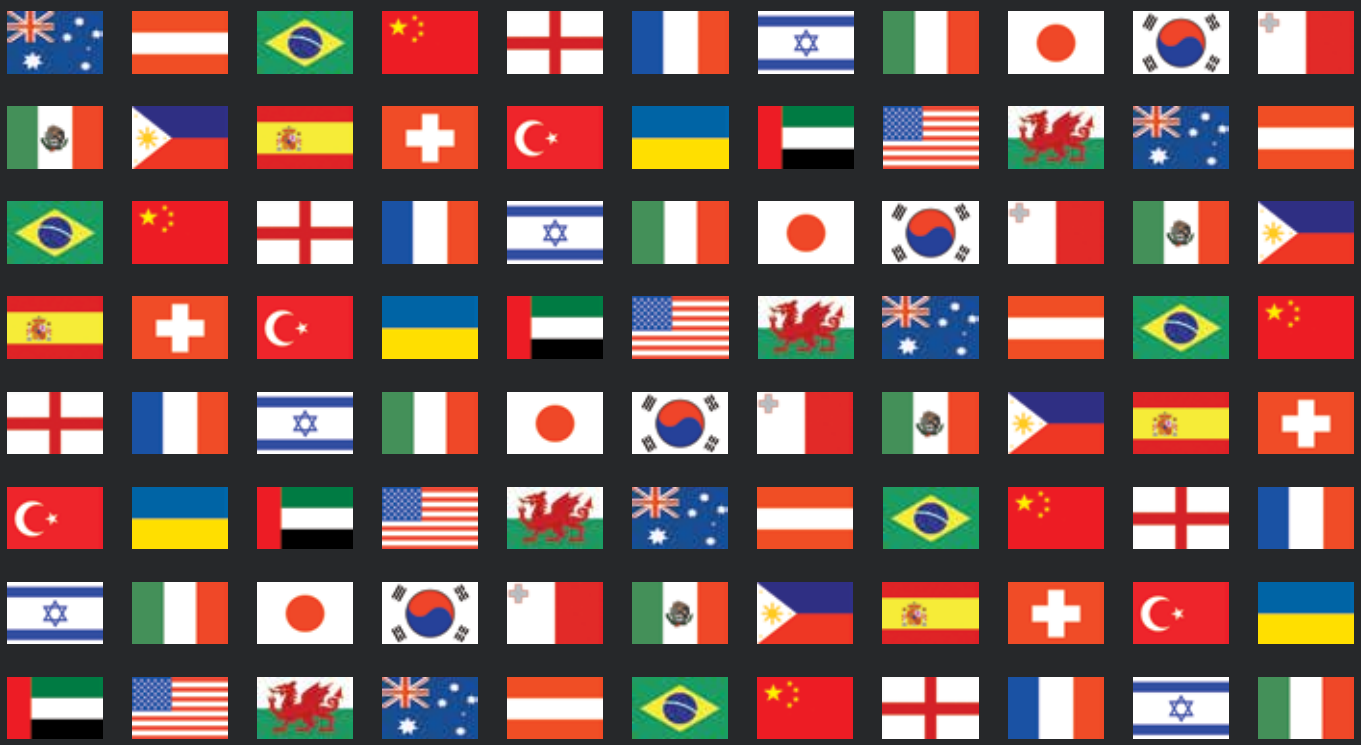
Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman



2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2018

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in January 2018
For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

First published 2015
Fourth edition
ISBN 978-1-912377-38-1

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Preface

Cybersecurity 2018

Fourth edition

Getting the Deal Through is delighted to publish the fourth edition of *Cybersecurity*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Australia, Italy, Philippines, Spain, Turkey and Ukraine.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
January 2018

Philippines

Rose Marie M King-Dominguez and Ruben P Acebedo II

SyCip Salazar Hernandez & Gatmaitan

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The Cybercrime Prevention Act of 2012 (CPA) defines the following as cybercrimes:

- offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices and cybersquatting);
- computer-related offences (computer-related forgery, computer-related fraud and computer-related identity theft); and
- content-related offences (cybersex, child pornography, unsolicited commercial communications and libel).

The CPA appointed the National Bureau of Investigation (NBI) and Philippine National Police (PNP) as enforcement authorities and regulates their access to computer data, creating the Cybercrime Investigation and Coordinating Center (CICC) as an inter-agency body for policy coordination and enforcement of the national cybersecurity plan, and an Office of Cybercrime within the Department of Justice (DOJ-OC) for international mutual assistance and extradition.

The Electronic Commerce Act of 2000 (ECA) provides for the legal recognition of electronic documents, messages and signatures for commerce, transactions in government and evidence in legal proceedings. The ECA penalises hacking and piracy of protected material, electronic signature or copyrighted works, limits the liability of service providers that merely provide access, and prohibits persons who obtain access to any electronic key, document or information from sharing them. The ECA also expressly allows parties to choose their type or level of electronic data security and suitable technological methods, subject to the Department of Trade and Industry guidelines.

The Access Devices Regulation Act of 1998 (ADRA) penalises various acts of access device fraud such as using counterfeit access devices. An access device is any card, plate, code, account number, electronic serial number, personal identification number or other telecommunications service, equipment or instrumental identifier, or other means of account access that can be used to obtain money, goods, services or any other thing of value, or to initiate a transfer of funds. Banks, financing companies and other financial institutions issuing access devices must submit annual reports of access device frauds to the Credit Card Association of the Philippines, which forwards the reports to the NBI.

The Data Privacy Act of 2012 (DPA): regulates the collection and processing of personal information in the Philippines and of Filipinos, including sensitive personal information in government; creates the National Privacy Commission (NPC) as regulatory authority; requires personal information controllers to (i) implement reasonable and appropriate measures to protect personal information and (ii) notify the NPC and affected data subjects of breaches; and penalises unauthorised processing, access due to negligence, improper disposal, processing for unauthorised purposes, unauthorised access or intentional breach, concealment of security breaches, and malicious or unauthorised disclosure in connection with personal information.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Enterprises heavily involved in collecting and handling personal data and electronic or online data would likely be the most affected. A good proxy for a 'most affected sectors' list are those sectors subjected to mandatory registration with the NPC: business process outsourcing (BPO), banks and financial institutions, insurance, telecommunications and internet service companies, education, healthcare and pharmaceuticals, businesses involved in direct marketing and networking, and government agencies.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The Department of Information and Communications Technology (DICT) Memorandum Circular No. 5 (2017) requires government agencies to adopt the Code of Practice in the Philippine National Standard (PNS) ISO/IEC 27002 (Information Technology – Security Techniques – Code of Practice for Information Security Controls) by 14 September 2018, and Critical Information Infrastructures (CII) to implement the PNS on Information Security Management System ISO/IEC 27001 by 14 September 2019. CII sectors include the government, transportation, energy, water, health, emergency services, banking and finance, business process outsourcing, telecommunications, and media. Non-CII sectors may voluntarily adopt PNS ISO/IEC 27002. DICT conducts risk and vulnerability assessment based on ISO 27000 and ISO 31000 and security assessment based on ISO/IEC TR 19791:2010 of CIIs at least once a year. The DICT also issues a Certificate of CyberSecurity Compliance to CIIs based on ISO/IEC 15408 (Information Technology – Security Techniques – Evaluation Criteria for IT Security) and ISO/IEC 18045 (Methodology for IT Security Evaluation).

In prescribing the government's Cloud First Policy, DICT Circular No. 2017-002 includes ISO/IEC 27001 as an accepted international security assurance control for verifying data that can be migrated to GovCloud or the public cloud, and ISO/IEC 17203:2011 Open Virtualization Format specification as a standard for interoperability of GovCloud workloads.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The specific obligation to keep informed of the adequacy of cybersecurity results from general obligations. Under the DPA, the employees, agents or representatives of a personal information controller who are involved in the processing of personal information are required to operate and hold personal information under strict confidentiality if the personal information is not intended for public disclosure, even after leaving the public service, transfer to another position or upon termination of employment or contractual relations. Also, diligence in preventing the commission of offences under the DPA are required of responsible company officers. If they participated in, or by gross negligence, allowed the commission of an offence, they may be penalised by a fine and imprisonment.

The CPA requires persons with leading positions in a corporation who act or decide on its behalf to exercise sufficient supervision or

control within the corporation to prevent cybercrime offences. If they fail this duty, then the corporation may suffer a fine and hold them responsible under the corporation's internal rules.

The Central Bank of the Philippines (BSP) Manual of Regulations for Banks requires directors of BSP-supervised institutions (BSI) to understand the BSI's IT risks and ensure that they are properly managed. BSIs include banks, non-banks with quasi-banking functions, non-bank electronic money issuers and other non-bank institutions subject to the BSP's supervision.

5 How does your jurisdiction define cybersecurity and cybercrime?

The CPA defines 'cybercrime' as those offences listed in question 1, while it defines 'cybersecurity' as the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets, where 'cyber' refers to a computer or a computer network, the electronic medium in which online communication takes place.

'Data privacy' is a DPA term that refers to personal information only as data. Thus, cybersecurity covers other kinds of data but data privacy covers environments other than cyber.

There are no regulations specific to 'information system security' that may be compared with cybercrime enforcement.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The DPA requires personal information controllers and their processors to include in their reasonable and appropriate organisational, physical and technical security measures against accidental or unlawful processing and natural or human dangers:

- safeguards to protect its computer network against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability;
- a security policy with respect to the processing of personal information; and
- a process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

The NPC requires all digitally processed personal data to be encrypted, preferably with AES-256, and passwords to be enforced through a policy and a system management tool. For on-site and online access by government agency or contractor personnel to sensitive personal information, the DPA requires security clearance from the head of the source agency, a secure encrypted link for access and multifactor authentication of identity, and middleware for full control over the access. For off-site access, the agency head must approve within two business days from request for, at most, 1,000 records at a time, and the most secure encryption standard recognised by NPC is used. Agencies must use full-disk encryption when storing personal data in laptops and send passwords on a separate email.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The ECA penalises piracy or the unauthorised copying, reproduction, dissemination, or distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public or broadcasting of protected material, electronic signature or copyrighted works, including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights, with a fine and imprisonment.

The CPA penalises cybersquatting or the acquisition of a domain name over the internet in bad faith to profit from, mislead, destroy the reputation of and deprive others from registering the same if such a domain name is:

- similar, identical or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
- identical or in any way similar to the name of a person other than the registrant, in the case of a personal name; and
- acquired without right or with intellectual property interests in it.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The CPA imposes a stiffer fine and prison term for offences against the confidentiality, integrity and availability of computer data systems if done against critical infrastructure. This refers to the computer systems, networks, programs, computer data and traffic data vital to the Philippines, whose destruction, incapacitation or interference with would have a debilitating impact on national or economic security, national public health and safety, or any combination of these.

DICT Memorandum Circular No. 5 (2017) prescribes policies and rules on CII protection based on the National Cybersecurity Plan 2022 (NCP2022). Aside from requiring compliance with international standards, the Circular requires each CII to have a Computer Emergency Response Team (CERT), which shall report cybersecurity incidents within 24 hours from detection to DICT as the National CERT, telecommunications operators and ISPs to conduct cyber hygiene on their networks, CII websites to obtain a DICT seal of cybersecurity, covered organisations to implement a disaster recovery plan and business continuity plan, and DICT to conduct annual CII cyber drills.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Under Philippine law, unauthorised access to or interception of communications is generally viewed as a violation of a citizen's constitutional right to privacy of communication and correspondence. It is illegal unless authorised by a lawful order of the court, or when public safety or order require otherwise. Data or any evidence obtained in violation of this right is inadmissible for any purpose or in any proceeding. This basic framework is reflected in statutes authorising the interception of messages.

The CPA prohibits interception by technical means without right to any non-public transmission, requiring a search and seizure court warrant for computer data to enable law enforcement authorities to collect or record traffic or non-traffic data in real time within the period stated in the warrant. The DPA penalises unauthorised processing, access and disclosure of personal information. The ECA penalises hacking, or the unauthorised access into or interference in a computer system or server, or information and communication system. Under Republic Act No. 4200, the Anti-Wiretapping Law, it is unlawful for any person, not being authorised by all the parties to any communication or spoken word, to tap any wire or cable, or use any other device, to secretly overhear, intercept or record such communication or speech; but court-authorised police may record communication or speech in cases involving crimes against national security, public order and kidnapping. The Human Security Act of 2007 allows court-authorised police surveillance of telecommunications messages to or from suspected terrorists. The Anti-Child Pornography Act of 2009 prohibits ISPs from monitoring any user, subscriber or customer, or the content of its communication.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

Question 1 describes the CPA cybercrimes and offences under the DPA, ECA and ADRA that may cover cyberactivities relevant to organisations as they may either be committed by organisations or committed against organisations (as possible targets).

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

They are mainly addressed through a general cybersecurity framework, regulations specific to the banking and government sectors, and participation in cybersecurity initiatives as a member of the International Telecommunications Union.

The BSP conditions the prior approval of a BSFI's use of cloud services on the conduct of due dilgence on the cloud service provider (CSP), the service's compliance with data security, confidentiality and

Update and trends

Since Philippine cybersecurity laws are relatively new, the lack of awareness about the need for cybersecurity and the relevant laws and regulations is the principal challenge for authorities. The NCP2022 will dictate the changes in policies and regulations over the next few years. Collaboration with the government by private companies on rule-making and compliance should encourage a favourable regulatory environment.

disaster recovery requirements, and mandatory provisions in the service contract. The BSP's 2017 Enhanced Guidelines on Information Security Management also requires BSFI management to 'fully understand the nature of the cloud technology in line with business requirements and satisfy themselves as to the level of security and compliance to data privacy and other relevant rules and regulations', and to oversee the cloud service provider's 'adherence to security, performance and uptime, and back-up and recovery arrangements contained in the contract/agreement.'

DICT Department Circular No. 2017-002 regulates the security of government-contracted cloud services with: data migration through international security assurance controls and industry-accepted encryption; baseline and optional security controls for CSPs to host classes of government data; and logical security audit on data access and continuous security monitoring to ensure data confidentiality, integrity and availability.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The regulatory obligations for domestic and foreign organisations doing business in the Philippines are the same.

Also, the DPA applies extraterritorially on an organisation's acts or practices outside of the Philippines if:

- the act, practice or process relates to personal information about a Philippine citizen or a resident;
- the organisation has a link with the Philippines; and
- the organisation is processing personal information in the Philippines, or even if the processing is outside the Philippines, as long as it is about Philippine citizens or residents.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As mentioned in question 1, the DICT recommends optional security controls for CSPs to host classes of government data. With respect to government agencies that process the personal data records of more than 1,000 individuals, the NPC recommends the use of ISO/IEC 27002 as the minimum standard to assess any gaps in the agency's control framework for data protection.

14 How does the government incentivise organisations to improve their cybersecurity?

Under the NCP2022, the DICT aims to raise the business sector's awareness of cyber risks, security measures, and possible public–private partnership on improving cybersecurity. The government has yet to especially incentivise organisations to improve their cybersecurity.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

See question 3.

16 Are there generally recommended best practices and procedures for responding to breaches?

NPC Circular No. 16-03 provides guidelines for personal data breach management, requiring organisations to implement a security incident management policy to ensure:

- the creation of a data breach response team, which will be responsible for implementing the policy;
- implementation of organisational, physical and technical security measures, and of policies to prevent or minimise personal data breaches and assure timely discovery of the same;
- implementation of an incident response procedure;
- mitigation of negative consequences to data subjects; and
- compliance with all laws and regulations on data privacy.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The DPA requires personal information controllers to report security breaches and intrusion attempts to the NPC. The NCP2022 aims to use the reports to develop cybersecurity measures and to promote the sharing of information between the government and private sector.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The DICT is creating technical working groups to review existing and develop new cybersecurity courses in order to integrate these courses into the curriculum of engineering, computer science, information technology, law and criminology. The National Cybersecurity Plan 2022 includes establishing and creating programmes among CERTs, law enforcement, academia and industries as one of the government's key initiatives.

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Only three insurance companies offer insurance for data security breaches, network interruption and cyber extortion as well as fines resulting from breach of administrative obligations relative to cybersecurity.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The NBI Cybercrime Division, PNP Anti-Cybercrime Group, DOJ-OC, CICC and NPC enforce various rules related to cybersecurity.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The CPA authorises the NBI Cybercrime Division and PNP Anti-Cybercrime Group to investigate cybercrimes. The DOJ prosecutes cybercrimes and its DOJ-OC coordinates international mutual assistance and extradition. The CICC CERT provides assistance to suppress real time commission of cybercrimes and facilitates international cooperation on intelligence, investigations, suppression and prosecution. Law enforcement authorities may collect or record traffic or non-traffic data in real time upon being authorised by a court warrant.

The NPC (i) enforces, monitors compliance of government and private entities with, and investigates and recommends to the DOJ the prosecution of violations under the DPA; (ii) facilitates cross-border enforcement of data privacy protection; and (iii) can issue cease-and-desist orders, or impose a temporary or permanent ban on the processing of personal information upon finding that the processing will be detrimental to national security or public interest, or both.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The NCP2022 describes the cybersecurity maturity level of the Philippines as 'reactive and manual', meaning the primary concern of regulators is to 'put out fires as opposed to finding the fire and preventing the fire from spreading'.

Recent incidents of cybersecurity breaches in the private sector indicate the government's current policy of supporting the private sector in identifying attacks and securing their systems, instead of punishing security breaches. Account holders in one of the Philippines' largest banks experienced changes in their account balances as a result of transactions that were neither authorised nor initiated by the account holders. This led the bank to suspend its online banking and ATM services, which inconvenienced millions of their clients and, to some extent, caused panic among the public. While the bank denied

allegations of a breach of security or data, citing alleged 'technical glitches' as the cause of the changes in the account balances of their client, the NPC treated it as security incident as it involved personal data of the bank's clients. The NPC conducted a privacy compliance check on the bank's systems and processes, particularly on the bank's breach management protocol, to prevent or mitigate similar incidents in the future. The NPC, however, has yet to release a report regarding the compliance check or issue a statement regarding any possible sanction against the bank for the incident. In another case, a potential system breach that may have involved personal information of clients of a leading online brokerage firm in the Philippines was reported to the NPC. In its response, the NPC issued a statement noting the need for 'personal data breach management' rules and informed the public that it was monitoring the incident. There are no reports yet regarding possible sanctions against the online brokerage firm for the data breach.

The NCP2022 sets out the following key programme areas:

- the protection of CII through cybersecurity assessment and compliance, national cyber drills and exercises, and a national database for monitoring and reporting;
- the protection of government networks through a national computer emergency response program, a capacity building and capability development programme, a pool of information security and cybersecurity experts, the Threat Intelligence and Analysis Operations Center, protection of electronic government transactions, and the update of licensed software;
- the protection for supply chain through a national common criteria evaluation and certification programme; and
- the protection of individuals through the acceleration of learning skills and development, a cybersecurity outreach project, a national cybersecurity awareness month, equipping the government and programmes for local and international cooperation.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

In general, the penalties consist of fines and imprisonment.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

BSIs that fail to report breaches in information security, especially incidents involving the use of electronic channels, may be penalised with fines, suspension of the BSI's privileges or access to the Central Bank's credit facilities, as well as revocation of a quasi-banking licence. Internet service providers and internet hosts that fail to promptly report child pornography to police authorities may be penalised with fines and imprisonment. As to breaches related to personal information, the NPC has yet to provide penalties specific to the failure to report.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The DPA entitles data subjects the right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorised use of personal information. Claims for indemnity may be filed with the NPC.

Parties may provide for redress in a contract and claim damages for breach of contract. Philippine tort law allows claims for damages resulting from acts or omissions involving negligence or those involving violations by private entities or individuals of the constitutional rights of other private individuals. Claims may be filed in court or through alternative dispute resolution mechanisms.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

A CERT that will respond to cyberattacks is required of every bureau, office, agency and instrumentality of the government.

For personal data protection, the NPC requires organisations to create a security incident management policy, which shall include:

- conduct of a privacy impact assessment to identify attendant risks in the processing of personal data, which should take into account the size and sensitivity of the personal data being processed, and impact and likely harm of a personal data breach;
- a data governance policy that ensures adherence to the principles of transparency, legitimate purpose and proportionality;
- the implementation of appropriate security measures, which protect the availability, integrity and confidentiality of personal data being processed;
- regular monitoring for security breaches and vulnerability scanning of computer networks;
- capacity building of personnel to ensure knowledge of data breach management principles and internal procedures for responding to security incidents; and
- a procedure for the regular review of policies and procedures, including the testing, assessment and evaluation of the effectiveness of the security measures.

Security measures are required to ensure the availability, integrity, and confidentiality of the personal data being processed, such as implementation of backup solutions; access control and secure log files; encryption; data disposal and return-of-assets policy.

SyCip Salazar Hernandez & Gatmaitan

Rose Marie M King-Dominguez **rmmking@syciplaw.com**
Ruben P Acebedo II **rpacebedo@syciplaw.com**

SyCip Law Center
105 Paseo de Roxas
Makati City, 1226
Philippines

Tel: +632 982 3500 / 3600 / 3700
Fax: +632 817 3896 / 818 7562
www.syciplaw.com

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

The NPC requires all actions taken by a personal information controller or personal information processor to be properly documented by the designated data protection officer, should a personal data breach occur.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

BSIs must report breaches in information security, especially incidents involving the use of electronic channels. Depending on the nature and seriousness of the incident, the BSP may require the BSI to provide further information or updates on the reported incident until the matter is finally resolved.

The Anti-Child Pornography Act requires internet service providers and internet hosts to notify the police authorities when a violation is being committed using its server or facility and preserve evidence of such violation.

The DPA requires personal data breach notification to the NPC.

29 What is the timeline for reporting to the authorities?

BSIs must submit reports to the BSP within 10 days of knowledge of the breach in information security. Companies engaged in the business of issuing access devices must submit an annual report to the Credit Card Association of the Philippines about access device frauds. Internet service providers and internet hosts must report any form of child pornography in their system to the police authorities within seven days of discovery. The NPC must be notified within 72 hours upon knowledge of, or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Apart from the personal data breach notification to the data subject required by the NPC, there are no rules for reporting threats or breaches.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-912377-38-1