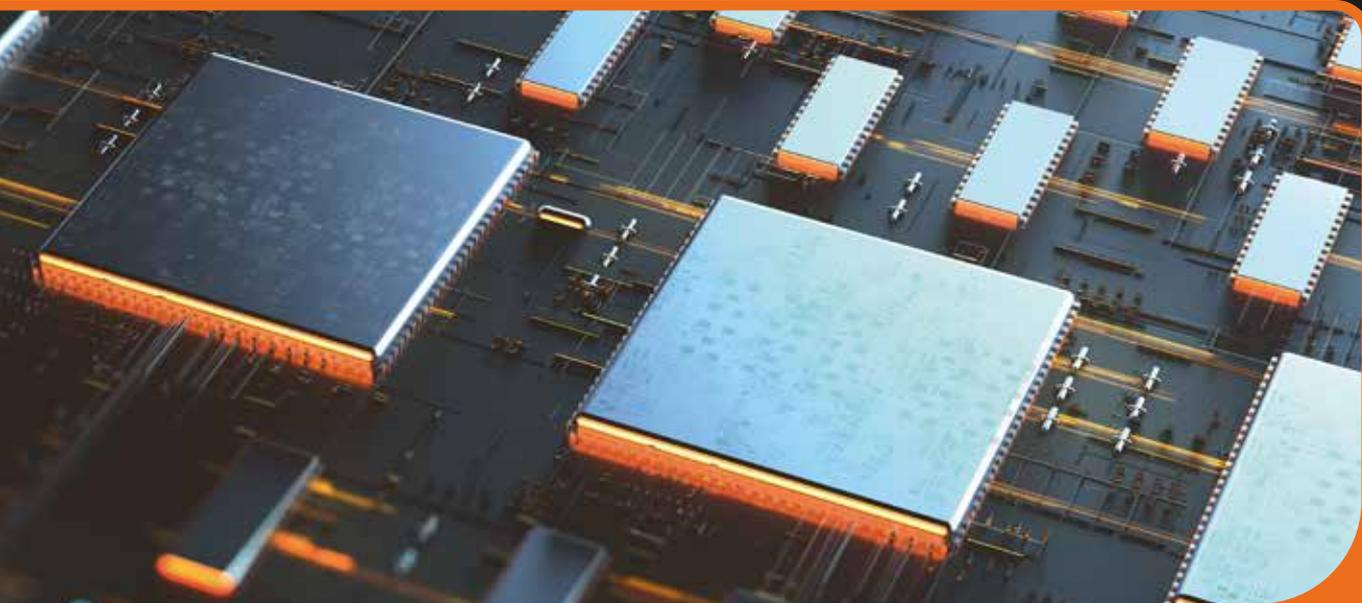


**International
Comparative
Legal Guides**



Practical cross-border insights into cybersecurity

**Cybersecurity
2022**

Fifth Edition

Contributing Editor:

Nigel Parker
Allen & Overy LLP

ICLG.com

Expert Analysis Chapters

- 1** **Infiltrate, Extort, Repeat – The Ransomware Pandemic**
Nigel Parker, Nathan Charnock & Daniel Ruben, Allen & Overy LLP
- 6** **Phantom Responsibility: How Data Security and Privacy Lapses Can Lead to Personal Liability for Officers and Directors**
Christopher Ott, Rothwell Figg
- 18** **Cyber Capability to Evade International Sanctions: Problems, Solutions and Innovations**
Julian Clark & Reema Shour, Ince
- 23** **Why AI is the Future of Cybersecurity**
Akira Matsuda & Hiroki Fujita, Iwata Godo

Q&A Chapters

- 27** **Australia**
Nyman Gibson Miralis: Dennis Miralis, Phillip Gibson & Jasmina Ceic
- 34** **Belgium**
Sirius Legal: Roeland Lembrechts & Bart Van den Brande
- 42** **Brazil**
Mattos Filho: Fabio Ferreira Kujawski, Paula Moreira Indalecio, Paulo Marcos Rodrigues Brancher & Thiago Luís Sombra
- 49** **Canada**
Baker & McKenzie LLP: Theo Ling, Andrew Chien, Ahmed Shafey & John Pirie
- 59** **China**
King & Wood Mallesons: Susan Ning & Han Wu
- 69** **England & Wales**
Allen & Overy LLP: Nigel Parker & Benjamin Scrace
- 79** **France**
BERSAY: Frédéric Lecomte
- 86** **Germany**
Eversheds Sutherland: Dr. Alexander Niethammer, Dr. David Rieks, Stefan Saerbeck & Constantin Herfurth
- 94** **Greece**
Nikolinakos & Partners Law Firm: Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos
- 103** **India**
Subramaniam & Associates (SNA): Aditi Subramaniam
- 111** **Ireland**
Maples Group: Claire Morrissey & Kevin Harnett
- 118** **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi, Masaki Yukawa & Daisuke Tsuta
- 127** **Kenya**
Rilani Advocates: Nzilani Mweu
- 133** **Mexico**
Creel, García-Cuellar, Aiza y Enríquez: Begoña Cancino Garín (Former Partner)
- 139** **Norway**
CMS Kluge: Stian Hultin Oddbjørnsen, Ove André Vanebo, Iver Jordheim Brække & Mari Klungsøyr Kristiansen
- 146** **Poland**
Leśniewski Borkiewicz & Partners (LB&P): Mateusz Borkiewicz, Grzegorz Leśniewski & Jacek Cieśliński
- 155** **Saudi Arabia**
Alburhan: Saeed Algarni, Mohammed Ashbah & Muhanned Alqaidy
- 161** **Singapore**
Drew & Napier LLC: Lim Chong Kin, David N. Alfred & Albert Pichlmaier
- 171** **Sweden**
TIME DANOWSKY Advokatbyrå AB: Jonas Forzelius & Esa Kymäläinen
- 178** **Switzerland**
Kellerhals Carrard: Dr. Oliver M. Brupbacher, Dr. Nicolas Mosimann, Dr. Claudia Götz Staehelin & Marlen Schultze
- 188** **Taiwan**
Lee and Li, Attorneys-at-Law: Ken-Ying Tseng
- 194** **Thailand**
Silk Legal: Dr. Jason Corbett & Koraphot Jirachocksubsin
- 201** **USA**
Ropes & Gray LLP: Edward R. McNicholas & Kevin J. Angle

Japan

Mori Hamada & Matsumoto



Hiromi Hayashi



Masaki Yukawa



Daisuke Tsuta

1 Cybercrime

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

Hacking (i.e. unauthorised access)

As background, there are two main laws that criminalise cyberattacks, namely (A) the Act on the Prohibition of Unauthorised Computer Access (the “UCAL”), and (B) the Penal Code.

(A) The UCAL imposes criminal sanctions on any person who makes an “**Unauthorised 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**”).

Unauthorised Access means any action that 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 “**Authorised User**”), without the permission of the Access Administrator or the Authorised User, or (ii) inputting any information (other than an identification code) or command that enables that person to evade control (e.g., cyberattack of a security flaw), without the permission of the Access Administrator (UCAL, Article 2, Paragraph 4).

The UCAL prohibits the following actions:

- (a) Unauthorised Access (Article 3);
- (b) obtaining the identification code of an Authorised User to make Unauthorised Access (Article 4);
- (c) providing the identification code of an Authorised User to a third party other than the Access Administrator or the Authorised User (Article 5);
- (d) keeping the identification code of an Authorised User that was obtained illegally to make Unauthorised Access (Article 6); and
- (e) impersonating the Access Administrator or causing a false impression of being the Access Administrator by: (a) setting up a website where a fake Access Administrator requests an Authorised User to input his/her identification code; or (b) sending an email where a fake Access

Administrator requests an Authorised 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 Unauthorised 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 mean (i) electromagnetic records that give a computer an improper command that causes the computer to be operated against the operator’s intentions or to fail to be operated in accordance with the operator’s intentions, and (ii) electromagnetic or other records that 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 the foregoing acts 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 that business to be operated against the operator’s intentions, or to fail to be operated in accordance with the operator’s intentions, 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 that 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 is Unauthorised 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, point 1, (B)). 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

These carry 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.

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

Other than the crime of providing Improper Command Records (see above) without any justifiable reason to any third party, which is subject to imprisonment of up to three years or a fine of up to JPY 500,000 (Penal Code, Article 168-2), there is no general prohibition against the distribution, sale or offering of hardware, software or other tools that may be used to commit a cybercrime.

Generally, if a person provides hardware, software or other tools knowing that those tools will be used for Unauthorised Access (see above) or to infect a computer with Improper Command Records, that person will be an accessory to these crimes. However, the Supreme Court has taken a relatively modest approach in punishing providers of software that can be used for either legitimate or illegal purposes. The Supreme Court on 19 December 2011 acquitted a developer of a P2P software that could be and actually was used for copyright violation, saying that a software provider may be punished as an accessory only if he knew that the software will be used for a specific criminal act or mostly for criminal acts. In this case, the court found that since the developer constantly warned users not to use the software in violation of any copyright, it was difficult to attribute knowledge to the developer.

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

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 people were prosecuted for uploading software that contained a computer virus to an online storage system, and that 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 an employer through theft, fraud, threat or other illegal actions (the “**Illegal Actions**”), including Unauthorised 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 to 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). Furthermore, any person who downloads electronic data that 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 that 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).

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

Since there is no exemption for this type of testing, unsolicited penetration testing is punishable as Unauthorised Access.

Vulnerability testing without permission is generally not allowed. However, the National Institute of Information and Communications Technology (the “**NICT**”) (and only the NICT) is allowed to conduct vulnerability testing without permission under the Law on the National Institute of Information and Communication Technology, which exempts the NICT from the prohibition against Unauthorised Access.

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.

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 also has extraterritorial application (Article 4-2).

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

The above-mentioned offences are not subject to exceptions such as "ethical hacking" or lack of intention to cause damage or make financial gains.

As discussed above (please see question 1.1), vulnerability testing without permission may be conducted only by the NICT based on a special law, and there are no general exceptions to similar activities for other persons.

2 Cybersecurity Laws

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

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

(A) Basic Act on Cybersecurity (the "BAC")

This provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity. In July 2018, pursuant to the BAC, the Japanese government issued the Cybersecurity Strategy (drafted by the Cybersecurity Strategy Headquarters (the "CSHQ") and established under Article 25 of the BAC to promote Japan's cybersecurity measures, and its secretariat, the National Center of Incident Readiness and Strategy for Cybersecurity (the "NISC")). Since the Cybersecurity Strategy has been revised every three years, the NISC prepared and sought public comments on the draft of the Cybersecurity Strategy for the next period from 2021 to 2024, in July 2021.

Furthermore, the BAC obligates operators of critical infrastructure to make efforts to voluntarily and proactively enhance cybersecurity, and to cooperate with the national and local governments to promote measures to enhance cybersecurity. In December 2018, the BAC was amended to establish the cybersecurity council (the "Cybersecurity Council"). The Cybersecurity Council is intended to be the avenue to allow national and local governmental authorities and business operators to share information that may facilitate the proposal and implementation of cybersecurity measures. The Cybersecurity Council was established in April 2019 and has 265 participating entities as of June 2021.

(B) 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 cyberattacks, it would be useful for telecommunications carriers to collect and use information regarding cyberattacks, e.g., access logs of infected devices, and share this information with other telecommunications carriers or public authorities. However, the TBA does not explicitly provide how a telecoms carrier may deal with cyberattacks without breaching Article 4(1). The Ministry of Internal Affairs and Communications (the "MIC"), the governmental agency primarily responsible for implementing the TBA, issued reports in 2014, 2015 and 2018 that addressed whether a telecoms carrier may deal with cyberattacks and the issues that may arise in connection with the secrecy of communications. The findings and contents of the MIC's three reports are included in the guidelines on cyberattacks and the secrecy of communications (the "Guidelines"), issued by the Council regarding the Stable Use of the Internet. This Council is composed of five associations that are the ICT Information Sharing and Analysis Center Japan (the "ICT-ISAC Japan"), the Telecommunications Carriers Association, the Telecom Services Association, the Japan Internet Providers Association, and the Japan Cable and Telecommunications Association. The Guidelines are not legally binding, although they carry a lot of weight because the MIC confirmed them before the Guidelines were issued.

Furthermore, in 2013, the MIC started a project called ACTIVE (Advanced Cyber Threats response Initiative) that aims to protect internet users from cyberattacks by collaborating with ISPs and IT systems vendors. To prevent computer virus infections, ISPs that are members of ACTIVE may warn users or block communications in accordance with the Guidelines.

In addition, in May 2018, the TBA was amended to introduce a new mechanism that enables a telecommunications carrier to share with other carriers' information on transmission sources of cyberattacks through an association confirmed by the MIC as being eligible to assist telecommunications carriers. After the amendments became effective in November 2018, the MIC confirmed that the ICT-ISAC Japan to be that association in January 2019.

(C) 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 that 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 cyberattacks, it would be useful for business operators to collect and use information regarding cyberattacks, e.g., access logs of infected devices, and share this 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.

(D) the Japanese Foreign Exchange and Foreign Trade Act (the “FEFTA”)

The FEFTA regulates the export of sensitive goods and technologies, including encryption software and hardware (please see question 3.3), as well as inward direct investments such as acquisition of shares in Japanese companies by non-Japanese investors. From the viewpoint of national security, prior notification to the Ministry of Finance and other competent authorities will be required for an acquisition of 1% or more of shares in a Japanese company that engages in information technologies, software, and telecommunications businesses, unless an exemption is applicable, and the foregoing authorities may order the cessation of the acquisition.

2.2 Critical or essential infrastructure and services: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorised 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 that 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).

The so-called “**Critical Information Infrastructure Operators**” are required to make efforts to deepen their interest and understanding of the importance of cybersecurity, and to voluntarily and proactively ensure cybersecurity for the purpose of providing services in a stable and appropriate manner (BAC, Article 6). Article 3(1) of the BAC defines Critical Information Infrastructure Operators as operators of businesses that provide an infrastructure that is a foundation of people’s lives and economic activities that could be enormously impacted by the functional failure or deterioration of that infrastructure.

The CSHQ formulated the Cybersecurity Policy for Critical Infrastructure Protection as a non-mandatory guideline that designated 14 critical infrastructure areas under its coverage. These 14 areas are information and communication, financial services, aviation, airports, railways, electric power, gas supply, government and administrative supply, medical, water, logistics, chemical, credit card, and petroleum.

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

(A) Cybersecurity Management Guidelines

The Ministry of Economy, Trade and Industry (the “METI”) and the Independent Administrative Agency Information-technology Promotion Agency (the “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 that have a dedicated division for information systems and that are utilising IT, should recognise to protect their company from cyberattacks, 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 (the “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 a security policy that 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: The CISO establishes a system to manage cybersecurity risks and set forth the responsibilities clearly.
Example: Directors examine whether a system that 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 that needs protection and cybersecurity risks against that 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 through multiple layers.
- (vi) Publish a cybersecurity measures framework (the “PDCA”) and its action plan.
Example: Develop a structure or process where one can constantly respond to cybersecurity risks (assurance of implementation of a PDCA).
- (vii) Develop an emergency response system (e.g., emergency contacts, initial action manual, and Computer Security Incident Response Team (the “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 cyberattack.
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 these 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 cyberattacks through participation in information-sharing activities and develop an environment to utilise such information.

Example: Help society guard against cyberattacks 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).

(B) Common Standards on Information Security Measures of Governmental Entities

The CSHQ and the NISC jointly issued the Common Standards on Information Security Measures of Governmental Entities under Article 26(1) of the BAC. The standards are a unified framework for improving the level of information security of governmental entities and define the baseline for information security measures to ensure a higher level of information security. Although these standards do not apply to private companies, some entities refer to these standards for their information security measures. The standards were amended in July 2021.

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

There is no mandatory requirement to report Incidents.

However, under the guidelines for banks issued by the Financial Services Agency (the "FSA"), banks are required to report an Incident immediately after becoming aware of it. The guidelines are not legally binding; however, because the FSA is a powerful regulator of the financial sector, banks would typically comply with the FSA's guidelines (please see question 4.1). 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 the 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 cyberattack 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 the MIC promptly after its occurrence. In addition, the carrier is required to report the details of the said Incident to the 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 that 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.

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

- (i) the location of 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 cyberattacks or any Unauthorised Access. According to the IPA's website, it had 9,698 consultations in 2020.

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 (a "Data Breach") and planned measures to prevent future occurrences.

However, under the newest amendments to the APPI, which were promulgated on 12 June 2020 and will take effect in April 2022 (the "Amended APPI"), the business operator must report a Data Breach to the PPC in the following cases:

- (i) a Data Breach of "Special Care-required Personal Information" (defined in the APPI), such as results of employees' health examinations;
- (ii) a Data Breach of Personal Data (defined in the APPI) that poses a risk of financial damage to data subjects, such as credit card numbers;
- (iii) a Data Breach caused by wrongful intent such as cyberattack or internal fraud;

- (iv) a large number (more than 1,000 data subjects) of Data Breach occurrences; and
- (v) when there is a possibility of any of the foregoing happening.

In addition, a business operator who undertakes “advanced encryption or other measures that are necessary to protect the rights and interests of the data subjects” will be exempted from the reporting or notification obligation, even if there is a Data Breach.

When a business operator recognises a Data Breach listed above or the possibility thereof, it must promptly submit a preliminary report on the matters known to it at the time, and must submit a definitive report within 30 days (60 days in the case of item (iii) above).

The report must include:

- (i) an outline of the Data Breach;
- (ii) details of personal data;
- (iii) the number of Data Breach occurrences;
- (iv) the cause of the Data Breach;
- (v) the existence of secondary damage and details thereof;
- (vi) the status of implementation of a response/notice to the data subjects;
- (vii) the status of implementation of a public announcement;
- (viii) measures to prevent recurrence; and
- (ix) other matters that may be helpful for the PPC.

The PPC issued the amended guidelines in light of the 2020 APPI amendments (the “**amended PPC GL**”) in August 2021.

According to the amended PPC GL, when a Data Breach or its possibility occurs, the business operator must take the following necessary measures, depending on the case:

- (i) internal reporting and damage prevention;
- (ii) investigation of the facts and the cause;
- (iii) specifying the scope of impact; and
- (iv) consideration and implementation of measures to prevent recurrence.

In addition, it is desirable to promptly disclose the relevant facts and measures to prevent recurrence, depending on the nature of the case.

The amended PPC GL interprets the phrase “possibility of Data Breach” as a case where the occurrence of a Data Breach is not known for certain but is suspected based on the facts known at the time.

Especially regarding cyberattacks, the following cases fall under the possibility of a Data Breach:

- (i) traces of data theft due to Unauthorised Access are found;
- (ii) confirmation of infection with malware that is known to behave in an information-stealing manner;
- (iii) communication with the command and control server is confirmed; and
- (iv) a business operator is informed by a security expert organisation that there is a possibility of a Data Breach based on certain grounds.

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

The Cybersecurity Management Guidelines recommend knowing who should be notified if a cyberattack 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).

Furthermore, 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.

However, under the Amended APPI, the business operator must notify the affected individuals of certain material Data Breaches (please see question 2.4).

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

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

The 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 that supervises the enforcement and application of the APPI.

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

Other than the report of a serious Incident under the TBA (please see question 2.4) and under the Amended APPI (please see questions 2.4 and 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. If a business operator does not report a serious Incident under the Amended APPI, the PPC may make recommendations or issue orders, and if the operator does not comply with a PPC order, it is subject to imprisonment of up to one year or a fine of up to JPY 1,000,000.

2.8 Enforcement: 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 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

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

Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of beacons is permissible so long as the use complies with the Guidelines and Applicable Laws.

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

Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of honeypots is permissible so long as the use complies with the Guidelines and Applicable Laws.

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

Applicable Laws do not differentiate between measures to detect and measures to deflect Incidents. Thus, the use of sinkholes is permissible so long as the use complies with the Guidelines and Applicable Laws.

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

As described in question 2.1, to prevent cyberattacks, the MIC issued reports that addressed whether a telecoms carrier may deal with cyberattacks and the issues that may arise in connection with the secrecy of communications, and the Council regarding the Stable Use of the Internet issued the Guidelines. These reports and the Guidelines cover policies regarding electronic communications on organisations' networks.

In addition, when a business operator monitors an employee's email or internet usage, monitoring may be considered illegal if the employees' Personal Information or privacy is not protected. The PPC recommends paying close attention to the following when conducting monitoring as part of employee supervision or personal data security management:

- (a) identifying the purpose of monitoring, specifying the purpose in internal regulations, and informing the employees of the purpose;
- (b) assigning a person responsible for monitoring and determining the authority of that person;
- (c) establishing rules regarding the implementation of monitoring and ensuring that the organisation complies with them; and
- (d) checking the adequacy of monitoring operations.

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

Under the FEFTA, encryption and intrusion program-related software and hardware are subject to export control regulations.

Regarding encryption, a cryptographic algorithm that meets certain requirements and any of the following three conditions is subject to export control regulations: (i) one main function is the security management of an information system; (ii) it constructs, manages, or operates a telecommunication line; and (iii) one main function is to record, store, and process information. However, there are many available exceptions. For example, hardware and software that use publicly known encryption technology or that secondarily use cryptographic functions are not subject to export control regulations.

Regarding intrusion program-related hardware or software (note that the intrusion program itself is not regulated), this

cannot be exported if it includes vulnerability information and malware information about the program. However, in order to reduce the impact on cybersecurity practice, exporting such a hardware or software for the purpose of disclosing security vulnerabilities or responding to cyberattacks is exempt from export control regulations.

4 Specific Sectors

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

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

The FSA issued in 2015, and updated in 2018, a summary of its policies to strengthen cybersecurity in the financial business sector. According to the updated summary, the FSA will continue to: (i) promote continuous dialogue with financial institutions to understand their cybersecurity risks; (ii) improve information sharing among financial institutions; (iii) implement cybersecurity exercises in which financial institutions, the FSA, and other public authorities participate; and (iv) develop cybersecurity human resources and also respond to new issues such as accelerated digitalisation and international discussions. The FSA's guidelines require banks to, among others, establish an organisation to handle emergencies (e.g., the CSIRT), designate a manager in charge of cybersecurity, prepare multi-layered defences against cyberattacks, and implement a periodic assessment of cybersecurity. The guidelines are not legally binding; however, because the FSA is a powerful regulator of the financial sector, banks would typically comply with the 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, the 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.

4.2 Excluding requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

Please see question 4.1.

5 Corporate Governance

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

Under 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 chuni 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.

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

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

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

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

There are no disclosure requirements that are specific to cybersecurity risks or Incidents, but the NISC recommends in its "Framework of Cybersecurity in Corporate Management", published on 2 August 2016, that companies should disclose their initiatives and policies for cybersecurity in their information security report, CSR report, sustainability report, annual report, or corporate governance report. The survey commissioned by the NISC published in March 2019 showed that cybersecurity risk is referred to in annual reports of 74% of the 225 listed companies included in the Nikkei 225, which is an equity index of Japanese blue-chip companies.

6 Litigation

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

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.

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

A vendor of a computer system was sued by a company that used the system provided by the vendor. The case related to

cyberattacks (SQL injections) to the system that resulted in the disclosure of credit card information of the company's clients. The company sought the payment of damages caused by the cyberattacks 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 that 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 23 January 2014).

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

Tort theory is available under the Civil Act of Japan (please see question 6.1).

7 Insurance

7.1 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.

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

There are no regulatory limitations on insurance coverage under the law. The coverage may differ depending on the insurance products of different insurance companies.

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 that are related to crimes under Applicable Laws. Under the current police system, the prefectural police are responsible for investigations and the National Police Agency is responsible for policy making and analysis. The National Police Agency plans to establish a new bureau dedicated to cybercrimes and a new unit that will investigate serious Incidents independently or jointly with the prefectural police in 2022.

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 is a partner at Mori Hamada & Matsumoto. Hiromi specialises in communications law and regulation and authored the Japanese section of *The Preston Gates Guide to Telecommunications in Asia* in 2005. Hiromi's other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. Hiromi was admitted to the Bar in Japan in 2001 and in New York in 2007. Hiromi worked at Mizuho Corporate Bank from 1989–1994 and was with Davis Polk & Wardwell in New York from 2006–2007.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Fax: +81 3 5220 1711
Email: hiromi.hayashi@mhm-global.com
URL: www.mhmjapan.com



Masaki Yukawa is counsel at Mori Hamada & Matsumoto. Masaki advises on cybersecurity issues for financial institutions, telecommunications businesses, and technology companies. Masaki was admitted to the Bar in Japan in 2009 and in California in 2016. Masaki worked at the Bank of Japan from 2003–2008 and was with the FSA from 2014–2015.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8764
Fax: +81 3 6266 8664
Email: masaki.yukawa@mhm-global.com
URL: www.mhmjapan.com



Daisuke Tsuta is an associate at Mori Hamada & Matsumoto. Daisuke specialises in cybersecurity and privacy laws. Daisuke was admitted to the Bar in Japan in 2010. Daisuke worked at the Kinki Local Finance Bureau of the Ministry of Finance from 2014–2015, at the MIC from 2015–2017, and at the NISC from 2017–2020.

Mori Hamada & Matsumoto
16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8769
Fax: +81 3 6266 8669
Email: daisuke.tsuta@mhm-global.com
URL: www.mhmjapan.com

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in other cities of Japan, and Bangkok, Beijing, Shanghai, Singapore, Yangon, and Ho Chi Minh. The firm has over 600 attorneys and a support staff of approximately 550, 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.

www.mhmjapan.com

MORI HAMADA & MATSUMOTO

ICLG.com



Current titles in the ICLG series

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