ICLG

The International Comparative Legal Guide to:

Cybersecurity 2018

1st Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Allen & Overy
Angara Abello Concepcion Regala & Cruz Law Offices
Baker McKenzie
Boga & Associates
BTG Legal
Christopher & Lee Ong
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
ENSafrica
Erkelens Law
Eversheds Sutherland
Holland & Hart LLP
JIPYONG
Josh and Mak International
King & Wood Mallesons
Lee, Tsai & Partners Attorneys-at-Law
Maples and Calder
MinterEllison
Mori Hamada & Matsumoto
Niederer Kraft & Frey Ltd.
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Shibolet & Co.
Simmons & Simmons LLP
Udo Udoma & Belo-Osagie

glg
global legal group

global legal group

Contributing Editors
Nigel Parker & Alex Shandro, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy, Rachel Williams

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 2017

ISBN 978-1-911367-77-2
ISSN 2515-4206

Strategic Partners

General Chapters:

1 **Would the Standard of Cybersecurity be Improved by the Introduction of Mandatory Cybersecurity Controls?** – Nigel Parker & Alex Shandro, Allen & Overy LLP 1

2 **Enemy at the Gates? The Cybersecurity Threat Posed by Outsourcing, Partnering and Professional Advisors** – Robert Allen & Paul Baker, Simmons & Simmons LLP 6

3 **Directors and Officers Liability for Data Breach** – Liz Harding, Holland & Hart LLP 12

Country Question and Answer Chapters:

4 **Albania** Boga & Associates: Renata Leka & Eno Muja 16

5 **Australia** MinterEllison: Paul Kallenbach & Leah Mooney 21

6 **Belgium** Erkelens Law: Johan Vandendriessche & Isaure de Villenfagne 28

7 **Canada** Baker McKenzie: Dean Dolan & Theo Ling 35

8 **China** King & Wood Mallesons: Susan Ning & Han Wu 43

9 **England & Wales** Allen & Overy LLP: Nigel Parker & Alex Shandro 50

10 **Germany** Eversheds Sutherland: Dr. Alexander Niethammer & Steffen Morawietz 58

11 **India** BTG Legal: Prashant Mara & Devina Deshpande 64

12 **Ireland** Maples and Calder: Kevin Harnett & Victor Timon 72

13 **Israel** Shibolet & Co.: Nir Feinberg 80

14 **Japan** Mori Hamada & Matsumoto: Hiromi Hayashi 87

15 **Korea** JIPYONG: Seung Soo Choi & Seungmin Jasmine Jung 95

16 **Kosovo** Boga & Associates: Sokol Elmazaj & Delvina Nallbani 101

17 **Malaysia** Christopher & Lee Ong: Deepak Pillai 107

18 **Mexico** Creel, García-Cuéllar, Aiza y Enríquez, S.C.: Begoña Cancino & Oscar Arias 116

19 **Nigeria** Udo Udoma & Belo-Osagie: Olajumoke Lambo & Godson Ogheneochuko 122

20 **Pakistan** Josh and Mak International: Aemen Zulfikar Maluka 128

21 **Philippines** Angara Abello Concepcion Regala & Cruz Law Offices: Leland R. Villadolid Jr. & Arianne T. Ferrer 133

22 **Poland** Allen & Overy A. Pędzich sp.k.: Krystyna Szczepanowska-Kozłowska & Justyna Ostrowska 141

23 **Singapore** Rajah & Tann Singapore LLP: Rajesh Sreenivasan & Michael Chen 148

24 **South Africa** ENSafrica: Suad Jacobs & Theo Buchler 156

25 **Switzerland** Niederer Kraft & Frey Ltd.: Dr. András Gurovits & Clara-Ann Gordon 164

26 **Taiwan** Lee, Tsai & Partners Attorneys-at-Law: Sean Yu-Shao Liu & Sophia Tsai 171

27 **Thailand** R&T Asia (Thailand) Limited: Saroj Jongsaritwang & Sui Lin Teoh 178

28 **USA** Allen & Overy LLP: Laura R. Hall & Kurt Wolfe 184

India

Prashant Mara

Devina Deshpande

BTG Legal

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)

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) accessing/securing unauthorised access to a computer resource (which includes computers, communication devices, computer networks, data, computer databases or software, etc.); and

(ii) providing assistance to any person to facilitate such unauthorised access (Sec. 43(a) and (b) Information Technology Act, 2000 ("**ITA**")).

The above offences are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Also see question 1.4 below in respect of cyberterrorism and criminal trespass and question 2.2 below in respect of 'protected system'.

Prosecutions:

- *Kumar v. Whiteley* (2009): the accused was sentenced to one year of rigorous imprisonment and a fine of INR 5,000 for hacking a government website, gaining unauthorised access to broadband internet and making alterations to subscriber accounts in the computer database.
- Call centre employees at Mphasis were prosecuted for securing unauthorised access to PIN codes of customers of Citi Group (a client of their call centre) and using these codes to transfer funds into their accounts (2005).

Denial-of-service attacks

- Causing disruption or denial of access to any person authorised to access any computer by any means is an offence when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of such computer (Sec. 43(e) and (f), ITA).
- Punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).
- Also see question 1.4 below in respect of cyberterrorism.

Phishing

While "phishing" is not expressly defined, the following acts constitute offences:

(i) **Identity theft**: fraudulent or dishonest use of the electronic signature, password or other unique identification feature of any other person (Sec. 66C, ITA).

(ii) **Cheating by personation**: using a computer/communication device to cheat by pretending/representing to be another person or knowingly substituting one person for another (Sec. 66D, ITA).

The above offences are punishable with imprisonment of up to three years and with a fine of up to INR 100,000.

(iii) **Deceptive/misleading emails**: sending emails/messages that deceive/mislead the recipient as to the origin of such message (Sec 66A(c), ITA).

The above is punishable with imprisonment of up to three years and a fine.

Cheating under the IPC may also be invoked (see question 1.4 below).

Prosecutions:

- Mumbai Cyber Cell registered an offence against a person who circulated misleading emails ostensibly emanating from ICICI Bank to obtain confidential information (including usernames, passwords, debit card numbers, PIN codes, etc.) from the recipient bank's customers.
- Persons were arrested for circulating emails indicating that the recipient had won a lottery prize and requiring them to deposit courier, VAT and insurance charges prior to the transfer of the 'lottery winnings'.

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

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) introduction of a computer contaminant/virus; and

(ii) damage to any computer, computer system or computer network or any data, database or computer program residing therein (Sec. 43(c) and (d), ITA).

The above offences are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Also, see question 1.4 below in respect of cyberterrorism.

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

Possession of any plate (including negative duplicating equipment, block, mould, etc.) for making infringing copies of copyrighted work is punishable with imprisonment of up to two years and a fine (Sec. 65, Copyright Act).

Dishonestly receiving stolen computer resources or communication devices is punishable with imprisonment of up to three years or a fine of up to INR 100,000 (Sec. 66B, ITA).

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

See "Phishing" above.

Publication of electronic signatures: (i) that are fake; or (ii) for fraudulent/unlawful purposes is punishable with imprisonment of up to two years or with a fine of up to INR 100,000 or with both (Sec. 73 and 74, ITA).

Prosecutions:

- *State of Odisha v. Jayanta Das* (2017): sentenced to six years' imprisonment and a fine on charges of forgery, identity theft and cyber pornography for creating a fake profile on a pornographic website in the name of the complainant's wife.

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

The following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) downloading, copying or extracting data/information from a computer resource (including any removable storage medium) (Sec. 43(b), ITA); and

(ii) charging services availed of by a person to the account of another person by tampering with/manipulating any computer (Sec 43(h), ITA).

The above are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Violation of privacy by intentionally or knowingly publishing/transmitting a private image of a person without his consent is punishable with imprisonment of up to three years or with a fine of up to INR 200,000 or with both (Sec. 66E, ITA).

Disclosure of personal information obtained while providing contractual services, with the intent/knowledge that wrongful loss/gain will result, is punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 72A, ITA).

Criminal copyright infringement (i.e. with knowledge): knowingly using an infringing copy of a computer program, and infringement and passing off of trademarks, are punishable with imprisonment of up to three years and a fine of up to INR 200,000. In each case, an enhanced penalty is invoked upon subsequent convictions (Sec. 63 and Sec. 63B, Copyright Act and Sec. 104 of Trade Marks Act).

Theft, cheating, fraud, dishonest misappropriation and criminal breach of trust provisions under the IPC may also be invoked (see question 1.4 below).

Prosecutions:

- *Shankar v. State* (2010): an employee caused the publication of confidential information which he obtained through unauthorised access of a computer at the office of the Directorate of Vigilance and Anti-Corruption. He was charged with securing unauthorised access to a 'protected system' and breach of confidentiality and privacy.
- An employee of HSBC's BPO arm in India was arrested on charges of data theft and cyber fraud for producing forged certificates used to illegally embezzle funds (2005).

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 following acts constitute offences when conducted fraudulently or dishonestly and without the permission of the owner/person in charge of the computer:

(i) destroying, deleting, injuring, altering or diminishing the value/utility of information residing in a computer resource; and

(ii) stealing, concealing, destroying or altering computer source code (including computer commands, design and layout, program analysis, etc.) with an intention to cause damage (Sec. 43(i) and (j), ITA).

The above are punishable with imprisonment of up to three years or with a fine of up to INR 500,000 or with both (Sec. 66A, ITA).

Knowingly or intentionally tampering (concealing, destroying or altering) with computer source documents required to be kept/maintained by law is punishable with imprisonment of up to three years or with a fine of up to INR 200,000 or with both (Sec. 65, ITA).

Prosecutions:

- *Shankar v. State* (2010) (see "Electronic theft" above): a case was also made out that by downloading, copying and causing the publication of confidential information, the accused diminished the value and utility of such information and affected it injuriously.
- The offence of tampering with computer source documents was held in the following:
  a) *Bhim Sen Garg v. State of Rajasthan* (2006): fabrication of an electronic record, or committing forgery by way of interpolations in a CD; and
  b) *Syed Asifuddin v. State of Andhra Pradesh* (2005): Tata Indicom employees were arrested for the manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

Failure by an organisation to implement cybersecurity measures

This is not applicable in our jurisdiction. See questions 2.10 and 5.1 below for non-penal repercussions.

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

Yes, provided that the offence committed outside India involves a computer, computer system or computer network located in India (Sec. 75, ITA).

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?

Acts under Sec. 43 of the ITA (including hacking, denial-of-service attacks, introduction of virus, etc.) not conducted fraudulently or dishonestly will invoke the civil (and not criminal) liability of compensation of up to INR 10,000,000 for damage caused.

For trademark/copyright infringement, no damages will be payable where the defendant can prove he was unaware, and had no reasonable ground for believing, that the work was trademark/copyright protected.

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.

The following Incidents will constitute "cyberterrorism", which are punishable with life imprisonment:

(i) unauthorised access, denial of access or introduction of a computer contaminant with the intent to threaten national security and causing (or likely to cause) death, injuries,

damage to property or disruption of essential supplies/services; and

(ii) intentionally/knowingly obtaining unauthorised access to restricted information/data which may be used to injure national security, public order, relations with foreign states, defamation, etc. (Sec. 66F, ITA).

Incidents may also invoke:

(i) Criminal offences under the IPC, such as cheating, theft, criminal breach of trust, criminal trespass, forgery of electronic records, dishonest misappropriation, etc.

(ii) Penal provisions under specialised legislations which punish publishing or transmitting obscene and sexually explicit materials (such as child pornography or indecent representation of women).

Prosecutions:

- Sedition charges were pressed against a former scientist for the hacking of an internet service provider and sending emails threatening national security to the Department of Atomic Energy (2001).
- A criminal case for cheating, theft and criminal conspiracy under the IPC was registered against hackers involved in stealing debit and credit card details using a proxy IP address (2017).
- *Dr. Prakash v. State of Tamil Nadu* (2002): sentenced to imprisonment for posting nude pictures of female patients online in contravention of the ITA, IPC and Indecent Representation of Women (Prohibition) Act, 1986.

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.

Information technology laws:

(i) Information Technology Act, 2000 ("**ITA**");

(ii) IT (Certifying Authority) Regulations, 2001;

(iii) IT (Security Procedure) Rules, 2004;

(iv) IT (Procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009 ("**Decryption Rules**");

(v) IT (Procedure and safeguards for blocking for access of information by public) Rules, 2009;

(vi) IT (Procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009;

(vii) IT (Intermediaries Guidelines) Rules, 2011 ("**Intermediary Rules**");

(viii) IT (Guidelines for Cyber Cafe) Rules, 2011;

(ix) IT (Electronic Services Delivery) Rules, 2011;

(x) IT (the Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013 ("**CERT Rules**"); and

(xi) National Cyber Security Policy, 2013.

In addition, relevant offences under the Indian Penal Code, 1860 ("**IPC**") may also be added to offences under the ITA at the time of prosecution.

Privacy and data protection laws:

(i) IT (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**Privacy Rules**").

Note: Data (Privacy and Protection) Bill, 2017 ("**Privacy Bill**") has been tabled before Parliament. Additionally, the Supreme Court of India has recently recognised the right to privacy as a fundamental right under the Indian Constitution.

Reserve Bank of India ("RBI") directions/notifications:

(i) RBI Notification – Cyber Security Framework in Banks (June 2016) ("**Bank Notification**").

(ii) RBI Press Release – Establishment of an Inter-Disciplinary Committee on Cyber Security (February 2017).

(iii) RBI Master Direction – IT Framework for NBFC Sector (June 2017) ("**NBFC Master Direction**").

Intellectual property ("IP") laws:

(i) Copyright Act, 1957.

(ii) Patent Act, 1970.

(iii) Trade Marks Act, 1999.

Telecommunications laws:

(i) Unified License Agreement ("**ULA**") issued under the Indian Telegraph Act, 1885.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, how (and according to what timetable) is your jurisdiction expected to implement the Network and Information Systems Directive? Please include details of any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

The government may declare any computer resource which affects critical information infrastructure as a 'protected system' and specifically identify persons authorised to access such protected systems. Securing/attempting to secure unauthorised access to a protected system is punishable with imprisonment of up to 10 years and a fine.

The government has designated the National Critical Information Infrastructure Protection Centre ("**NCIIPC**") as the national nodal agency for critical information infrastructure protection.

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.

Intermediaries/persons in charge of computer resources may be required by the government to provide access/assistance in respect of: (i) the interception, monitoring or decryption of information stored/transmitted through a computer resource; (ii) the monitoring and collecting of traffic data/information to enhance cybersecurity and to identify/prevent the spread of computer contaminant; and (iii) the prevention, detection, investigation, prosecution, punishment, etc. of an Incident (Sec. 69 and 69A, ITA and Rule 3(7), Intermediary Rules).

Intermediaries and body corporates which store/handle/deal with personal information must implement reasonable security practices and procedures (i.e. control measures commensurate with the information assets being protected) (Rule 3(8), Intermediary Rules and Rule 4, Privacy Rules).

Persons authorised to issue electronic signatures under the ITA ("**Certifying Authorities**") must: (i) use secure hardware and software; and (ii) implement security procedures to ensure secrecy and privacy of electronic signatures (Sec. 30, ITA).

Banks, Non-Banking Finance Companies ("**NBFCs**") and insurance companies must implement a board-approved cybersecurity policy (distinct from their broader IT/IS security policy) with arrangements for continuous surveillance and vulnerability testing.

Telecom companies must, within 12 months of being licensed, create facilities to monitor intrusions, attacks and frauds on their technical facilities and provide related reports to the Department of Telecommunications ("**DOT**") (Clause 39.10(i), ULA).

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 government's approach is to maintain access to electronic communications for itself, while ensuring protection against unauthorised access by third parties. To that extent, there is a conflict in the expectation that networks/data should be protected by a "key", but that such key should be made available to the government when requested. However, there are no inherent conflicts in legislations which are drafted to achieve the above.

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

(a) The circumstance in which this reporting obligation is triggered:

- Individuals, organisations and corporate entities must promptly report the occurrence of certain Incidents (including unauthorised access, compromise of critical systems and infrastructure, malicious code, server attacks, identity theft, denial-of-service, etc.). Service providers, intermediaries, data centres and body corporates must report Incidents within a reasonable time of the occurrence or of becoming aware of the Incident (Rule 12(1), CERT Rules, and Rule 3(9), Intermediary Rules).
- In the financial services sector, all Incidents (successful and attempted) must be reported to the RBI: (i) by Banks within two to six hours; and (ii) by NBFCs within 24 hours.
- Insurance companies must report Incidents which critically affect business operations and a large number of customers to the Insurance Regulatory and Development Authority ("**IRDA**") within 48 hours of knowledge of the Incident.
- See question 2.3 above in respect of telecom companies.

(b) The regulatory or other authority to which the information is required to be reported:

- Indian Computer Emergency Response Team ("**CERT-In**").
- NCIIPC (for sectors falling under "critical infrastructure").
- See (a) at question 2.5 above for sector-specific reporting authorities.

(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):

- Reports to CERT-In must specify: (i) the time of occurrence; (ii) information regarding the affected system/network; (iii) symptoms observed (i.e. suspicious probes, denial of service, unaccounted changes in firewall rules, etc.); and (iv) the relevant technical information (i.e. security systems deployed, hosts affected, actions taken to mitigate the damage, etc.). Details regarding formats for reporting Incidents are published on the CERT-In website (www.cert-in.org.in) and are updated from time to time.
- Reports to the RBI must include: (i) details of the Incident (i.e. outage of critical IT system, theft/loss of information, etc.); (ii) actions taken; (iii) impact assessment; (iv) root cause analysis; and (v) impact of the attack, etc.

(d) Whether any defences or exemptions exist by which the organisation might prevent publication of that information:

- CERT-In will not disclose any information which may lead to the identification of individuals or organisations affected by, or those reporting, cybersecurity Incidents without their written consent or pursuant to a court order (Rule 13(2), CERT Rules).

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) A regulatory or other authority in your jurisdiction:

- Please see the response to (a) at question 2.5 above.

(b) A regulatory or other authority outside your jurisdiction:

- No express permission or prohibition (insofar as such disclosure does not violate privacy and data protection requirements, telecom user data or banking user data).

(c) Other private sector organisations or trade associations in or outside your jurisdiction:

- Same as (b) above.

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.

Certifying Authorities must, upon an event/situation which may materially/adversely affect the integrity of its computer system or conditions under which an electronic signature was granted, use reasonable efforts to notify persons likely to be affected (Sec. 34, ITA).

While there is no legal requirement to notify data breaches to affected individuals at present, the draft Privacy Bill mandates such notification (except where notification will impede a criminal investigation or the affected individual cannot be identified).

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

The responses do not change.

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

- Indian Computer Emergency Response Team.
- National Information Infrastructure Protection Centre.
- Department of Information Technology.
- Department of Telecommunications.
- National Information Board (NIB).
- National Crisis Management Committee.
- National Security Council Secretariat.
- Ministry of Home Affairs.
- Ministry of Defence.
- National Disaster Management Authority.

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

ITA/CERT Rules/Intermediary Rules:

(i) There is no penalty prescribed for non-compliance with the mandatory reporting of Incidents. As such, a residuary penalty (of up to INR 25,000) under the ITA will apply (Sec. 45, ITA).

(ii) The licence of the Certifying Authority may be revoked for failure to maintain/follow required security standards (Sec. 25, ITA).

ULA:

Telecom companies will be liable:

(i) for any inadvertent security breach: a penalty of up to INR 500,000,000; and

(ii) for any inadequate compliance with the licence, intentional omission, deliberate vulnerability, etc.: a penalty of INR 500,000,000 per breach. The licence may also be terminated and the vendor who supplied the hardware/software responsible for the breach could be blacklisted (Clause 39.10(i) and (ii), Clause 3.11(ii), ULA).

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

Poona Auto Ancillaries v. Punjab National Bank (2011): money was fraudulently transferred from the complainant's account after he responded to a phishing email. The bank was found negligent due to the lack of proper security checks against fraud accounts and was ordered to pay INR 4,500,000 as compensation.

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.

Organisations in the defence, power and other national security sectors may (on a case-by-case basis) be subject to more stringent information security requirements.

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?

(a) The financial services sector:

- **Banks and NBFCs**
  - The RBI requires banks/NBFCs to, *inter alia*:
    (i) evolve a 'Cyber Crisis Management Plan' ("**CCMP**") to address potential Incidents and face emerging cyber threats such as 'zero-day' attacks and remote access threats;
    (ii) create awareness among stakeholders (failing which, stakeholders will not be responsible for Incidents that occur due to their ignorance);
    (iii) Banks are additionally required to: (a) set up a 'security operations centre' to conduct continuous surveillance and testing for vulnerabilities; and (b) appoint a Chief Information Security Officer ("**CISO**") to identify gaps in preparedness and propose measures/controls; and
    (iv) NBFCs are additionally required to: (i) consider the use of digital signatures for high-value fund transfers; (ii) develop a mechanism for safeguarding information assets (including end-to-end encryption) in respect of mobile financial services; and (iii) develop controls and secure connections when using social media for marketing products.
- **Internet-based trading/securities using wireless technology**
  - The Securities and Exchange Board of India requires stock exchanges to:
    (i) ensure brokers implement secure end-to-end encryption for all data transmission, safety features against internal/external Incidents, two-factor authentication for login, etc.; and
    (ii) arrange periodic systems audits of broker systems and include wireless technology trading in investor awareness programmes.
- **Insurance**
  - IRDA requires insurances companies to, *inter alia*:
    (i) evolve a CCMP and create awareness about cyber threats among stakeholders;
    (ii) designate a CISO to formulate and enforce policies to protect information assets;
    (iii) constitute an 'Information Security Committee' for information security management; and
    (iv) undertake measures for data and application security, Incident response planning, vulnerability assessments, penetration tests, etc.

(b) The telecommunications sector:

- Vendor contracts with telecom companies must: (i) allow inspection of hardware, software, manufacturing facility, etc. by the telecom company/DOT; (ii) allow security checks of vendor software any time; and (iii) acknowledge the DOT's discretion to blacklist vendors for security breaches.
- The DOT will constitute a five-member committee (including two cybersecurity experts) to assess breaches and determine applicable penalties.
- The DOT may mandate (as necessary) that telecom companies:
  - (i) enter into vendor agreements: (a) certifying services/software are 'safe to connect' and have been checked for risks/vulnerabilities; (b) covering security measures (such as access and password control); and (c) addressing service continuity and upgradation, etc.;
  - (ii) create a forum to increase security assurance levels and share common issues; and
  - (iii) build capability and capacity (through local maintenance personnel) to maintain security of the telecom network.
- Encryption standards have been prescribed for telecom and internet service providers, and bulk encryption is expressly prohibited.

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?

Where a company is legally subject to cybersecurity requirements (such as data storage or privacy under the ITA), the occurrence of a related Incident due to the failure of the directors to implement proper systems to comply with such requirements, or to ensure the adequacy and effectiveness of the systems, may amount to a breach of directors' duties under company law (Sec. 134, Companies Act, 2013).

Persons in charge of the conduct of business of a company will be considered guilty for any contravention by the company of the provisions of the ITA or rules (unless he is able to prove lack of knowledge of the contravention or exercise of due diligence) (Sec. 85, ITA).

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

The above requirements are mandatory for banks, NBFCs (with the exception of designation of a CISO), insurance companies and telecom companies.

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)?

No specific disclosure requirements are imposed.

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

Listed companies/companies with over 1,000 shareholders must:

(i) provide e-voting facilities with votes recorded in an electronic registry with adequate cybersecurity; and

(ii) ensure the security of any electronic records, including: (i) protection against unauthorised access, alteration or tampering; (ii) security of computer systems, software and hardware; (iii) periodic backups; (iv) ability of computer systems to discern invalid/altered records; and (v) retrieval of readable/printable records, etc. (Rule 20 and Rule 28, Companies (Management and Administration) Rules, 2014).

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.

See question 1.3 above in respect of civil liability under Sec. 43, ITA.

An organisation will be liable for damages of up to INR 50,000,000 if it fails to implement reasonable security practices and procedures to protect sensitive personal information (such as passwords, financial information, biometrics, etc.) ("**SPI**") and such negligence results in a wrongful gain or loss (Sec. 43A, ITA).

Organisations required to furnish information, records, returns, etc. or to maintain books of account/records under the ITA/rules will be liable to monetary penalties for any failure to comply (Sec. 44, ITA).

Civil suits may be brought in respect of infringement of IP rights including in respect of injunction, damages and account of profits.

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

Prosecution under the ITA:

(i) See the *Poona Auto* case under question 2.11 above.

(ii) Compensation has been imposed for breach of privacy in a number of cases, including *Amit Patwardhan v. Rud India Chains* and *Nirmalkumar Bagherwal v. Minal Bagherwal* (both 2013), where the complainants' financial information (constituting SPI) was obtained from their respective banks without their consent and used against them in legal proceedings.

IPR infringement:

(i) In *Adobe Systems Inc. v. Sachin Naik* (2010), the plaintiff was held entitled to damages of INR 200,000 and costs for software infringement.

(ii) In *Infosys Technologies v. Akhil Gupta* (2005), the plaintiff was awarded a permanent injunction against the defendant's use of the trademark/name "Infosys", along with damages of INR 300,000 and costs.

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

Tortious liability may arise in respect of trespass (hacking), fraudulent misrepresentation (phishing/identity theft), breach of privacy, breach of confidentiality, nuisance (denial-of-service), etc.

6 Insurance

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

Yes, cyber insurance may be taken as a standalone liability policy or as an extension under E&O or professional indemnity insurance.

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?

This is not applicable in our jurisdiction.

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?

This is not applicable in our jurisdiction.

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?

This is not applicable in our jurisdiction.

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.

Offences under the ITA must be investigated by police officers not below the rank of Inspector (Sec. 78, ITA). Investigatory powers include:

(i) confiscating computer systems, hardware, tape drives, etc. containing information or used to contravene the ITA (Sec 76, ITA);

(ii) entering any public place and searching and arresting without a warrant persons guilty/reasonably suspected of committing an offence under the ITA (Sec. 80(1), ITA); and

(iii) search and seizure procedures, issuing summons, requiring the attendance of witnesses and making arrests under the Criminal Procedure Code, 1973.

Authorised officers empowered to investigate contraventions of the ITA and rules can: (a) access and undertake searches of computer systems to obtain information/data; and (b) by order require persons in charge of the computer system to provide reasonable technical assistance (Sec. 28 and 29, ITA).

Intermediaries must, upon lawful order and receipt of a written request, provide information/assistance to authorised government agencies for the investigation, prosecution and punishment of offences under Applicable Law (Rule 3(7), Intermediary Rules).

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?

Authorised government authorities can require information generated, transmitted, received or stored in a computer resource to be intercepted, monitored or decrypted by requiring, *inter alia*: (i) access to such computer resource; (ii) cooperation and technical assistance by intermediaries (including for installation and use of interception/monitoring/decryption equipment by the authorities); and (iii) disclosure of decryption key or provision of decryption assistance by the key holder (Sec. 69, ITA and Decryption Rules).

Consent of the provider of SPI is not required for sharing such SPI with legally mandated government agencies for identity verification or for the prevention, investigation, prosecution, etc. of offences (Rule 6, Privacy Rules).

Telecom/internet service providers must provide the DOT with all the details of the technology employed, drawings, testing instruments, installation tools, etc. Licence conditions do not expressly require means of decryption to be provided to the government, but the language is sufficiently broad to include such access (ULA).

Prashant Mara
BTG Legal
804, Lodha Supremus
Dr. E. Moses Road
Worli
Mumbai – 400018
India

Tel: +91 22 2482 0801 / +91 72080 12801
Email: prashant@btg-legal.com
URL: www.btg-legal.com

Prashant is a commercial lawyer specialising in strategic investments, collaborations, compliance and procurement projects – mostly cross-border. He specialises in the digital business, defence (with a focus on technology transfer and licensing) and industrial (with a focus on technology deployment) sectors. His clients include Facebook, Expedia, TripAdvisor, Fitbit, AirBnB, News Corp, Indigo, MAN group, Zeppelin, Rolls Royce, Voith and Tech Mahindra.

Prashant has spent nine years in Europe, working with top-tier law firms in France, Germany and the UK.

Over the last decade, he has worked closely, as a trusted advisor, with the in-house teams of his clients. This has equipped him to approach a transaction with its strategic rationale in mind, which makes the transaction interesting and the execution effective.

Prashant is proficient in providing compliance and crisis response advice, including dispute management, and acting as the interface between his clients and the regulator.

Devina Deshpande
BTG Legal
804, Lodha Supremus
Dr. E. Moses Road
Worli
Mumbai – 400018
India

Tel: +91 22 2482 0807 / +91 70454 29808
Email: devina@btg-legal.com
URL: www.btg-legal.com

Devina is a senior associate with BTG Legal, focusing on the digital business, defence and industrials sectors. Her experience includes cross-border and domestic private equity investments, M&A, debt capital markets, Islamic finance, investment management, fund formation, corporate governance and corporate advisory.

Devina has previously worked at a magic circle UK law firm, in their London and Dubai offices. She is dual-qualified, being admitted to practise law in India and a solicitor of the Senior Courts of England and Wales.

BTG Legal is a transactional law firm with best-of-breed technical expertise, a culture of innovation, and an unrelenting commitment to excellence.

Our team has specialist sector knowledge in key areas including:

- Defence.
- Industrials.
- Digital business.
- Energy and infrastructure.
- Life sciences.
- Retail.
- Financial services.
- Transport.

Our practices include corporate transactions, M&A, private equity, commercial contracting and procurement, regulatory advice, banking and finance, project finance, labour, fraud and anti-bribery compliance and other areas of law that are fast developing to keep up with rapid changes in technology and methods of doing business.

Our lawyers have worked in-house in large conglomerates as well as in established Indian and international law firms, bringing immense depth to the team. We work closely with Osborne Clarke, a leading international law firm, and are able to extend our global reach significantly.

Clients such as Facebook, WhatsApp, Jet Airways, Indigo Airlines, Tech Mahindra, MAN, Zeppelin, News Group, TripAdvisor, Wirecard and Leica Cameras continue to trust us with their work, given our innovative service delivery models, our understanding of their sectors and our appreciation of the challenging business environment in which they operate.

Current 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
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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