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:

Japan

Mori Hamada & Matsumoto

Hiromi Hayashi

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:

As background, there are two main laws criminalising cyber attacks, namely (A) the Act on the Prohibition of Unauthorized Computer Access (the "**UCAL**"), and (B) the Penal Code.

(A) The UCAL imposes criminal sanctions on any person who makes an Unauthorized Access to a computer (an "**Access Controlled Computer**"), the access to and operation of which are under the control of an administrator (the "**Access Administrator**").

An "**Unauthorized Access**" means any action which operates an Access Controlled Computer by either (i) inputting an identification code (*shikibetsu-fugou*) (e.g., password and ID) allocated to a user who is authorised to access the Access Controlled Computer (an "**Authorized User**"), without the permission of the Access Administrator or the Authorized User, or (ii) inputting any information (other than an identification code) or command which enables that person to evade control (e.g., cyber attack of a security flaw), without the permission of the Access Administrator (UCAL, Article 2, Paragraph 4).

The UCAL prohibits the following actions:

(a) an Unauthorized Access (Article 3);

(b) obtaining the identification code of an Authorized User to make an Unauthorized Access (Article 4);

(c) providing the identification code of an Authorized User to a third party other than the Access Administrator or the Authorized User (Article 5);

(d) keeping the identification code of an Authorized User which was obtained illegally to make an Unauthorized Access (Article 6); and

(e) committing the following acts by impersonating the Access Administrator or causing a false impression of being the Access Administrator: (a) setting up a website where the fake Access Administrator requests an Authorized User to input his/her identification code; or (b) sending an email where the fake Access Administrator requests an Authorized User to input his/her identification code (Article 7).

Any person who commits (a) above (Article 3) is subject to imprisonment of up to three years or a fine of up to JPY 1,000,000 (Article 11). Any person who commits (b) to (e) above (Articles 4 to 7) is subject to imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12). However, if the person committing (c) (Article 5) does not know that the recipient intends to use the identification code for an Unauthorized Access, that person is subject to a fine of up to JPY 300,000 (Article 13).

(B) The Penal Code provides for criminal sanctions on the creation and provision of Improper Command Records which give improper commands, such as a computer virus, to a computer (*fusei shirei denji-teki kiroku*). "**Improper Command Records**" means (i) electromagnetic records that give a computer an improper command which causes the computer to be operated against the operator's intention or to fail to be operated in accordance with the operator's intention, and (ii) electromagnetic or other records which describe such improper commands.

Under the Penal Code, any person who creates or provides, without any justifiable reason, Improper Command Records or who knowingly infects or attempts to infect a computer with Improper Command Records is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Article 168-2). Any person who obtains or keeps Improper Command Records for the purpose of implementing such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Article 168-3).

In addition, the Penal Code provides for the following additional penalties:

(i) any person who obstructs the business of another by causing a computer used in the business to be operated against the operator's intention, or to fail to be operated in accordance with the operator's intention, by (a) damaging that computer or any electromagnetic record used by that computer, or (b) giving false information or an improper command to the computer, is subject to imprisonment of up to five years or a fine of up to JPY 1,000,000 (Article 234-2);

(ii) any person who gains or attempts to gain, or causes or attempts to cause a third party to gain, illegal financial benefits by (a) creating false electromagnetic records by giving false information or an improper command to a computer, or (b) providing false electromagnetic records, for processing by a third party, in either case in connection with a gain, a loss or a change regarding financial benefits, is subject to imprisonment of up to 10 years (Article 246-2); and

(iii) any person who creates, provides or attempts to provide electromagnetic records for the purpose of causing a third party to mistakenly administer matters which relate to rights, obligations or proofs of facts, is subject to imprisonment of up to five years or a fine of up to JPY 500,000. However, if the act relates to records to be made by public authorities or public servants, the penalty is imprisonment of up to 10 years or a fine of up to JPY 1,000,000 (Article 161-2).

Hacking (i.e. unauthorised access)

Hacking is an Unauthorized Access under the UCAL, punishable by imprisonment of up to three years or a fine of up to JPY 1,000,000.

If the hacking is made through Improper Command Records, it is also punishable under the Penal Code (please see question 1.1(B) above). In addition, if a business is obstructed by such hacking, the crime is punishable by imprisonment of up to five years or a fine of up to JPY 1,000,000 (Penal Code, Article 234-2).

Denial-of-service attacks

This carries the same penalties as hacking.

Phishing

Article 7 of the UCAL prohibits phishing, while Article 4 of the UCAL prohibits obtaining any identification code through phishing. These actions are punishable by imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12).

In addition, any person who gains illegal benefits by using identification codes obtained by phishing is subject to imprisonment of up to 10 years under Article 246-2 of the Penal Code.

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

This carries the same penalties as hacking.

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

Any person who obtains or keeps Improper Command Records for the purpose of using such records is subject to imprisonment of up to two years or a fine of up to JPY 300,000 (Penal Code, Article 168-3).

As an example, nine persons were prosecuted for uploading software which contained a computer virus to an online storage system and which infected the computers of people who accessed the storage and downloaded the software from September to December 2016.

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

This carries the same penalties as phishing.

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

In addition to the criminal penalties applicable to phishing, electronic theft is penalised under the Unfair Competition Prevention Act. If a current or former employee (a) acquires a trade secret of the employer through theft, fraud, threat, or other illegal actions (the "**Illegal Actions**"), including an Unauthorized Access, or (b) uses or discloses a trade secret of the employer acquired through Illegal Actions, for the purpose of obtaining wrongful benefits or damaging the owner of the trade secret, that employee is subject to imprisonment of up to 10 years or a fine of up to JPY 20,000,000, or both (Article 21, Paragraph 1). In addition, if that employee commits any of the foregoing acts outside Japan, the fine is increased up to JPY 30,000,000 (Article 21, Paragraph 3).

Under the Copyright Act, any person who uploads electronic data of movies or music, without the permission of the copyright owner, to enable another person to download them, is subject to imprisonment of up to 10 years or a fine of up to JPY 10,000,000, or both (Article 119, Paragraph 1). Further, any person who downloads electronic data which is protected by another person's copyright, and who knows of such protection, is subject to imprisonment of up to two years or a fine of up to JPY 2,000,000, or both (Article 119, Paragraph 3). In addition, any person who sells, lends, manufactures, imports, holds or uploads any device or program which may remove, disable or change technology intended to protect copyright (e.g., copy protection code), is subject to imprisonment of up to three years or a fine of up to JPY 3,000,000, or both (Article 120-2).

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

This carries the same penalties as electronic theft.

Failure by an organisation to implement cybersecurity measures

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorized Users, examine the validity of functions to control access to the Access Controlled Computer, and to implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes which have not been used for a long time, implementing a batch program to address a security hole, program updates, and appointing an officer for network security) (Article 8). However, there is no criminal sanction on a breach of these obligations.

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

The UCAL provides for the extraterritorial application of Articles 3, 4, 5 (except where the offender did not know the recipient's purpose) and 6 of the UCAL (Article 14).

The Penal Code has extraterritorial application (Article 4-2).

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?

No, there are no such actions.

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.

No. The Organized Crime Act, which applies to an act of terrorism, designates certain material crimes, such as murder, identified in the Penal Code, and imposes penalties which are heavier than those under the Penal Code. However, criminal offences regarding cybersecurity which are described in question 1.1 above are not designated crimes under the Organized Crime Act.

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.

In addition to the UCAL, the Penal Code and the Unfair Competition Prevention Act described above, the following laws are also applicable to cybersecurity.

- Basic Act on Cybersecurity

  This provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity. Further, it obligates operators of

material infrastructure (e.g., financial institutions, operators of railroads, airplanes and other means of transportation, and providers of electricity, gas and water) and networks (e.g., telecommunications networks) to make efforts to voluntarily and proactively enhance cybersecurity and to cooperate with the national and local governments to promote measures to enhance cybersecurity. Based on this Basic Act, the National Center of Incident Readiness and Strategy for Cybersecurity was established in 2015.

A bill to revise the Basic Act in order to establish a cybersecurity council was recently submitted to the Diet. The cybersecurity council is intended to be the avenue which will allow national and local governmental authorities and business operators to share information which may facilitate the proposal and implementation of cybersecurity measures. However, the bill was not approved at the Diet session which took place on July 22 and will be discussed at the next Diet session.

- Telecommunication Business Act (the "**TBA**")

Article 4 of the TBA provides that (1) the secrecy of communications being handled by a telecommunications carrier shall not be violated, and (2) any person who is engaged in a telecommunications business shall not disclose secrets obtained, while in office, with respect to communications being handled by the telecommunications carrier, even after he/she has left office.

The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, data on access logs and IP addresses are protected under the secrecy of communications. If a telecommunications carrier intentionally obtains any information protected under the secrecy of communications, discloses protected information to third parties, and uses protected information without the consent of the parties who communicated with each other, that telecommunications carrier is in breach of Article 4(1).

To prevent cyber attacks, it would be useful for telecommunications carriers to collect and use information regarding cyber attacks, e.g., access logs of infected devices, and share information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyber attacks without breaching Article 4(1). The Ministry of Internal Affairs and Communications ("**MIC**"), the governmental agency primarily responsible for implementing the TBA, issued reports in 2014 and 2015 which address whether a telecoms carrier may deal with cyber attacks and the issues that may arise in connection with the secrecy of communications. The findings in both reports are included in the guidelines on cyber attacks and the secrecy of communications (the "**Guidelines**") issued by the Council regarding the Stable Use of the Internet (the "**Council**"), a council composed of five associations which include the Japan Internet Providers Association, a voluntary association of telecommunications carriers, cable TV service providers and other companies conducting businesses related to the Internet. The Guidelines include the contents of MIC's 2014 and 2015 reports. The Guidelines, however, are not legally binding, although they carry a lot of weight because MIC confirmed them before they were issued by the Council.

Further, in 2013, MIC started a project called ACTIVE (Advanced Cyber Threats response InitiatiVE) that aims to protect Internet users from cyber attacks by collaborating with ISPs and vendors of IT systems. To prevent computer virus infections, warning users or blocking communications in accordance with the Guidelines may be done by ISPs which are members of ACTIVE. For example, according to ACTIVE's release dated February 26, 2016, MIC has started a program through ACTIVE to prevent malware infection. The program aims to mitigate damage by blocking telecommunications between the malware and the C&C (Command and Control) server and by warning users who have infected devices. According to the website of ACTIVE, ACTIVE gathers information from business operators such as vendors of IT systems and makes a list of computer viruses and malware and infected websites.

In addition, in May 2018, the TBA was amended to introduce a new mechanism which enables a telecommunications carrier to share with other carriers information on transmission sources of cyber attacks. The amendments will be effective in November 2018.

- Act on the Protection of Personal Information (the "**APPI**")

The APPI is the principal data protection legislation in Japan. It is the APPI's basic principle that the cautious handling of Personal Information under the principle of respect for individuals will promote the proper handling of Personal Information. "**Personal Information**" means information about specific living individuals which can identify them by name, date of birth or other descriptions contained in the information (including information that will allow easy reference to other information which may enable individual identification) (Article 2, Paragraph 1). A business operator handling Personal Information may not disclose or provide Personal Information without obtaining the subject's consent, unless certain conditions are met.

To prevent cyber attacks, it would be useful for business operators to collect and use information regarding the cyber attacks, e.g., access logs of infected devices, and share information with other business operators or public authorities. However, if the information includes Personal Information, it would be subject to the restrictions on the use and disclosure of Personal Information under the APPI.

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 UCAL requires Access Administrators to make efforts to manage the identification codes of Authorized Users, examine the validity of functions to control access to the Access Controlled Computer, and implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes which have not been used for a long time, implementing a batch program to address a security flaw, program updates, and appointing an officer for network security) (Article 8).

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 Ministry of Economy, Trade and Industry ("**METI**") and the Independent Administrative Agency Information-technology Promotion Agency ("**IPA**") jointly issued the Cybersecurity Management Guidelines (the latest version of which is as of November 2017). The guidelines describe three principles that the management of companies, which have a dedicated division for information system and are utilising IT, should recognise to protect their company from cyber attacks and 10 material items on which

management should give instructions to executives or directors in charge of IT security including the chief information security officer ("**CISO**").

The 10 material items and some examples of recommended actions for each item described in the guidelines are as follows:

(i) Recognise cybersecurity risks and develop company-wide measures

Example: Develop security policy which incorporates cybersecurity risk management while aligning it with the company's management policy so that management can publish company-wide measures.

(ii) Build a structure or process for cybersecurity risk management

Example: CISO to establish a system to manage cybersecurity risks and set forth the responsibility clearly.

Example: Directors to examine whether a system which will manage cybersecurity risks has been established and is being operated properly.

(iii) Secure resources (e.g., budget and manpower) to execute cybersecurity measures

Example: Allocating resources to implement specific cybersecurity measures.

(iv) Understand possible cybersecurity risks and develop plans to deal with such risks

Example: During a business strategy exercise, identify information which needs protection and cybersecurity risks against the information (e.g., damage from leakage of trade secrets on a strategic basis).

(v) Build a structure to deal with cybersecurity risks (i.e., structure to detect, analyse and defend against cybersecurity risks)

Example: Secure the computing environment and network structure used for important operations by defending them at multiple layers.

(vi) Publish cybersecurity measures framework ("**PDCA**") and its action plan

Example: Develop a structure or process where one can constantly respond to cybersecurity risks (assurance of implementation of PDCA).

(vii) Develop an emergency response system (emergency contacts, initial action manual, and Computer Security Incident Response Team ("**CSIRT**")), and execute regular hands-on drills

Example: Issue instructions to promptly cooperate with relevant organisations and to investigate relevant logs to ensure that efficient actions or investigations can be taken to identify the cause and damage of a cyber attack.

Example: Execute drills, including planning activities, to prevent recurrence after Incidents and reporting Incidents to relevant authorities.

(viii) Develop a system to recover from the damages caused by an Incident

Example: Establish protocols for recovery from business suspension or other damages caused by an Incident and execute drills in accordance with protocols.

(ix) Ensure that entities in the company's entire supply chain, including business partners and outsourcing companies for system operations, take security measures

Example: Conclude agreements or other documents to provide clearly how group companies, business partners and outsourcing companies for system operations in the company's supply chain will take security measures.

Example: Have access to and understand reports on how group companies, business partners and outsourcing companies for system operations in the company's supply chain take security measures.

(x) Collect information on cyber attacks through participation in information-sharing activities, and develop the environment to utilise such information

Example: Help society guard against cyber attacks by actively giving, sharing and utilising relevant information.

Example: Report information on malware and illegal access to the IPA in accordance with public notification procedures (standards for countermeasures for computer viruses and for illegal access to a computer).

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.

The secrecy of communications is strongly protected under the TBA. To prevent cyber attacks, it would be useful for telecommunications carriers to collect and use information regarding the cyber attacks, e.g., access logs of infected devices, and share information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyber attacks without breaching Article 4(1). Thus, it is difficult for telecommunications carriers to balance prevention of cyber attacks with the protection of secrecy of communications. MIC tried to deal with this issue by helping to establish the Guidelines, by collaborating with ISPs through ACTIVE and by introducing a new mechanism to share the information on transmission sources of cyber attacks (please see question 2.1 above).

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 is no mandatory requirement to report Incidents.

However, under the guidelines for banks issued by the Financial Services Agency ("**FSA**"), banks are required to report an Incident immediately after becoming aware of it. The guidelines are not legally binding; however, because FSA is a powerful regulator of the financial sector, banks would typically comply with FSA's guidelines (please see question 3.1). The report must include:

(i) the date and time when the Incident occurred and the location where the Incident occurred;

(ii) a summary of the Incident and which services were affected by the Incident;

(iii) causes of the Incident;

(iv) a summary of the facilities affected by the Incident;

(v) a summary of damages caused by the Incident, and how and when the situation was remedied or will be remedied;

(vi) any effect to other business providers;

(vii) how banks responded to enquiries from users and how they notified users, public authorities and the public; and

(viii) possible measures to prevent similar Incidents from happening.

In addition, if a cyber attack causes a serious Incident specified in the TBA and the enforcement rules of the TBA, such as a temporary suspension of telecommunications services or a violation of the secrecy of communications, the telecommunications carrier is required to report the Incident to MIC promptly after its occurrence. In addition, the carrier is required to report the details of the said Incident to MIC within 30 days from its occurrence. The detailed report must include:

(i) the date and time when the Incident occurred;

(ii) the date and time when the situation was remedied;

(iii) the location where the Incident occurred (the location of the facilities);

(iv) a summary of the Incident and which services were affected by the Incident;

(v) a summary of the facilities affected by the Incident;

(vi) details of the events or indications of the Incident, the number of users affected, and the affected service area;

(vii) measures taken to deal with the Incident, including the persons who dealt with it, in chronological order;

(viii) causes which made the Incident serious, including how the facilities have been managed and maintained;

(ix) possible measures to prevent similar Incidents from happening;

(x) how the telecoms carrier responded to inquiries from users and how it notified users of the Incident;

(xi) internal rules in connection with the Incident;

(xii) if the telecoms carrier experienced similar Incidents in the past, a summary of the past Incidents;

(xiii) the name of the manager of the telecoms facilities; and

(xiv) the name and qualifications of the chief engineer of the telecoms facilities.

Further, it is recommended that companies report the Incident to the IPA (please see question 2.3 above). The report must include:

(i) the location where the infection was found;

(ii) the name of the computer virus. If the name is unknown, features of the virus found in the IT system;

(iii) the date when the infection was found;

(iv) the types of OS used and how the IT system is connected (e.g. LAN);

(v) how the infection was found;

(vi) possible cause of the infection (e.g., email or downloading files);

(vii) extent of the damage (e.g., the number of infected PCs); and

(viii) whether the infection has been completely removed.

The IPA also has a contact person whom the companies may consult, whether or not they file a report with the IPA, as to how they can deal with cyber attacks or any Unauthorized Access. According to the IPA's website, it had 7,600 consultations in 2017.

If the Incidents involve any disclosure, loss, or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the Personal Information Protection Committee (the "**PPC**") regarding the APPI, the operator is expected to promptly submit to the PPC a summary of such disclosure, loss or damage, and planned measures to prevent future occurrences.

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?

Please see question 2.5. Further, through ACTIVE, business operators are permitted to share information regarding cyber attacks (please see question 2.1).

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 Cybersecurity Management Guidelines recommend knowing who should be notified if a cyber attack has caused any damage, gathering information to be disclosed, and promptly publishing the Incident, taking into account its impact on stakeholders (please see question 2.3).

Further, if the Incidents involve any disclosure, loss or damage of Personal Information handled by a business operator, then, according to the guidelines issued by the PPC regarding the APPI, the operator is expected, depending on the contents or extent of the disclosure, loss or damage, to notify the affected individuals of the facts relevant to the disclosure, loss or damage, or to make the notification readily accessible to the affected individuals (e.g., posting the notification on the operator's website), in order to prevent secondary damages or similar Incidents.

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?

The secrecy of communications protects not only the contents of communications but also any information that would enable someone to infer the meaning or the contents of communications. In this regard, IP addresses and email addresses are protected under the secrecy of communications. Further, personally identifiable information is protected under the secrecy of communications if it is delivered through telecommunications facilities. With respect to an Incident, a telecommunications carrier may not share information protected under the secrecy of communications unless it complies with the Guidelines or the instructions of ACTIVE (please see questions 2.1 and 2.5).

In addition, personally identifiable information of cyber threat-makers and individuals who have been inadvertently involved in an Incident would be Personal Information under the APPI which cannot be provided to a third party without obtaining the prior consent of the data subjects, except in limited instances. One such exception is where a public authority needs the cooperation of a private person to implement the authority's legal duties, and the performance of those legal duties will likely be impeded if the private person has to

first obtain the data subject's consent. In this regard, the provision of personally identifiable information of cyber threat-makers would not require their consent.

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

MIC is the governmental agency primarily responsible for implementing the TBA.

METI is not a regulator that has a specific mandated regulatory authority under specific laws. Rather, it promulgates desirable policies for each industry.

The PPC is an independent organ which supervises the enforcement and application of the APPI.

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

Other than the report of a serious Incident under the TBA (please see question 2.5), reporting is not mandatory. If a telecommunications carrier does not report a serious Incident, it is subject to a fine of up to JPY 300,000.

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

No examples can be found based on publicly available information.

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.

In general, the financial business sector and the telecommunications service sector closely collaborate with relevant authorities on information security.

In July 2015, FSA issued a summary of its policies to strengthen cybersecurity in the financial business sector. According to the summary, FSA's five policies are: (i) continuous dialogue with financial institutions to understand their cybersecurity risks; (ii) improving information-sharing among financial institutions; (iii) implementing cybersecurity exercises in which financial institutions, FSA and other public authorities participate; (iv) developing cybersecurity human resources; and (v) establishing a department in FSA to handle cybersecurity matters. Based on these policies, FSA amended its guidelines for banks to include standards on cybersecurity management, such as establishing an organisation to handle emergencies (e.g., CSIRT), designating a manager in charge of cybersecurity, preparing multi-layered defences against cyber attacks and implementing a periodic assessment of cybersecurity. The guidelines are not legally binding; however, because FSA is a powerful regulator of the financial sector, banks would typically comply with FSA's guidelines.

As described above, telecommunications carriers are required to report a serious Incident specified in the TBA (please see question 2.5). In addition, if a telecommunications carrier does not take appropriate measures to remedy problems with its services, MIC may order it to improve its business. Failure to comply with the order is subject to a fine of up to JPY 2,000,000.

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?

Please see question 3.1.

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?

Under the Companies Act, a director has the duty to act with "due care as a prudent manager" in performing his/her functions as director (*zenkan chuui gimu*). The applicable standard of care is that which a person in the same position and situation would reasonably be expected to observe. In general, if a director fails to get relevant information, enquire or consider how to prevent Incidents, to the extent these acts are reasonably expected of him/her based on the facts when he/she made a decision (e.g., decision to purchase the IT system), then he/she would be in breach of this duty.

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?

The Cybersecurity Management Guidelines jointly issued by METI and IPA recommend companies to build a structure or process for cybersecurity risk management and, as an example, to designate a CISO according to the companies' policies, including the security policy (please see question 2.3).

Further, FSA's guidelines for banks provide the standards regarding cybersecurity management, such as establishing an organisation to handle emergencies (e.g., CSIRT), designating a manager in charge of cybersecurity and implementing a periodic assessment of cybersecurity (please see question 3.1).

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)?

There are no disclosure requirements that are specific to cybersecurity risks or Incidents.

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

No, there are no other specific requirements.

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.

Basically, if a person breaches a contract, the other party may bring a civil action based on the breach. The plaintiff has the burden of proving the breach, the damages incurred by it, and the causation between the breach and the plaintiff's damages.

In addition, the Civil Act of Japan provides for a claim based on tort. If a person causes damages to another, the injured party may bring a civil action based on tort. The plaintiff has the burden of proving the damages incurred by it, the act attributable to the defendant, and the causation between the defendant's act and the plaintiff's damages.

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

A vendor of a computer system was sued by a company which used the system provided by the vendor. The case related to cyber attacks (SQL injections) to the system which resulted in the disclosure of credit card information of the company's clients. The company sought the payment of damages caused by the cyber attacks in the amount of approximately JPY 100,000,000, based on breach of contract. The Tokyo District Court decided that although the vendor was required to provide programs which are suitable for blocking SQL injections in accordance with existing standards when the computer system was provided, the Incident was also partially attributable to the company because it ignored the vendor's proposal to improve the system. The vendor was ordered to pay only approximately JPY 20,000,000 (Tokyo District Court decision dated January 23, 2014).

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

Tort theory is available under the Civil Act of Japan (please see question 5.1).

6 Insurance

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

Yes. In general, there are two categories of insurance against Incidents, namely (i) insurance to cover the losses incurred by the vendor of an IT system, and (ii) insurance to cover the losses incurred by a business operator using the IT system.

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 regulatory limitations on insurance coverage under the law. The coverage may differ depending on the insurance products of insurance companies.

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?

No, there are no specific requirements.

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?

No, there are no Applicable Laws.

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.

Law enforcers have the power to investigate Incidents which are related to crimes under Applicable Laws. In accordance with the "cybercrime project" of the National Police Agency, the police in each prefecture have established a contact point where consultations and information regarding cybercrimes are handled.

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

No, there are no such requirements.

Hiromi Hayashi
Mori Hamada & Matsumoto
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: *+81 3 5220 1811*
Email: *hiromi.hayashi@mhmjapan.com*
URL: *www.mhmjapan.com*

Hiromi Hayashi is a partner at Mori Hamada & Matsumoto, which she joined in 2001. She specialises in communications law and regulation, and authored the Japanese portion of *Telecommunication in Asia* in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. She was admitted to the Bar in 2001 in Japan and in 2007 in New York. She worked at Mizuho Corporate Bank from 1989 to 1994 and at Davis Polk & Wardwell in New York from 2006 to 2007.

MORI HAMADA & MATSUMOTO

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in Fukuoka, Nagoya, Osaka, Beijing, Shanghai, Singapore, Yangon Bangkok and Ho Chi Minh, and a Jakarta desk. The firm has over 450 attorneys and a support staff of approximately 450, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well-known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise on, telecommunications, broadcasting, the Internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

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