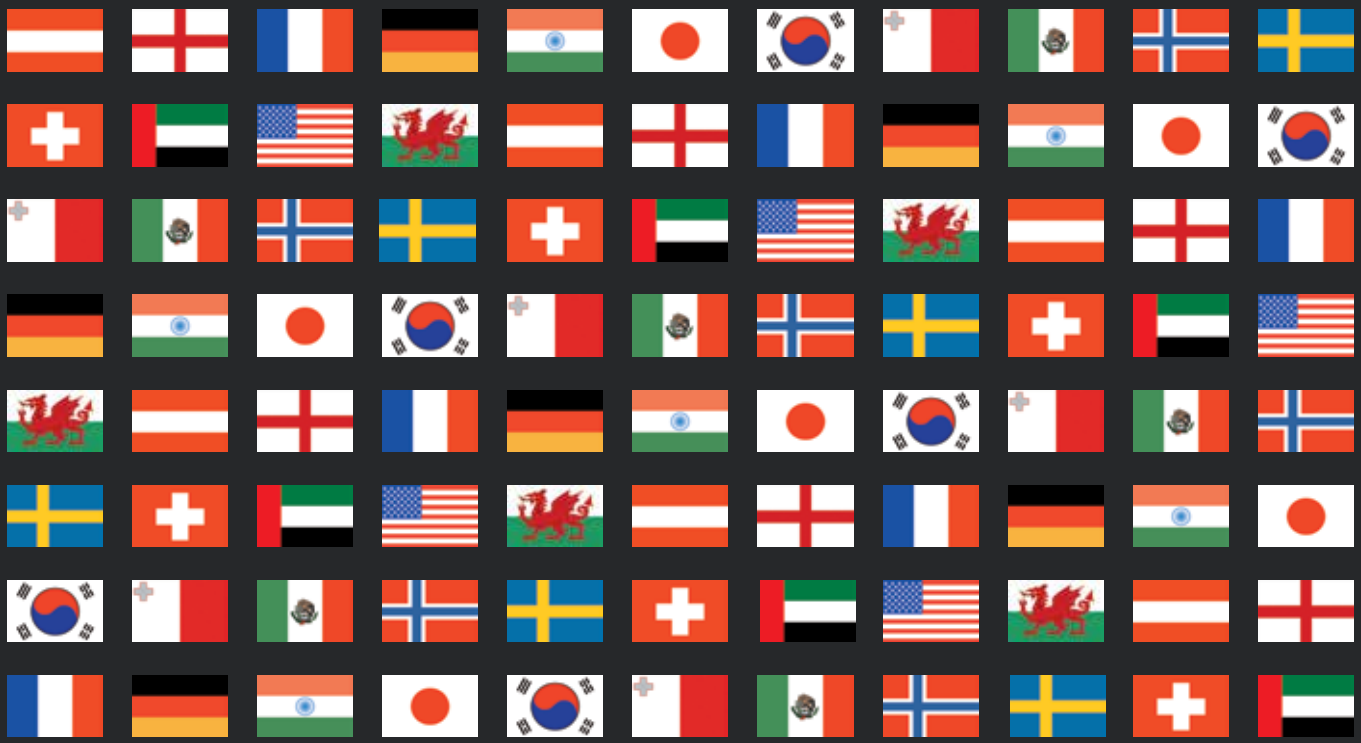
Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman



2016

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2016

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2015
Second edition
ISSN 2056-7685

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

CONTENTS

India

Salman Waris

TechLegis, Advocates & Solicitors

Legal framework

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

India does not have dedicated cyberlaws for the promotion of cybersecurity. However, the cybersecurity regulations are enshrined under the Information Technology Act, 2000 as amended from time to time (IT Act).

The IT Act and the rules framed under it embody the principles and rules governing cybersecurity. The following rules under the IT Act have a bearing on cybersecurity:

- the Information Technology (Security Procedure) Rules, 2004;
- the Information Technology (Procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009;
- the Information Technology (Procedure and safeguards for blocking for access of information by public) Rules, 2009;
- the Information Technology (Procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009;
- the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011;
- the Information Technology (Intermediaries guidelines) Rules, 2011;
- the Information Technology (Guidelines for Cyber Cafe) Rules, 2011;
- the Information Technology (Electronic Services Delivery) Rules, 2011; and
- the National Cyber Security Policy, 2013.

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

The industry sectors most affected by the cybersecurity laws and regulation in India are information technology (IT), information technology enabled services, software and services, banking, e-commerce, health care including telemedicine and mobile clinics, financial services including mobile banking and payment gateways, and social media. These sectors are directly affected by acts concerning cyberlaws and security.

There have been drastic steps initiated towards the implementation of cybersecurity for these activities, such as implementation of secure payment gateways, use of secure encryption standards, etc. The Reserve Bank of India and the Securities and Exchange Board of India have prescribed standards for secure financial transactions in the country.

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

International standards pertaining to cybersecurity have been incorporated and prescribed under the IT Act and the rules thereunder.

In this regard, the International Standard ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements' has been prescribed by rule 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 for security practices and procedures.

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?

Responsibility of the personnel and directors of a company has been set out in provisions of section 85 of the IT Act, where such company acts in violation of the provisions of the IT Act or the rules thereunder.

At the time the contravention was committed, every person who was in charge of and was responsible for the conduct of business of the company, as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Where a contravention of any of the provisions of the IT Act or of any rule, direction or order made thereunder has been committed by a company and it is proven that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

5 How does your jurisdiction define cybersecurity and cybercrime?

'Cybersecurity' has been defined under section 2(nb) of the IT Act and means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

'Cyber incidents' have been defined under rule 2(d) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 as any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource or processing or storage of information or changes to data or information without authorisation.

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

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 impose strict conditions for the collection, transfer and disclosure of 'sensitive personal data or information'. The Rules also prescribe the situations and modes wherein 'sensitive personal data or information' can be collected, transferred or disclosed. Conditions such as prior consent, collection and use for a lawful purpose or activity and retention, disclosure and transfer only to such extent as required have been imposed with regard to the data falling within the category of 'sensitive personal data or information'. Any body corporate handling sensitive personal data or information is obligated to implement and maintain reasonable security practices and procedures.

The IT Act defines an 'intermediary' under section 2, as any person, with respect to any particular electronic record, who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record. An intermediary includes telecoms service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online marketplaces and cybercafes, etc.

Additionally, the Information Technology (Intermediaries Guidelines) Rules, 2011 stipulates that all entities covered within the definition of intermediary and performing functions thereof are obligated to observe due diligence while discharging its duties as an intermediary.

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

There are no specific regulations concerning cyberthreats to intellectual property. However, the Trade Marks Act, 1999 provides for protection against the infringement of trademarks and the Copyrights Act, 1957 provides for protection against the infringement of copyright. The said legislation generally covers and protects against all acts of infringement. The Indian courts have judicially extended the principles of the legislation to include infringement that occurs in the cyberworld as well.

The Information Technology (Intermediaries Guidelines) Rules, 2011 provides that the intermediaries, as defined under the IT Act, are required to ensure they do not host, display, upload, modify, publish, transmit, update or share any information that infringes any patent, trademark, copyright or other proprietary rights.

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

The Information Technology (National critical information infrastructure protection centre and manner of performing functions and duties) Rules, 2013, issued on 16 January 2014 under the provisions of section 70A of the IT Act, specifically deals with the critical information infrastructure.

'Critical information infrastructure' has been defined by the IT Act as such computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety.

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

While there is no specific law restricting the sharing of cyberthreat information there is, however, section 66 E of the amended IT Act, which deals with issues relating to violation of privacy, which may be interpreted to cover the issue of recording or accessing private communication, an act that may be interpreted as a punishable offence.

Besides, where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource that it owns, controls or operates is negligent in implementing and maintaining reasonable security practices and procedures and, thereby, causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Additionally, any person who is required under the IT Act to:

- furnish any document, return or report to the controller or the certifying authority fails to furnish the same, shall be liable to a penalty not exceeding 150,000 rupees for each such failure;
- file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file a return or furnish the same within the time specified therefor in the regulations, shall be liable to a penalty not exceeding 5,000 rupees for every day during which such failure continues; and
- maintain books of account or records fails to maintain the same, shall be liable to a penalty not exceeding 10,000 rupees for every day during which the failure continues.

The IT Act also provides for a residuary penalty, which states that for the contravention of which no penalty has been separately provided, a person shall be liable to pay compensation not exceeding 25,000 rupees to the person affected by such contravention.

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

With regard to the criminalisation of cyberactivities and offences, the IT Act provides for the following offences and punishments:

- tampering with computer source documents: punishable by imprisonment of up to three years, or a fine of up to 200,000 rupees, or both;
- computer-related offences: the IT Act provides that where any person commits the following acts, they shall be liable to pay damages as compensation to the person so affected. Further, if such act is carried on by the person dishonestly or fraudulently, such person shall be punishable by imprisonment for a term of up to three years or a fine of up to 500,000 rupees, or both:
  - accesses or secures access to such computer, computer system or computer network;
  - downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
  - introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
  - damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;
  - disrupts or causes disruption of any computer, computer system or computer network;
  - denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
  - provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
  - charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
  - destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; or
  - steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;
- sending offensive messages through a communication service that is grossly offensive or has menacing character or is for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will: punishable by imprisonment of up to three years and a fine;
- dishonestly receiving stolen computer resources or communication devices: punishable by imprisonment of up to three years or a fine of up to 100,000 rupees, or both;
- identity theft: punishable by imprisonment of of up to three years and a fine of up to 100,000 rupees;
- cheating by impersonation by using a computer resource: punishable by imprisonment of up to three years and a fine of up to 100,000 rupees;
- violation of privacy: punishable by imprisonment of up to three years or a fine of up to 200,000 rupees, or both;
- cyberterrorism: punishable by imprisonment, which may extend to imprisonment for life;
- publishing or transmitting obscene material in electronic form: punishable, on first conviction, by imprisonment of up to three years and a fine of up to 500,000 rupees, and in the event of a second or subsequent conviction by imprisonment of up to five years and a fine of up to 1 million rupees;
- publishing or transmitting of material containing sexually explicit acts, etc, in electronic form: punishable, on first conviction, by imprisonment of up to five years and a fine of up to 1 million rupees, and in the event of a second or subsequent conviction by imprisonment of up to seven years and a fine of up to 1 million rupees;
- publishing or transmitting of material depicting children in sexually explicit acts, etc, in electronic form: punishable, on first conviction, by imprisonment of up to five years and fine of up to 1 million rupees, and in the event of a second or subsequent conviction by imprisonment of up to to seven years and a fine of up to 1 million rupees;

- preservation and retention of information by intermediaries for a duration not in line with the manner and format as prescribed by the government: punishable by imprisonment of up to three years and a fine;
- non-compliance with any order of the controller: punishable by imprisonment of up to two years or a fine of up to 100,000 rupees, or both;
- non-compliance with directions for interception or monitoring or decryption of any information through any computer resource: punishable by imprisonment of up to seven years and a fine;
- non-compliance with directions for blocking public access to any information through any computer resource by an intermediary: punishable by imprisonment of up to seven years and a fine;
- not providing support for monitoring and collection traffic data or information through any computer resource for cybersecurity: punishable by imprisonment of up to three years and a fine;
- securing access or attempting to secure access to a protected system, as declared by the government: punishable by imprisonment of up to 10 years and a fine;
- failure to provide the information called for or failure to comply with the directions of the Computer Emergency Response Team: punishable by imprisonment of up to one year or a fine of up to 100,000 rupees, or both;
- misrepresentation or suppressesion of any material fact from the controller or the certifying authority for obtaining any licence or electronic signature certificate: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both;
- breach of confidentiality and privacy: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both;
- disclosure of information in breach of lawful contract: punishable by imprisonment of up to three years, or a fine of up to 500,000 rupees, or both;
- publishing false electronic signatures in certain particulars: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both;
- publication for fraudulent or unlawful purpose: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both; and
- confiscation: any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Further, it is provided that no compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law currently in force.

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

At present there are no specific legislative or regulatory measures implemented to addressed information security challenges associated with cloud computing. Issues relating to cloud computing and associated information security challenges are currently dealt with contractually between parties who may impose internationally applicable standards or measures.

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 IT Act has been made applicable to any offence or contravention committed outside India by any person irrespective of his or her nationality. Section 75 of the IT Act provides that this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Best practice

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

The authorities have not recommended additional norms and practices and primarily enforce the provisions mandated by the IT Act and the rules made thereunder. However, certain self-regulatory bodies have issued regulatory frameworks and best practices for their member entities. The Data Security Council of India (DSCI) has published the DSCI Privacy Best Practices and the DSCI Security Framework, which would be applicable to its members.

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

At present, no provision for such incentives has been initiated through the existing legislation.

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

The primary rules for cybersecurity are enshrined in the IT Act and the rules made thereunder. The International Standard ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements' has been prescribed by rule 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 for the security practices and procedures.

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

There have been instances where various self-regulatory organisations have laid down best practices and procedures for responding to breaches of cybersecurity by the DSCI. The DSCI has issued the DSCI Privacy Best Practices and the DSCI Security Framework, which would be applicable to its members.

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

The sharing of information about cyberthreats has been discussed above.

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

The cooperation between the government and the private sector is stipulated in terms of the formulation of the reasonable security practices and procedures. The IT Act under the provisions of section 43A obligates a body corporate handling sensitive personal data or information to implement and maintain reasonable security practices and procedures. These 'reasonable security practices and procedures' mean security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law currently in force and in the absence of such agreement or any law, such reasonable security practices and procedures as may be prescribed by the government in consultation with such professional bodies or associations as it may deem fit.

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

Cyber liability insurance is generally regarded as an extension to professional indemnity policy. Such policies cover computer virus, misrepresentation, defamation, confidentiality breach, intellectual property infringement and other related risks. However, such provisions are not universally applicable and the term of policy should be considered before relying on such policies in an absolute manner.

Enforcement

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

The regulatory bodies responsible for enforcing cybersecurity rules comprise the following:

- the Indian Computer Emergency Response Team (CERT-In) and the sectoral CERTs;
- the Department of Information Technology;
- the Department of Telecommunications;
- the Ministry of Home Affairs;
- the Ministry of Defence;
- the National Information Board;

- the National Crisis management Committee;
- the National Security Council Secretariat;
- the National Information Infrastructure Protection Centre;
- the National Disaster Management Authority of India; and
- the Standardisation, Testing and Quality Certification Directorate.

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

The regulatory authorities dealing with cybersecurity investigations are as follows:

- the CERT-In monitors Indian cyberspace and coordinates alerts and warnings of imminent attacks and detection of malicious attacks among public and private cyber users and organisations in the country;
- the National Information Infrastructure Protection Centre is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyberthreats in strategic sectors including national defence;
- the Department of Information Technology (DIT) is under the Ministry of Communications and Information Technology, government of India. The DIT strives to make India a global leading player in information technology and at the same time take the benefits of IT to every walk of life in order to develop an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion and policies in electronics and IT;
- the Department of Telecommunications, under the Ministry of Communications and Information Technology, government of India, is responsible for coordinating with all ISPs and service providers with respect to cybersecurity incidents and response actions as deemed necessary by CERT-In and other government agencies;
- the National Information Board (NIB) is an apex agency with representatives from relevant departments and agencies that form part of the critical minimum information infrastructure in the country;
- the National Crisis Management Committee is an apex body of the government of India for dealing with major crisis incidents that have serious or national ramifications;
- the National Security Council Secretariat is an apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB;
- the Ministry of Home Affairs (MHA) issues security guidelines from time to time to secure physical infrastructure. The MHA sensitises the administrative departments and organisations about vulnerabilities and also assists the respective administrative ministry and departments;
- the Ministry of Defence (MoD) is the nodal agency for cybersecurity incident response with respect to defence sector. The MoD, Integrated Defence Staff (IDS), formed under the aegis of Headquarters IDS, is the nodal tri-services agency at the national level to effectively deal with all aspects of information assurance and operations;

Update and trends

In September 2015, a draft Encryption Policy formulated by an expert group set up by the Department of Electronics and Information Technology under section 84A of the Information Technology Act, 2000 was issued. The draft, which was applicable to everyone including government departments, academic institutions and citizens for all kinds of communications, proposed legal action that could entail imprisonment for failure to store and produce on demand the encrypted message from any mobile device or computer. However, after much criticism the government withdrew the draft and is reworking it.

- the National Disaster Management Authority is the apex body for disaster management in India and is responsible for the creation of an enabling environment for institutional mechanisms at the state and district levels; and
- the Standardisation, Testing and Quality Certification (STQC) Directorate is a part of the DIT and is an internationally recognised assurance service providing organisation. The STQC has established a nationwide infrastructure and developed competence to provide quality assurance and conformity assessment services in IT.

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

Some enforcement issues faced by the regulatory bodies in India are as follows:

- there is no territorial boundary and thus the jurisdiction issue arises when international breaches occur;
- technical complexities;
- law enforcement officials lack proper training in cyberlaws;
- anonymity over the internet and multiple protective layers instated by criminals are sometimes very hard to break and thus enforcement is negated; and
- the lack of proper user logs and lack of proper tools to monitor internet traffic.

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

A list of the penalties set out under the IT Act has been segregated into civil liabilities and criminal penalties in questions 9 and 10 respectively. The same would be imposed for the relevant threats and breaches. In addition to the specific liabilities and penalties, the IT Act also provides for a residuary penalty, which states that for the contravention of which no penalty has been separately provided, a person shall be liable to pay compensation not exceeding 25,000 rupees to the person affected by such contravention.

Salman Waris **salman.waris@techlegis.com**

Level 1 Redfort Capital Parsavnath Towers
Bhai Veer Singh Marg
Gole Market, Connaught Place
New Delhi 110001
India

Tel: +91 98 9142 7685
Fax: +91 11 2636 0037
www.techlegis.com

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

See questions 9, 10 and 22.

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

The parties are at liberty to seek private redress. The parties may either mutually negotiate and settle the matter or are also entitled to initiate arbitration proceedings under the provisions of and as prescribed by the Arbitration and Conciliation Act, 1996.

Threat detection and reporting

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

To ensure protection from cyberthreats, a body corporate handling sensitive personal data or information is obligated to implement reasonable security practices and procedures. The body corporate is bound to adhere to the strict conditions for the collection, transfer and disclosure of the sensitive personal data or information, in order to ensure data protection.

Additionally, in terms of the Information Technology (Intermediaries Guidelines) Rules, 2011, the intermediary is also under an obligation not to host, display, upload, modify, publish, transmit, update or share any information that contains software viruses or any other computer codes, files or programs designed to interrupt, destroy or limit the functionality of any computer resource.

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

There is no explicit requirement to keep a record of cyberthreats or breaches. However, the same is implicit in the manner that the cybersecurity incidents are to be reported to CERT-In by individuals, organisations or corporate entities.

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

Cybersecurity incidents are to be reported to CERT-In by individuals, organisations or corporate entities.

29 What is the timeline for reporting to the authorities?

Pursuant to the Information Technology (the Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013, individuals, organisations or corporate entities, as the case may be, are required to report cybersecurity incidents to CERT-In within a reasonable time of the occurrence or of becoming aware of the incident.

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

Individuals, organisations or corporate entities, as the case may be, are required to report incidents of cybersecurity breach to CERT-In, however, the obligation to report to the public is not a provision of the IT Act. Nevertheless, CERT-In, under the Information Technology (the Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013, has been assigned the function of publishing alerts and offering information for the improvement of cybersecurity.

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
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
Enforcement of Foreign Judgments
Environment & Climate Regulation
Executive Compensation & Employee Benefits
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
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 Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
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

Law Business Research

Cybersecurity
ISSN 2056-7685

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law