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:

Philippines

Leland R. Villadolid Jr.

Angara Abello Concepcion Regala & Cruz Law Offices

Arianne T. Ferrer

1 Criminal Activity

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

Hacking (i.e. unauthorised access)

Yes, hacking is a criminal offence under Republic Act No. 8792 or the Electronic Commerce Act ("ECA"). Hacking is defined as (1) unauthorised access of or interference with computer systems, servers, or other information and communication systems, (2) unauthorised access to corrupt, alter, steal, or destroy electronic data using computers or other information and communication systems without the computer or system owner's knowledge and consent, or (3) the introduction of computer viruses resulting in the corruption, alteration, theft, or loss of such data.

Hacking is punished by a maximum fine in an amount commensurate to the damage incurred. A mandatory penalty of imprisonment between six months and three years shall be meted out in either case.

Hacking, when it involves illegal access or interception, data interference, or system interference that affects the confidentiality, integrity, and availability of electronic data or computer systems, is also punished as a criminal offence under Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 ("CPA") by a maximum fine in an amount commensurate to the damage incurred. An additional penalty of imprisonment of six years and one day to 12 years (*prision mayor*) may also be imposed.

Criminal cases are pending prosecution before the courts.

Denial-of-service attacks

Yes, a denial-of-service attack ("DOS attack") is a criminal offence under the CPA because it involves system interference that affects the availability of electronic data or computer systems.

Criminal cases are pending prosecution before the courts.

Phishing

Yes, phishing is penalised under the CPA as an offence relating to computer-related forgery, fraud and/or identity theft. An attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication ("phishing"), is punishable by a maximum fine of PHP 200,000.00 and/or imprisonment of *prision mayor*.

Criminal cases are pending prosecution before the courts.

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

Yes, the infection of IT systems with malware is a criminal offence. It may be punished as hacking under the ECA or as an offence against the confidentiality, integrity and availability of computer data and systems under the CPA.

Under the ECA, the infection of IT systems with malware is punishable by a maximum fine in an amount commensurate to the damage incurred and imprisonment for a period of between six months and three years. Under the CPA, the same act is punishable by a maximum fine in an amount commensurate to the damage incurred and/or imprisonment of *prision mayor*. If the act is committed against critical infrastructure of the Philippines, the penalty is a maximum fine in an amount commensurate to the damage incurred and/or imprisonment for a period of between 12 years and 20 years and one day (*reclusion temporal*).

Criminal cases are pending prosecution before the courts.

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

Yes, the possession of cybercrime tools is a criminal offence. The possession of a device (including a computer program) that may be used to perpetrate any offence under the CPA, when coupled with the intent to use such device unlawfully, is punishable by a maximum fine of PHP 500,000.00 and/or imprisonment of *prision mayor*.

Criminal cases are pending prosecution before the courts.

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

Identity theft, when defined as the intentional acquisition, use, transfer, possession, alteration, or deletion of identifying information belonging to another natural or juridical person without right, is a criminal offence under the CPA. Identity theft is punishable by a maximum fine in an amount commensurate to the damage incurred and/or imprisonment of *prision mayor*.

The unauthorised or fraudulent use of an access device (any card, plate, code, account number, electronic serial number, personal identification number, telecommunications service, equipment or instrument, or other means of account access that may be used to obtain anything of value or to initiate a fund transfer) belonging to another natural person is prohibited under Republic Act No. 8484 or the Access Devices Regulation Act of 1998 ("ADRA"). It is punishable by a maximum fine of PHP 10,000.00 or twice the value obtained (whichever is greater) and imprisonment for a period of between six years and 10 years. If the perpetrator was previously convicted of another offence under the ADRA, the punishment is a maximum fine and/or imprisonment for a period of between 12

years and 20 years. Notably, "identity theft" or "identity fraud" is not expressly defined under the ADRA.

Criminal cases are pending prosecution before the courts.

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

Criminal copyright infringement is covered by Sections 177, 193, 203, 208 and 211 in relation to Section 217 of the Intellectual Property Code. The penalty for infringement of electronic data or through electronic means is one degree higher than imprisonment for a period of between one year and three years and a fine between PHP 50,000.00 and PHP 150,000.00.

Though a case that deals squarely with criminal copyright infringement of electronic data has yet to reach the Supreme Court, criminal copyright infringement was discussed in the context of a news video in *ABS-CBN Corporation v. Gozun*. In that case, the Supreme Court held that audio-visual work, like a news video, is protected from the moment of its creation, regardless of its "mode or form of expression". Accordingly, the unauthorised reproduction, distribution, or communication of audio-visual work through electronic means would be punishable as criminal copyright infringement.

One should note that Section 30 of the ECA limits a service provider's liability for criminal copyright infringement to instances when the service provider (1) had actual knowledge of the unlawful act, (2) received financial benefit from the unlawful act, and (3) did not directly commit or cause another person to commit the unlawful act. Unlawful acts include any activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data.

Offences against the confidentiality, integrity, and availability of electronic data and computer systems, e.g., illegal access, illegal interception, data interference, system interference, misuse of devices, and cyber-squatting, are punishable under the CPA. Except for misuse of devices, these offences are punishable by a maximum fine in an amount commensurate to the damage incurred or imprisonment of *prision mayor*. For an offence involving misuse of devices, the penalty is a maximum fine of PHP 500,000.00 and/or imprisonment of *prision mayor*.

Further, when these offences are committed by a natural person on behalf of a juridical person (provided that the natural person was authorised and acted within the scope of such authority), the juridical person shall be given a maximum fine of PHP 10,000,000.00.

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

The Philippine National Police Anti-Cybercrime Group ("PNP-ACG") regularly releases cybersecurity updates through issuances of security bulletins on its website, designed to raise public awareness of potential threats, vulnerabilities in their systems and information on better protection of their IT environment. Aside from these security bulletins, the PNP-ACG also updates its database to inform, educate and protect the public on cybercrime issues, internet frauds and scams and gives suggestions on how to address them.

Failure by an organisation to implement cybersecurity measures

Yes, a juridical person's failure to take appropriate measures to protect its computer systems, servers, or information and communication systems may be a criminal offence.

Under Republic Act No. 10173 or the Data Privacy Act of 2012 ("DPA"), a juridical person, who allowed a crime involving personal data to occur through fault or negligence, shall have its rights as a data subject suspended or revoked. The DPA's implementing rules and regulations state that failure to implement security measures for the protection of personal data may lead to civil and criminal liability.

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

Section 21 of the CPA gives Regional Trial Courts ("RTC") in the Philippines jurisdiction over cybercrimes committed by Filipino citizens, regardless of the place of commission.

Section 6 of the DPA provides for extraterritorial application over acts committed by Filipino citizens or entities with a link to the Philippines, e.g., entities that do business in the Philippines, collect or store personal information in the Philippines, or enter into contracts in the Philippines, as well as acts committed against Filipino citizens or residents.

For other laws defining and punishing offences involving cybersecurity that do not expressly provide for extraterritorial application, Article 14 of the Civil Code applies (penal laws only cover acts or omissions committed within Philippine territory, subject to customary or conventional international law).

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?

Applicable Laws do not provide actions that mitigate or absolve a perpetrator from criminal liability arising from cybersecurity offences. However, for offences punishable under the Revised Penal Code ("RPC") and committed with a cybercrime element, the rules on mitigating, justifying, and exempting circumstances found in Articles 11 through to 13 of the RPC apply.

Notably, notification is itself an obligation under the DPA, such that failure to notify the proper authority of an Incident may amount to a violation of the DPA.

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.

All crimes defined and punished under the RPC and special penal laws, when committed through information and communication systems and technology, shall be covered by the CPA. The general effect is that the penalties shall be increased one degree higher than the imposable penalties under the RPC and special penal laws.

Incidents can be considered terrorism when (1) they are performed to accomplish the following: piracy or mutiny; rebellion or insurrection; *coup d'état*; murder; kidnapping and serious illegal detention; and other crimes of destruction enumerated in Section 3 of Republic Act No. 9372 or the Human Security Act of 2007 ("HSA"), and (2) they cause widespread and extraordinary fear and panic among the public in order to coerce the government to give in to an unlawful demand.

2 Applicable Laws

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

The ECA, ADR, DPA, CPA, Republic Act No. 10844 or the Creation of the Department of Information and Communications Technology Act ("DICTA"), Republic Act No. 10627 or the Anti-Bullying Act ("ABA"), Republic Act No. 8293 as amended by Republic Act No. 10372 or the Intellectual Property Code ("IPC"), and their respective implementing rules and regulations.

Other laws, orders, rules, and regulations related to cybersecurity are: Supreme Court Administrative Matter No. 01-7-01-SC or the Rules on Electronic Evidence; Republic Act No. 10867 or the National Bureau of Investigation Reorganization and Modernization Act; Executive Order No. 189 or the Creation of the National Cyber-Security Inter-Agency Committee; and the HSA with respect to Sections 3 and 7.

On 19 February 2018, the Senate unanimously concurred on the ratification of the Budapest Convention on Cybercrime. The Budapest Convention seeks to pursue a common criminal policy aimed to protect society against cybercrime, harmonise procedural laws, improve investigative techniques and gathering of electronic evidence, and foster multilateral cooperation. The Philippines' accession to the Convention signifies the government's acknowledgment of cybercrime not only in a domestic setting but on an international level, and shows the country's resolve in addressing cybercrime as a major threat to national security.

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.

There is as yet no specific law enacted. However, the Department of Information and Communications Technology ("DICT") launched a national cybersecurity strategy framework that will ensure the protection of critical infrastructure from cyber attacks through effective coordination with law enforcement agencies. National Cybersecurity Plan 2022, which seeks to safeguard the ICT environment of the country through the establishment of a robust cybersecurity infrastructure, is intended to ensure the continuous operation of the country's critical infrastructure, public and military networks, to implement cyber-resiliency measures to enhance the ability to respond to threats before, during and after cyber attacks, and to implement a public awareness campaign on cybersecurity measures.

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

Under the DPA, a juridical person must take reasonable and appropriate organisational, physical and technical measures to protect personal information from unlawful destruction, alteration, disclosure, access, and other unlawful processing. These measures must include: (1) safeguards to protect the juridical person's computer network against use of or interference with the network's functionality or availability; (2) a security policy for processing personal information; (3) a process for identifying and accessing reasonably foreseeable vulnerabilities in the network and for taking preventive and corrective action against Incidents; (4) regular monitoring of Incidents; (5) the juridical person's personal information controller must ensure that third parties processing personal information on the juridical person's behalf will similarly take reasonable and appropriate measures; and (6) the juridical person's personal information controller must promptly notify the National Privacy Commission ("NPC") and affected data subjects when an Incident resulted in a security breach.

The DPA's implementing rules and regulations provide guidelines on measures to be taken by a juridical person dealing with personal information. They highlight the key principles for the protection of personal data: availability; integrity; and confidentiality.

The suggested organisational security measures are: (1) employing compliance officers or protection officers; (2) creating and implementing policies that take into account the nature, scope, context and purposes of the information processing, as well as the risks posed to the rights and freedoms of data subjects; (3) maintaining records that sufficiently describe the data processing system and identifying the duties and responsibilities of employees who have access to personal data; (4) ensuring that employees keep information confidential even after leaving their positions; (5) developing, implementing, and reviewing the procedure for personal data collection, access management, system monitoring, and protocols to be taken after Incidents occur as well as policies for the exercise of rights by data subjects, the retention of personal data, and the processing of information only for declared, specified, and legitimate purposes; and (6) ensuring that personal information processors take measures in accordance with the DPA.

The suggested physical security measures are: (1) implementing policies and procedures to monitor and limit access to facilities where electronic data can be used; (2) designing facilities to ensure privacy of personal information processors; (3) clearly defining duties, responsibilities, and schedules of personal information processors such that only those performing their official duties have access to electronic data at a given time; and (4) implementing policies and procedures to prevent mechanical destruction of files and equipment and to protect against natural disasters, power disturbances, external access, and other reasonably expected threats.

The suggested technical security measures are: (1) ensuring the ability to restore availability and access to personal data in a timely manner in the event of an Incident; (2) testing, assessing, and evaluating the effectiveness of security measures regularly; (3) encrypting personal data for storage and while in transit; and (4) implementing authentication processes and other technical security measures that control and limit access to information.

In determining whether a juridical person has taken reasonable and appropriate security measures, the NPC shall consider the nature of the personal data that requires protection, the risks posed by the processing, the size of the organisation and complexity of its operations, current data privacy best practices, and the cost of security implementation.

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 Supreme Court has yet to hear and resolve any conflict-of-laws specifically in relation to cybersecurity. The DPA does not cover personal information that was collected in a foreign jurisdiction in a manner that complies with Applicable Laws of that jurisdiction. However, security measures must still be undertaken when there is processing of personal information, regardless of the place of collection.

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.

A personal data breach is defined as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed". A personal data breach exists when (1) sensitive personal information that may be used to commit identity fraud is reasonably believed to have been acquired by an unauthorised person, and (2) the personal information controller believes that such acquisition poses a real risk of harm to the affected data subjects.

Under the DPA, the personal information controller must inform the NPC and affected data subjects within 72 hours of the former's knowledge or reasonable belief that a personal data breach has occurred.

On one hand, the notification to the affected data subjects should contain the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. It should also contain measures taken to reduce the harm or negative consequences of the breach, the contact details of representatives of the personal information controller so that data subjects can obtain additional information about the breach, and the assistance to be provided. On the other hand, the notification to the NPC should include the nature of the breach and the measures taken to remedy the breach but exclude any description of the personal privileged information.

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?

A juridical person processing personal information is not absolutely prohibited from sharing non-personal information related to Incidents by the DPA. On the other hand, personal information may be shared but with the consent of the affected data subject.

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.

A juridical person processing personal information is required to notify the affected data subjects in case of a personal data breach, in the same manner as discussed in question 2.5. The notification to the affected data subjects shall also contain instructions on how they may acquire more information on the breach.

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

No, once there has been a personal data breach, a juridical person, through its personal information controller, must notify the affected data subjects. The personal privileged information itself shall not be disclosed to any party, including the NPC, without the consent of the affected data subjects.

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

The regulator tasked to ensure compliance with the DPA is the NPC, which is an independent body mandated to administer and implement the DPA and to monitor and ensure the Philippines' compliance with international personal data protection standards. The NPC is attached to the DICT, though it performs its functions independently.

The NPC is a collegial body composed of one commissioner and two deputy commissioners. Its functions are: rule-making; advising; educating; compliance and monitoring; adjudicating complaints and investigations; and enforcing the DPA. Further, the NPC may issue official directives and administrative issuances, orders, and circulars that deal with procedural rules, schedules of administrative fines and penalties, and procedures for registration of data processing systems and notification.

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

The DPA does not expressly penalise the failure to adopt the suggested reasonable and appropriate measures or to submit the required notification, except with respect to persons found to have intentionally concealed the existence of a personal data breach despite knowing of the breach and the obligation to notify the NPC. In such case, concealment shall be punishable by imprisonment for a period of between one year and six months and five years as well as a fine of not less than PHP 500,000.00, but not more than PHP 1,000,000.00.

Additionally, persons who allow unauthorised access to personal data shall be punished by imprisonment ranging from one year to

three years and a fine of not less than PHP 500,000.00, but not more than PHP 2,000,000.00. Persons who allow unauthorised access to sensitive personal information shall be punished by imprisonment ranging from three years to six years and a fine of not less than PHP 500,000.00, but not more than PHP 4,000,000.00.

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

In January 2018, the NPC directed Globe Telecom, Inc., a leading provider of telecom services, to enforce more stringent subscriber verification protocols when one of its prepaid mobile customers fell victim to identity theft, which was perpetrated through unauthorised access to the customer's online banking account. This "SIM swap scheme" involves a perpetrator illegally obtaining a replacement SIM card from a telecom operator belonging to another and using the number for fraudulent activities. The *modus* involves the perpetrator posing as the owner of the number and claiming the original SIM card is stolen. In getting access to the mobile number, the perpetrator is able to access the owner's online banking and other personal accounts and use it in various transactions by exploiting the one-time password mobile authentication functions of the owner's registered mobile number.

Following this Incident, NPC directed Globe Telecom, Inc. to upgrade the latter's security procedures and tasked the telecom company to look into security gaps in its SIM replacement procedures. As a result, the latter committed to enforce a 24-hour delay in the activation of newly replaced SIM cards to subscribers who report either a lost or stolen phone, if the subscriber cannot present the original SIM bed or provide government-issued ID cards as proof of identification.

In March 2018, following the controversy wherein Aleksandr Kogan's personality quiz was installed by Facebook users and personal data was improperly shared with Cambridge Analytica, the NPC opened an investigation on Facebook to establish the scope and impact of the Incident on Filipino users and possible violations of the DPA. Notably, it was found that the Philippines was the second-most affected country in terms of data subjects. As a result, Facebook gave its plans to restrict data access of third parties on Facebook starting 9 April 2018, and in the process, users shall be notified if there was unauthorised processing of their personal data by Cambridge Analytica.

The NPC may compel government entities, agencies and instrumentalities to take specific actions to comply with the DPA. More generally, pursuant to its investigation of a complaint, adjudication of a dispute, or preparation of a report, the NPC may also issue cease-and-desist orders and impose a temporary or permanent ban on the processing of personal 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.

Applicable Laws on cybersecurity generally do not differ across different industries. However, under the DPA, the requirement to register processing operations and to notify the NPC of any changes to the automation of such processing operations only applies to a juridical person with 250 or more employees or with more than a *de minimis* amount of data subjects with sensitive personal information (at least 1,000 data subjects).

Meanwhile, under the ADRA, companies engaged in the business of issuing access devices (usually banks, financing companies, and other financial institutions) are required to report any fraudulent acts involving access devices that were committed in the previous calendar year to the Credit Card Association of the Philippines.

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?

The Bangko Sentral ng Pilipinas ("BSP") is the primary regulator of the financial services sector. The BSP issued BSP Circular No. 808 series of 2013 which provides guidelines on Information Technology Risk Management for all banks and BSP-supervised financial institutions ("BFSP"). The BSP is currently in the process of drafting a circular that would introduce amendments to Circular 808: incorporating the latest standards on information security; and presenting a more holistic information technology security management system integrated with the information security programs and risk management systems of banks. Other pertinent issuances of the BSP are: Circular No. 859 series of 2014, which requires banks and BFSPs to migrate from magnetic stripe technology to chip-enabled technology based on Europay, MasterCard and Visa ("EMV"); Circular No. 863 series of 2016, which are guidelines on the implementation of EMV Card Fraud Liability Shift Framework (banks and BFSPs that have not yet shifted to EMV technology shall be allowed subject to the condition that they will be held responsible for losses associated with the use of counterfeit cards in a card-present environment); and Circular No. 958 series of 2017, which are guidelines for banks and BFSPs in implementing multi-factor authentication as a replacement for single-factor authentication in their systems.

The DICT and the National Telecommunications Commission, which regulates the telecommunications sector, have yet to issue specific legal requirements relating to cybersecurity. However, the DICT recently launched a national cybersecurity strategy framework that will ensure the protection of critical infrastructure from cyber attacks through effective coordination with law enforcement agencies (National Cybersecurity Plan 2022).

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 CPA, if the commission of a punishable offence was made possible by the lack of supervision or control by a natural person with a leading position who acts individually or on behalf of a juridical person and said natural person has a power of representation or is otherwise authorised to make decisions and act on behalf of the juridical person, the juridical person shall be fined an amount of double the imposable fines under Section 7 or PHP 5,000,000.00 (whichever is higher).

Under the DPA, if a juridical person has committed a punishable offence, the responsible officers who participated in or allowed, through gross negligence, the offence to be committed may be prosecuted.

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?

Under the DPA, a Data Privacy Officer ("DPO") must be registered with the NPC if a company has more than 250 employees or the processing of personal information is: (1) likely to pose a risk to data subjects' rights and freedoms; (2) not occasional; or (3) involves sensitive personal information of at least 1,000 individuals. The application for registration shall include the name and address of the personal information controller or processor, the general description of privacy and security measures for data protection and copies of all policies relating to data governance, data privacy and information security.

Thus, the DPA does not specifically require the designation of a Chief Information Security Officer ("CISO"), only the designation of a DPO. However, with respect to (b), (c) and (d), while not specifically stated in the DPA, they may be deemed reasonable requirements to implement the objectives of the DPA.

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)?

Under the DPA, the NPC requires the annual submission of a summary of documented security Incidents and personal data breaches.

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

Yes. When ordered by a court to preserve or examine computer data, service providers (public or private entities that provide a service that allows users to communicate by means of a computer system, or any other entity that processes or stores computer data on behalf of users) are required to: (1) preserve the integrity of traffic data and subscriber information for a minimum period of six months from the date of the transaction; (2) preserve the integrity of content data for six months from the date of receipt of the order from law enforcement or competent authorities requiring its preservation; (3) preserve the integrity of computer data for an extended period of six months from the date of receipt of the order from law enforcement or competent authorities requiring extension on its preservation; (4) preserve the integrity of computer data until the final termination of the case and/or as ordered by the court, as the case may be; (5) ensure the confidentiality of the preservation order and its compliance; (6) collect or record by technical or electronic means and/or cooperate and assist law enforcement or competent authorities in the collection or recording of computer data covered by the court warrant; (7) disclose or submit users' information, traffic or relevant data to law enforcement or competent authorities within 72 hours from receipt of the court warrant; and (8) immediately and completely destroy the computer data that is the subject of a preservation order after the expiration of the period provided under the CPA.

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.

Civil actions involving Incidents may be brought before the proper court in two cases: (1) an action to demand the civil liability arising from a criminal offence under Article 30 of the Civil Code; and (2) an action to demand indemnification for damage to human relations under Articles 19 through to 21, 26 and 32 of the Civil Code.

Articles 19 through to 21 of the Civil Code are catch-all provisions to hold a person civilly liable for his injurious act or omission. Article 19 requires a person to act with justice, give everyone his due, and observe honesty and good faith. If a person wilfully or negligently causes damage to another person contrary to Article 19, he must indemnify the latter pursuant to Article 20. Similarly, a person who causes damage to another person contrary to morals, good customs, or public policy shall compensate the latter under Article 21.

Article 26 of the Civil Code requires a person to respect the dignity, personality, privacy and peace of mind of another person. Violating another person's privacy in relation to his residence under this provision and to his communication and correspondence under Article 32 of the Civil Code allows the offended party to recover damages.

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

The Supreme Court has yet to resolve a case involving civil and criminal actions arising from Incidents. It did, however, rule on the CPA's constitutionality in *Disini v. Secretary of Justice*. Before the lower courts, most cases with a cybersecurity element are criminal actions for computer hacking, child pornography, cybersex, ATM fraud and libel.

In 2016, the NPC issued a decision in NPC Case No. 16-001, which ruled that the COMELEC violated the DPA after the group Anonymous hacked the Philippines' voter registration database. The hack involved at least 75,302,683 voter records and 1,267 COMELEC employee records. The NPC found that the COMELEC Chairman wilfully and intentionally disregarded his duties as a personal information controller and recommended his prosecution under the CPA.

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

Yes. Incidents may lead to liability based on quasi-delict. Under Article 2176 of the Civil Code, a person whose act or omission injures another person, whether through fault or negligence, is liable to pay damages to the latter.

6 Insurance

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

Yes, with prior approval, the Insurance Commission ("IC") allows cyber-insurance products in the Philippines. Cyber-insurance may offer protection against losses due to: improper denial or approval

of access to data; breach of computer software, system or security; or theft of computer hardware, among others. Cyber-insurance may also include protection against extortion and loss as a result of an Incident and payment for an investigation to determine the source thereof. Thus, cyber-insurance may address loss resulting from cyber attacks, e.g., "Wannacry" ransomware.

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?

Generally, there are no regulatory limitations to insurance coverage against the types of losses mentioned above. However, exceptionally, the insured cannot recover amounts paid arising from damages, fines or penalties that are exemplary in nature. Likewise, there is no recovery for amounts paid arising from the insured's wilful and/or intentional violation of the DPA.

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?

Under the DPA, covered juridical persons must have systems and processes in place to make their employees aware of their responsibilities (ensuring integrity, availability and confidentiality of data) and the organisational requirements that must be met to comply with the DPA.

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?

Yes, Applicable Laws did not amend or repeal the Secrecy of Bank Deposits Act (Republic Act No. 1405), the Foreign Currency Deposits Act (Republic Act No. 6426), the Credit Information System Act (Republic Act No. 9510), and the Anti-Money Laundering Act (Republic Act No. 9610). Thus, these acts may prevent the reporting of Incidents to the proper authorities.

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.

Under Section 7 of the HSA, law enforcement authorities may listen to, intercept and record, with the use of any mode, form, kind or type of electronic or other surveillance equipment or intercepting and tracking devices, or with the use of any other suitable ways and means for that purpose, any communication, message, conversation, discussion, or spoken or written words between members of a judicially declared and outlawed terrorist organisation, association, or group of persons or of any person charged with or suspected of the crime of terrorism or conspiracy to commit terrorism, upon written order of the Court of Appeals. However, Section 7 is limited by Section 44 of the DPA, which requires law enforcement authorities to comply with the principles of transparency, proportionality, and legitimate purpose.

Under the CPA, the National Bureau of Investigation ("NBI") and the PNP Cybercrime Unit are responsible for enforcement. They are authorised to collect traffic data in real time, with due cause as evidenced by a court warrant. They may also issue an order requiring any person or service provider to disclose relevant information or data in his possession and control within 72 hours from receipt, also after securing a court warrant.

The NBI and the PNP may perform the following, upon securing a search and seizure warrant and within the time period provided therein: (1) secure a computer system or a computer data storage medium; (2) make and retain a copy of computer data secured; (3) maintain the integrity of the relevant stored computer data; (4) conduct forensic analysis or examination of the computer data storage medium; and (5) render inaccessible or remove computer data in the accessed computer or network. Further, they may order any person, who has knowledge of the computer system, server, or information and communication system and the measures to protect and preserve the electronic data therein, to assist in the search and seizure.

When computer data is found to *prima facie* violate the CPA, the Department of Justice may issue an order to restrict or block access to the data.

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, juridical persons are not required to leave backdoors in their information and communication systems or to give law enforcement officers encryption keys.

Acknowledgment

The authors would like to thank Aileen P. Cruz, Associate of the Litigation & Dispute Resolution Department, for her invaluable assistance in the preparation of this chapter.

Tel: +632 830 8329 / Email: apcruz@accralaw.com

Leland R. Villadolid Jr.
Angara Abello Concepcion Regala & Cruz Law Offices
ACCRALAW Tower
Second Avenue Corner 30th Street
Crescent Park West
Bonifacio Global City, 1635 Taguig, NCR
Philippines

Tel: +632 830 8131
Email: lrvilladolid@accralaw.com
URL: www.accralaw.com

Mr. Villadolid is a Senior Partner of the Litigation & Dispute Resolution Department. He obtained his Bachelor of Laws from the Ateneo de Manila University. He also holds a Bachelor of Arts in Philosophy from the University of the Philippines. His postgraduate education includes a Master of Laws from the George Washington University and training at the Environmental Law Institute in Washington, D.C.

Mr. Villadolid is a consultant of the following: Information Security Officers Group (ISOG); and the Philippine National Police Anti-Cybercrime Group (PNP-ACG) Advisory Council. He is also a member of the Philippine Dispute Resolution Center, Inc. (PDRCI) and Forum for International Irregular Network Access (FIINA). Finally, Mr. Villadolid serves as a Commissioner in the Commission on Bar Discipline of the Integrated Bar of the Philippines (IBP).

Mr. Villadolid handles cases involving litigation and/or arbitration on information communication and technology, cybercrimes, public utilities, antitrust and trade regulation and white-collar crimes.

Arianne T. Ferrer
Angara Abello Concepcion Regala & Cruz Law Offices
ACCRALAW Tower
Second Avenue Corner 30th Street
Crescent Park West
Bonifacio Global City, 1635 Taguig, NCR
Philippines

Tel: +632 830 8329
Email: atferrer@accralaw.com
URL: www.accralaw.com

Ms. Ferrer is an Associate of the Litigation & Dispute Resolution Department. She obtained a *Juris Doctor* degree from the University of the Philippines College of Law in 2015 and a Bachelor of Science degree in Business Economics from the University of the Philippines, where she graduated *cum laude* in 2010. While at law school, Ms. Ferrer served as an editor of the *Philippine Law Journal* and represented the Philippines in the Philip C. Jessup International Law Moot Court Competition.

Ms. Ferrer was admitted to the Philippine Bar in 2016. Since then, she has handled litigation, alternative dispute resolution, and arbitration cases involving civil and commercial disputes. Ms. Ferrer has acted as an administrative secretary in arbitration proceedings before the International Commercial Court and the Philippine Construction Industry Arbitration Commission.

ACCRALAW®

ANGARA ABELLO CONCEPCION REGALA & CRUZ ("ACCRALAW") is a multi-disciplinary team of legal professionals with in-depth knowledge in specialised fields of law. Seven practice departments in three regions offer timely, creative, and strategic legal solutions matched with cost-efficient administration and expert handling of client requirements.

ACCRALAW is the undisputed leader in Philippine litigation and alternative dispute resolution ("ADR"). With a deep bench of litigators and ADR practitioners and a consistent, outstanding track record covering more than 40 years, ACCRALAW has extensive expertise in handling large-scale and complex disputes. Its trial experience before courts, tribunals, administrative agencies, and ADR fora is unmatched. ACCRALAW has contributed to Philippine jurisprudence by successfully representing clients in landmark legal controversies.

ACCRALAW's pre-eminence in litigation and ADR is due to the structured, hands-on training of its junior lawyers, who are among the top graduates in the Philippines, and the wide areas of expertise and the varied experience of its senior lawyers. Most ACCRALAW lawyers have completed postgraduate studies abroad, while others are faculty members of the best law schools. ACCRALAW lawyers have been commissioned by the Supreme Court to revise the Rules of Court and draft other rules in connection with the practice of law.

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