prevent publication of that information.

The DBN Public Consultation Paper is expected to come into force by the end of 2018.

Certain sector-specific guidelines have been issued imposing such requirements. Some examples are as follows:

- **Banking Sector:** *BNM's Guidelines on Management of IT Environment* ("**GPIS 1**") outline the minimum responsibilities and requirements for mitigating risks pertaining to the IT environment.

  Under the Guidelines, banks are required to report to BNM on any serious security breaches, system down-time and degradation in system performance that critically affects the bank/financial institution, immediately upon detection by providing "initial information/observation" and the subsequent formal report within two days; and
- **Capital Market:** *Securities Commission Malaysia's Guidelines on Management of Cyber Risk* sets out the roles and responsibilities of capital market entities, policies and procedures that should be developed and implemented, requirements for managing cyber risk and reporting requirements to the Securities Commission Malaysia. Under the said Guidelines, the capital market entities must report to the Securities Commission Malaysia on any detection of a cyber Incident impacting the entity's information assets or systems, on the same day of the Incident. The entities are also required to report any cyber breaches to the board of directors and periodically update the board on emerging cyber threats and their potential impact on the entity.

**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. Additionally, where the information involves personal data, the organisation needs to make sure that the disclosure of the said personal data must fall within the exceptions under the PDPA.

**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.**

There are currently no general requirements under Applicable Laws for organisations to report information relating to Incidents or potential Incidents to affected individuals. Notwithstanding the foregoing, the DBN Public Consultation Paper (which is currently in the public consultation stage, and pending formal issuance as discussed in question 2.5 above) requires organisations to provide information in relation to:

(i) details of actions/measures taken or to be taken to contain the breach;

(ii) advice given to the affected individual; and

(iii) the potential harm of the breach on the affected individuals and the method(s) used by the organisation to notify affected individuals about the Incident.

Apart from the general requirement for data users to report on data breach events, the DBN Public Consultation Paper has not specified the circumstances (i.e. what constitutes a "data breach") in which this reporting obligation is triggered.

Further to the above, certain sector-specific guidelines require the applicable organisations to implement policies or procedures to inform the relevant stakeholders of the Incident (e.g. the *SC Guidelines on Management of Cyber Risk* requires the relevant entity to implement communication procedures that will be activated by the entity in the event of a cyber breach, which include reporting procedures, information to be reported, communication channels, list of internal and external stakeholders and a communication timeline).

**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, they do not.

**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 | Regulator |
|---|---|---|
| Information Security/Network Reliability and Integrity | Communications and Multimedia Act 1998 | Malaysian Communications and Multimedia Commission (MCMC) |
| Personal Data | Personal Data Protection Act 2010 | Personal Data Protection Department/ Commissioner's Office |
| Penal Offences | Penal Code, Computer Crimes Act 1997 | Royal Malaysian Police |
| Sector-Specific Regulations | Banking and Financial Sector Guidelines | Central Bank of Malaysia or Bank Negara Malaysia (BNM) |
| | Securities Commission Guidelines | Securities Commission Malaysia (SC) |

**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:

- non-compliance with the PDPA may result in the organisation, upon conviction, to be liable to a maximum fine ranging from RM100,000 to RM500,000 or imprisonment ranging from one to three years, or both;
- non-compliance with the provisions under the CMA may result in the organisation, upon conviction, to be liable to a maximum fine ranging from RM50,000 to RM500,000 or imprisonment ranging from one to five years, or both;
- contravention of the provisions under the CCA or Penal Code would subject the organisation to enforcement by the Royal Malaysian Police, and may expose the organisation to liability involving a fine ranging from RM25,000 to RM150,000 or imprisonment of three to 10 years or both; or
- non-compliance with the relevant sector-specific guidelines may expose the organisation to enforcement actions by the relevant regulators (e.g. BNM or the SC), and may subject the organisation to regulatory sanctions such as a warning, public or private reprimands, an order to mitigate remedy the non-compliance, or even imposition of a monetary penalty. In cases involving severe non-compliance, the regulators may commence prosecution against the organisation.

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

There are no reported cases in Malaysian law journals in relation to any non-compliance of the abovementioned requirements.

From the regulatory perspective, regulators may impose regulatory sanctions on their licensees. These regulatory sanctions may be issued either privately (e.g. BNM) or publicly (e.g. MCMC) by regulators, depending on the regulator.

A list of investigations and prosecutions is available on MCMC's official website.

## 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.**

As stated in questions 2.3 and 2.5 above, apart from the PDP Standards which prescribe a list of minimum security standards to be complied with by data users, cybersecurity obligations and requirements vary across different sectors and are imposed in sector-specific legislation, regulations, standards and/or guidelines.

**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**

Guidelines on Internet Insurance

The Guidelines state that an internet insurance system security arrangement should minimally achieve data privacy and confidentiality, data integrity, authentication, and non-repudiation and network and access controls. Insurers are required to put in place critical technologies and to have a thorough and documented security procedure in relation to the risk exposures and needs of its internet insurance, such as:

(a) the latest critical technologies available such as firewalls, intrusion detection systems, anti-virus or virus-protection, encryption, virtual private networks (VPNs), public key infrastructure (PKI) and payment protocols; and

(b) security procedures such as user IDs and passwords, time stamping, reconciliation of all transactions, segregation of roles and responsibilities, audit trails, and testing.

BNM Guidelines on the Provision of Electronic Banking (e-banking) Services

In the *Guidelines on E-Banking*, security standards to be applied are based on the risk management of different e-banking types. The Guidelines set out different minimum security standards for different types of banking services. For example, in transactional services which present the greatest risk in e-banking (as it links to the financial institutions' internal networks and computer systems that hold critical account information and other information assets), the Guidelines require utilisation of the highest level of protection including strong authentication and encrypted transmission of highly sensitive data.

Bank Negara Guidelines on Data Management and Management Information System (MIS) Framework

These Guidelines set out several principles and elaborate on the specific safeguards to be applied for each principle. Among the safeguards required are that banks/financial institutions are to obtain the MS ISO/IEC 27001 Information Security Management Systems (ISMS) certification for critical systems, particularly the payment and settlement systems, to ensure that safeguards and security measures implemented over data and IT systems are effective.

**Telecommunications sector**

There are currently no specific cybersecurity obligations imposed on licensees under the CMA. However, under section 263 of the CMA, the Commission or other authority, may make requests in writing to its licensees requesting the licensees to assist the Commission or any other authority, as far as reasonably necessary, in preventing the committing or attempted committing of an offence under any written law of Malaysia, or otherwise in enforcing the laws of Malaysia, including the protection of the public revenue and preservation of national security.

## 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 would potentially give rise to a breach of directors' duties.

In the event of any breach or non-compliance of statutory requirements by the organisation, the directors may also be held jointly or severally liable for such breach or non-compliance.

Under section 133 of the PDPA, it is expressly provided that the commission of any offence by the body corporate may also render the officers of the body corporate (e.g. directors, the chief executive officer, managers, etc., who were responsible for the management of the affairs of the body corporate) to be charged severally or jointly with the body corporate, and in such instances may also be found to have committed the offence.

Directors may also be found liable for such failure under the relevant sector-specific standards or guidelines. For example, in the banking

and financial sector, the *Guidelines on Data Management and MIS Framework* issued by BNM provide that senior management and the board of directors must play a key role in the development of a data management and management information system framework; and in capital markets sector, the *Guidelines on Management of Cyber Risk* issued by the SC set out the roles and responsibilities of the board of directors and management in the oversight and management of cyber risk. These provide that directors are subject to certain responsibilities and consequently may be held responsible for any non-compliance therewith.

**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 no general requirement under Malaysian laws for 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. Requirements are generally sector-specific and in accordance with the relevant standards or guidelines (e.g. *SC Guidelines on Management of Cyber Risk* requires cyber risk policies and procedures to be implemented by the organisation, and sets out the required contents of such policies and procedures as well as an Incident response template).

Notwithstanding the above, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that a training/awareness programme and detailed guidance should be given to the organisation's staff for handling such Incidents.

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

Disclosure requirements in relation to cybersecurity risks or Incidents are sector-specific. For example, the *Guidelines on Management of Cyber Risk*, issued by the Securities Commission Malaysia, requires capital market entities to develop and implement cyber risk policies and procedures, which must include the strategy and measures to manage cyber risk encompassing prevention, detection and recovery from a cyber breach.

Notwithstanding the above, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that notification of Incidents must also be made to other regulatory bodies/law enforcement agencies.

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

Apart from the Applicable Laws (as set out at question 2.1 above), companies would also be subject to specific requirements in relation to cybersecurity under the relevant sector-specific standards or guidelines.

## 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.**

In the event of an Incident, the company or organisation may be subject to civil actions on grounds of breach of contract or breach of statutory duties under the Applicable Laws (as set out at question 2.1 above).

In order to bring a claim on grounds of breach of contract, the claiming party must establish that there was a contractual duty in respect of cybersecurity (e.g. duty to protect confidential information or personal data), that there was a breach of such duty, and the loss or damage occasioned by such breach. A breach of statutory duty in itself would give rise to a right to commence civil action, although the quantum of damages would be dependent on the extent of loss or damage suffered by the claiming party. The company or organisation may also be liable under tort, as set out in question 5.3 below.

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

An example would be *Dynacraf Industries Sdn Bhd v Lee Kooi Khoon* [2008] 3 ILR 265, where an employer commenced action against a dismissed employee for alleged unauthorised interception and disclosure of electronic communication (in this case, another employee's private emails), in contravention with section 234 of the CMA (interception of communication). Apart from the foregoing, civil actions on grounds of copyright infringement, breach of confidence, have been brought in Malaysian courts.

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

In the event of an Incident, the company or organisation may also potentially be exposed to tortious liability on grounds of negligence, as the aggrieved party may allege loss or damage as a result of the company's or organisation's breach of duty of care in relation to cybersecurity.

## 6 Insurance

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

Yes, organisations are permitted to take out cyber risk insurance against Incidents in Malaysia. Cyber risk insurance may either be first party coverage (i.e. to insure against loss and damage sustained by the insured, i.e. the organisation itself) or third-party coverage (i.e. to insure against liability for loss, damage or personal injury caused to a third person, namely the customers or clients of the organisation).

**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?**

There are no known regulatory limitations in respect of cyber risk insurance coverage. However, risk exposure due to the company's

or organisation's own negligence or wilful default will likely be excluded by the insurer from the scope of insurance policy coverage.

## 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?**

There are no specific requirements under the Applicable Laws requiring monitoring of employees and for the employees to be under an obligation to report cyber risks, security flaws, Incidents, etc. to the employer. However, sector-specific guidelines may prescribe that employees be made aware of and understand the cyber risk policies procedures, the possible impact of cyber threats, as well as their roles in managing such threats (*Guidelines on Management of Cyber Risk*, issued by the Securities Commission Malaysia).

Additionally, the DBN Public Consultation Paper (which, as described in question 2.5 above, is still in the public consultation stage and pending official issuance by the PDP Commissioner) provides in general that a training/awareness programme and detailed guidance should be given to the organisation's staff for handling such Incidents.

**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 no known Applicable Laws that may prohibit or limit the reporting of cyber risks, security flaws, Incidents by an employee, etc. In fact, the Whistleblower Protection Act 2010 ("**WPA**") was passed to encourage and facilitate the disclosures of improper conduct of companies or organisations by protecting the informants making such disclosures. It is further provided under section 6(5) of the WPA that any provision in any contract of employment which purports to preclude the employee from making a disclosure of improper conduct shall be to that extent void.

## 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.**

The Royal Malaysian Police, the MCMC and other relevant regulatory authorities are granted wide investigatory powers under the relevant statutes (as set out in question 2.9 above).

In general, the law enforcement or regulatory authorities are authorised under the relevant statutes to exercise the following investigatory powers during an investigation:

- the power to investigate the relevant persons;
- search and seizure, by warrant or without warrant;
- request for access to computerised data;
- the power to intercept communications;
- the power to require the production of records, accounts, computerised data, documents, etc., and to make such inquiry as may be necessary to ascertain if the relevant statutory provisions have been complied with;
- the power to require attendance of persons acquainted with the case;
- examination of persons acquainted with the case; and
- the power to institute prosecution, with consent in writing of the Public Prosecutor.

**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?**

While there are no legal requirements under the Applicable Laws for organisations to implement backdoors in IT systems specifically for law enforcement authorities, several cybersecurity-related statutes provide the need for law enforcement authorities to be provided with the relevant encryption keys, passwords, decryption codes, software or hardware or any other means required in order to have access to computerised data during the course of investigations (section 249 of the CMA; section 10 of the CCA).

**Deepak Pillai**
Christopher & Lee Ong
Level 22 Axiata Tower
No. 9 Jalan Stesen, Sentral 5
Kuala Lumpur Sentral, 50470
Kuala Lumpur
Malaysia

*Tel:* +603 2267 2675
*Email:* deepak.pillai@christopherleeong.com
*URL:* www.christopherleeong.com

Deepak has practised exclusively in the areas of Telecommunications & Technology law and Personal Data Protection for two decades and is acknowledged as a leading Telecommunications & Technology lawyer in Malaysia.

Deepak advises clients on matters relating to IT contracts, electronic commerce, online financial services, outsourcing, telecommunications, IT security, personal data protection and digital media. He advises a wide array of international, private and public sector clientele in addressing the commercial, regulatory and policy issues relating to information and communications technology law, ranging from negotiating complex information technology contracts to advising public sector agencies on proposed technology related legislation and policies.

Described in *The Legal 500* over the years as "*the most recognised IT specialist in Malaysia*", and "*pioneering the practice of IT law as a discrete area of law in Malaysia*".

Deepak has been listed by the *Asia Pacific Legal 500* as a leading individual in the area of IT and Telecommunications from 2001 to date.

**Yong Shih Han**
Christopher & Lee Ong
Level 22 Axiata Tower
No. 9 Jalan Stesen, Sentral 5
Kuala Lumpur Sentral, 50470
Kuala Lumpur
Malaysia

*Tel:* +603 2267 2715
*Email:* shih.han.yong@christopherleeong.com
*URL:* www.christopherleeong.com

Shih Han practices exclusively in the areas of Technology, Media and Telecommunications (TMT), and Data Protection. Prior to joining the firm, she was a dispute resolution associate in a reputable firm handling primarily civil and corporate litigation matters. Since joining the firm and making the transition to corporate practice, she has been involved in the areas of corporate commercial, mergers & acquisitions, and general corporate advisory. She currently focuses on the areas of technology, media, telecommunications and data protection, with information security and data protection being her specialised area.

She now regularly advises clients on matters relating to information and communications technology, information security and data protection, telecommunications, and media and advertising laws. This ranges from the preparation and drafting of technology-related contracts and policies to advising clients on matters potentially leading to dispute resolution. She also regularly advises clients on technology- and media-related regulatory and compliance matters.

CHRISTOPHER & LEE ONG

Christopher & Lee Ong ("CLO") is one of Malaysia's established and respected law firms, providing high-quality advice to clients across the commercial spectrum, with extensive experience in handling complex deals and disputes involving large local and multinational corporations, and governments and their agencies, as well as smaller local enterprises.

CLO's technology, media & telecommunications ("TMT") practice group is one of the most established and respected practices in the Asia Pacific region. With clients ranging from state governments and statutory boards to multinational corporations in the telecommunications, computer hardware and software sectors, the firm has been involved in many of the largest and most complex IT and telecommunications projects in recent years. The firm regularly advises clients on matters relating to IT contracts, electronic and mobile commerce, online financial services, outsourcing, telecommunications, cybersecurity, personal data protection, as well as regulatory and policy issues relating to information and communications technology law.

The firm's TMT practice group was recently awarded the *Technology, Media and Telecommunications Law Firm of the Year 2017* by *Asian Legal Business* at the Malaysian Law Awards 2017.

Other 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
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- 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
- 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