Cybersecurity Laws and Regulations India 2024

ICLG - Cybersecurity Laws and Regulations - India Chapter covers common issues in cybersecurity laws and regulations, including cybercrime, applicable laws, preventing attacks, specific sectors, corporate governance, litigation, insurance, and investigatory and police powers.

Published: 14/11/2023

Chapter Content

Free Access

1. Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction: hacking; denial-of-service attacks; phishing; infection of IT systems with malware; distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime; possession or use of hardware, software or other tools used to commit cybercrime; identity theft or identity fraud; electronic theft; unsolicited penetration testing; or any other activity adversely affecting or threatening the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Yes, the above-mentioned activities amount to a criminal or administrative offence in India under the Information Technology Act, 2000 (IT Act).

The relevant portion of Section 43 reads as follows:

Section 43. There is a penalty and compensation for damage to a computer, computer system, etc. if any person, without permission of the owner or any other person who is in charge of a computer, computer system or computer network:

a. accesses or secures access to such computer, computer system or computer network (or computer resource);

b. 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;

be introduced any computer contaminant or computer virus into any computer, mputer network;

e. disrupts or causes disruption of any computer, computer system or computer network;

f. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

g. 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;

h. 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;

i. 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

j. 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.

Hacking

The Act defines in Sections 43 and 66 the term "Hacking" to mean and include a wide range of activities done fraudulently or dishonestly without the permission of the owner or representative of the owner in charge of the system. This includes the section mentioned above. The penalty for such offence is:

Section	Offence	Penalty
66	Hacking with a computer system with the intent or knowledge to cause wrongful loss.	Imprisonment up to three years, a fine up to Rs 500,000, or both.
43	Damage to computer, computer system, etc.	Compensation up to Rs 1 crore to the affected person.

Infection of IT systems with malware

Refers to the unauthorised introduction of malicious software (malware) into computer systems, networks, or devices. Malware is a broad term that encompasses various types of harmful software such as viruses, worms, trojans, spyware, and ransomware. This has been covered in Section 43 as introducing computer contaminants and in Section 65 as tampering with computer source documents.

The penalties are covered under the following sections:

Section	Offence	Penalty
43	Damage to computer, computer system, etc.	Compensation up to Rs 1 crore to the affected person.
65	Tampering with computer source documents.	Imprisonment up to three years, a fine up to Rs 200,000, or both.

	to cause wrongful loss.	200,000, or both.
66F	For Cyberterrorism.	Imprisonment that may extend to life imprisonment.

Denial-of-service (DoS) attacks

DOS attacks involving disrupting the normal functioning of computer systems or networks can be considered offences. The relevant section and associated penalty for such attacks are as follows:

Section	Offence	Penalty
66	Hacking a computer system with the intent or knowledge to cause wrongful loss.	Imprisonment up to three years, a fine up to Rs 200,000, or both.
43	Damage to computer, computer system, etc.	Compensation up to Rs 1 crore to the affected person.

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

The IT Act does not contain clauses directly referring to the distribution, sale or offering for sale tools for use in the commission of cybercrime. Having said that, Section 43 (g) prescribes that the provision of any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the IT Act is liable for fines as mentioned above.

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

The IT Act does not contain clauses directly referring to possession of tools for use in the commission of cybercrime. See the answer under the heading "Distribution, sale or offering for sale".

Section 66B of the Information Technology (Amendment) Act, 2008 (IT Amendment Act) states that whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be a stolen computer resource or communication device shall be punished with imprisonment of up to three years, a fine of up to Rs 100,000 or both.

Identity theft or identity fraud

Identity theft in its plain terms is impersonating another. This is done through obtaining information through multiple ways and fraudulently using that information to cause financial or reputational loss to individuals. Phishing and spam/fraud calls are ways in which identity theft takes place.

Section	Offence	Penalty

	source.	100,000.

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

Please see "Hacking" above.

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

This is punishable as indicated in the answers above. While the IT Act does not make specific reference to penetration testing (Pen testing) it is covered under Section 43 as described above, as it constitutes unauthorised access except for circumstances as mentioned in the question 1.3 below.

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

Section 66F of the IT Amendment Act defines and penalises cyberterrorism.

Section	Offence	Penalty
66F	For Cyberterrorism.	Imprisonment that may extend to life imprisonment.

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

The IT Act, 2000 has extra-territorial jurisdiction for offences committed outside "if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India".

The newly notified Digital Personal Data Protection Act 2023 (DPDPA) vide Section 3 (b) clearly mentions that the Act shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.

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

The statute does not mention exceptions such as ethical hacking. The key test is of *mens rea* or *mala fide* intent. However, the same may be considered to be a valid defence and hence not a defence if the host has invited the intrusion to verify security standards of their programs, systems and servers, i.e. Pen testing, bug bounty, etc.

2. Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, data protection and e-privacy laws, trade secret protection laws, data breach notification laws, confidentiality laws, and information security laws, among others.

The ention monitoring, detection, prevention, mitigation and management of Incidents. The sa nes are as follows:

The IT Act, along with its allied Rules is the primary law dealing with the varied aspects of how to look at issues related to electronic records and documents, digital signatures, and cybercrime on information, systems etc. The Act also prescribed the offences and fines. Over a period of time the changing technology landscape brought about an amendment in this Act, which is the IT Amendment Act. This further enhanced the scope of cybercrimes and introduced penalties for offences related to data breaches, identity theft, and online harassment.

As per the IT Act, the Computer Emergency Response Team – India (CERT-In) provides guidelines for monitoring, detecting, preventing, and managing cybersecurity Incidents.

As per this, service providers, intermediaries, data centres, body corporates, and Government organisations are obligated to take specific actions or provide information for cyber Incident responses, as well as for protective and preventive measures against cyber Incidents.

National Cyber Security Policy 2023

The objective of this policy is to safeguard both information and the infrastructure in cyberspace. It seeks to establish the capabilities needed to prevent and respond effectively to cyber threats, as well as to minimise vulnerabilities and mitigate the impact of cyber Incidents.

This will be achieved through a combination of institutional structures, skilled individuals, established processes, advanced technology, and collaborative efforts.

The policy is designed to instil a high level of trust and confidence in IT systems. It also aims to fortify the regulatory framework to ensure security and bolster the safeguarding and resilience of the nation's critical information infrastructure (CII).

This will be accomplished by the operation of a 24/7 National Critical Information Infrastructure Protection Centre (NCIIPC) and the enforcement of security practices pertaining to the design, procurement, development, utilisation, and operation of information resources.

Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021

In 2021, India implemented regulations commonly referred to as the Intermediary Rules. These guidelines establish a legal structure governing social media platforms, over-the-top (OTT) platforms, and digital news providers. Additionally, they encompass clauses pertaining to safeguarding data and addressing complaints.

The DPDPA is an Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes. It has a clear mandate for reporting Incidents and fines for not following said mandates.

There is also the upcoming Digital India Act; the Government is presently looking to replace the IT Act with the Digital India Act, which will deal with online safety, trust and accountability, open internet, and regulations of new age technologies like artificial intelligence and blockchain technologies.

The Indian Penal Code also has provisions related to cyber Incidents, although this must be read with the IT Act.

The Central Government launched a National Cyber Crime Reporting Portal, [Hyperlink], to enable citizens to report complaints pertaining to all types of cybercrimes, with a special focus on cybercrimes against women and children.

The Government is also operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), which pro cious programs and free tools for cleaning malicious code as well as tools such as M-K for addressing threats related to mobile phones.

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

As per the IT Act, CII is monitored by the NCIIPC. CII is defined as "facilities, systems or functions whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation".

The NCIIPC is required to monitor and report national-level threats to CII. The critical sectors include:

- Power and energy.
- Banking, financial services, and insurance.
- Telecommunication and information.
- Transportation.
- Government.
- Strategic and public enterprises.

Recently, some private banks such as ICICI and HDFC have also been included.

The NCIIPC has been working on policy guidance awareness programmes and knowledge-sharing documents for getting organisations ready.

The Reserve Bank of India (RBI) has issued a comprehensive Cyber Security Framework for all scheduled commercial banks, which requires all banks to adhere to strict cybersecurity and data protection guidelines. The RBI sets minimum standards and norms for banks and non-banking finance companies, and other lenders and payment services.

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

The Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011, refer to the ISO27001 standards. While this is not defined as mandatory, it is a recommendation to follow these standards.

Similarly, in the recent DPDPA, the measures that need to be adopted include having the appropriate technological and organisational measures as well as taking all steps to prevent Incidents.

The Information Technology Rules, 2013 are responsible for mandating all Indian data centres, service providers, and their intermediates. All intermediaries are required to report any cybersecurity Incidents to CERT-In, the primary task force to:

- Analyse cyber threats, vulnerabilities, and warning information.
- Respond to cybersecurity Incidents and data breaches.
- Coordinate suitable Incident response to cyberattacks and conducts forensics for Incident handling.
- Identify, define, and take suitable measures to mitigate cyber risks.
- Recommend best practices, guidelines, and precautions to organisations for cyber Incident management so that they can respond effectively.

2.4 s: Are organisations required under Applicable Laws, or otherwise expected by a re ry or other authority, to report information related to Incidents or potential Incidents (including cyber threat

of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

As per the CERT-In Rules, organisations now have a six-hour window to report Incidents as mentioned in the Annexure I as under:

i. Targeted scanning/probing of critical networks/systems.
ii. Compromise of critical systems/information.
iii. Unauthorised access of IT systems/data.
iv. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites, etc.
v. Malicious code attacks such as spreading of virus/worm/Trojan/bots/spyware/ransomware/cryptominers.
vi. Attacks on servers such as databases, mail and domain name systems, and network devices such as routers.
vii. Identity theft, spoofing and phishing attacks.
viii. DoS attacks and Distributed Denial of Service (DDoS) attacks.
ix. Attacks on critical infrastructure, supervisory control and data acquisition (SCADA) and operational technology systems, and wireless networks.
x. Attacks on application such as e-governance, e-commerce, etc.
xi. Data breaches.
xii. Data leaks.
xiii. Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers.
xiv. Attacks or Incidents affecting digital payment systems.
xv. Attacks through malicious mobile apps.
xvi. Fake mobile apps.
xvii. Unauthorised access to social media accounts.
xviii. Attacks or malicious/suspicious activities affecting cloud computing systems/servers/software/applications.
xix. Attacks or malicious/suspicious activities affecting systems/servers/networks/software/applications related to big data, blockchain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, and drones.
xx. Attacks or malicious/suspicious activities affecting systems/servers/software/applications related to artificial intelligence and machine learning.

Rule 12 outlines the requirements for service providers, intermediaries, data centres, and corporate entities to notify CERT-In about cybersecurity Incidents.

The CERT-In website also offers details on the channels and formats for reporting such Incidents, along with offering advice on reporting vulnerabilities and following Incident response protocols.

The DPDPA talks of requirements to be maintained to have appropriate technological and organisational measures adopted also as measures to prevent personal data breach.

According to rule 3(1)(l) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, intermediaries are obligated to notify and provide information regarding cybersecurity Incidents to CERT-In, following the guidelines outlined in the CERT-In Rules.

respond to the attacks.

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

The IT Act and specifically the CERT-In and Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011, also known as the SPDI Rules, mandates reporting to the authorities and not to individuals.

The new DPDPA is aimed at creating a framework for this kind of reporting. However, the Rules are yet to be notified and we will get more clarity on the same once the Rules are notified.

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

Please refer to question 2.4.

Further, the IT Act also envisages a Cyber Appellate Tribunal (CAT) wherein any person aggrieved by the orders from the controller or adjudicating officers can prefer an appeal. The CAT is not bound by the Indian Code of Civil Procedure, 1908 (CPC) and instead is at liberty to regulate its own procedures, limited only by the principles of natural justice and the IT Act itself. The CAT has the same powers as are vested in a civil court under the CPC and, while trying a suit, such powers shall include:

- summoning and enforcing the attendance of any person and examining them under oath;
- requiring the discovery and production of documents or electronic records;
- requiring evidence on affidavits;
- issuing commissions for the examination of witnesses or documents;
- reviewing its decisions;
- dismissing an application for default or deciding it *ex parte*; and
- any other matter as may be prescribed.

This comprises a chairperson appointed by the Central Government by notification, as provided under Section 49 of the IT Act 2000 and such a number of other members as the Central Government may notify or appoint.

However, due to the non-availability of a Presiding Officer, it was merged with the Telecom Disputes Settlement Appellate Tribunal (TDSAT) in 2017.

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

The relevant sections of the IT Act, 2000 are tabulated below:

Section	Offence	Penalty
Section 70B (7) of Amendment Act	Section 70B (7) states that any service provider, ries, data centres, body corporate or person who fails to provide the information called for or to comply with the directions of	This is punishable by imprisonment for up to one year or a fine of Rs 100,000, or both. However, this provision applies only to non-compliance

Section 44(b) of the IT Act	Section 44(b) states that if a person who is required to furnish information under this Act or Rules or regulations made thereunder fails to do so, he shall be liable to a penalty.	A penalty not exceeding Rs 150,000 will apply for each failure. This section also states that if a person who is required to furnish information fails to do so within a time specified by the Authority, he shall be liable to a penalty not exceeding Rs 5,000 for each day of delay until the failure continues.
Section 45 of the IT Act	Section 45 provides for a residual penalty. Whoever contravenes any Rules or regulations under the IT Act, where the contravention of which has no specific penalty provided, shall be liable to pay compensation.	Compensation not exceeding Rs 25,000 to the affected party, or a penalty not exceeding Rs 25,000.

In addition to the foregoing points, the newly enacted DPDPA included the following provisions in the Schedule 1:

1.	Breach in observing the obligation of a Data Fiduciary to take reasonable security safeguards to prevent a personal data breach under sub-section (5) of Section 8.	Penalty may extend up to Rs 250 crores.
2.	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (6) of Section 8.	Penalty may extend up to Rs 200 crores.
3	Breach in observance of additional obligations in relation to children under Section 9.	Penalty may extend up to Rs 200 crores.
4.	Breach in observance of additional obligations of a Significant Data Fiduciary under Section 10.	Penalty may extend up to Rs 150 crores.
5.	Breach in observance of the duties under Section 15.	Penalty may extend up to Rs 10,000 crores.
6.	Breach of any other provision of this Act or the Rules made thereunder.	Penalty may extend to Rs 50 crores.

It is pertinent to mention that the Rules under the DPDPA are yet to be notified and we expect some more guidelines to em ed in the *Official Gazette*.

cybersecurity incidents to CERT-In.

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

These laws are still in a nascent stage and jurisprudence is still being set by the enforcement actions taken. As of now, the emphasis is on creating a compliance framework. While quite a few cases have transpired, especially during the COVID-19 pandemic, the *Air India*, *Dr. Lals Pathlab* and *Domino's* cases were at the forefront.

3. Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems): (i) beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content); (ii) honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data); or (iii) sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)?

Though these measures are not specifically stated in the law(s), the organisation in both the Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011 and DPDPA talks of adopting appropriate measures to secure the data. However, this will need to meet the standard principles of privacy and rights of individuals.

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

Yes. At present both in the Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011 and DPDPA the organisations are permitted to do this. It should be noted that the DPDPA will override the Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011 as mentioned.

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

While this is not specifically dealt with in the IT Act, Indian laws do provide for export controls with respect to certain surveillance technologies.

The Government is also looking at controlling through licensing the import of laptops and devices as well as other software.

4. Specific Sectors

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

Yes, it does, as the law is not prescriptive but leaves it on the requirements of a particular business depending on the nature and volume of data being processed.

At present, all organisations strictly follow the compliances set up to follow the mandates of the law as envisioned in the Act and Rules. It is envisioned that once the Digital India Act comes into force, there may be sector-specific laws

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

Various sectors have their own rules and guidelines issued in order to take care of the security of the infrastructure.

The DPDPA brings in the general requirements of how the personal data needs to be handled. However, there are sector-specific regulations and guidelines. The proposed Digital Information Security in Healthcare Act (DISHA) by the Health Ministry provides especially for the protection of healthcare data to third parties. Further, the Government has also released a draft Health Data Management Policy in April 2022, which aims to protect citizens' health data under the Ayushman Bharat Digital Mission.

Similarly, the RBI provides certain rules and guidelines for the financial sector, as well as the Telecom Regulatory Authority of India prescribing guidelines for data collected in the telecom sector. Security is also an important aspect including Incident reporting to the Department of Telecommunications under The Unified License Agreement.

The Insurance Regulatory and Development Authority prescribes similar rules for insurance companies.

5. Corporate Governance

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

While the IT Act and Rules do not directly talk of a breach of directors' or officers' duties, various provisions both in the Act and allied Rules speak of this. Section 85 of the IT Act does require that, in the event of contravention of provisions of the Act, every person who was in charge of and was responsible to the company for the conduct of its business (including a director and any officer) at the time of the contravention shall be: guilty of said contravention; liable to be proceeded against; and punished accordingly. Due diligence or lack of knowledge is a good defence to this.

Also, the Companies Act, 2013 and more specifically The Companies (Management and Administration) Rules, 2014, require that the Board of a company shall appoint a person in the company responsible for the management, maintenance and security of electronic records. Any failure by such person to do so would result in a breach of their duties of care under the law.

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

While the law will never detail these aspects of practice because technology and standards are always fluid, it is important to note the language of the law. In the IT Rules as well as the DPDPA, the language speaks of having appropriate technological and organisational measures and reasonable security safeguards to prevent a breach.

To demonstrate compliance with the applicable laws in India regarding information security, businesses are mandated to undertake several key measures. This includes designating a Chief Information Security Officer (CISO) or an equivalent role, establishing a documented Incident Response Plan or policy, conducting regular cyber risk assessments, which should encompass evaluations of third-party vendors, and performing Pen testing or vulnerability assessments. These actions collectively form a crucial framework for ensuring adherence to legal requirements, safeguarding sensitive information, and fortifying resilience against cyber threats.

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 mandate that all the Intermediaries and other companies operating in the Digital space must appoint a Grievance Redressal Officer. Fur at appropriate grievance redressal mechanisms should be available to all users of social

Similarly, there is a requirement in the NCIIPC guidelines for CIIs to appoint a CISO who heads the department for information security within the companies. This requirement is also echoed by the IRDA so as to have a designated department for the implementation of a requisite framework to ensure cybersecurity.

The IT Rules further provide for appointing a Grievance Redressal Officer who shall act on behalf of the Company to remedy any grievances that are being aired by any of the parties or individuals.

This requirement has been further reinforced by the newly implemented DPDPA and, as a result of this Act, all service providers, intermediaries, data centres, corporate bodies and Government organisations must have a designated person or contact who shall be responsible for acting as the interface with CERT-In or any other Government-appointed body under the new DPDPA.

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

In an effort to ensure transparency and good governance, in India there is a requirement for all companies, whether public or private to bring to the notice of the regulators as soon as any Incidents of data breach or cybersecurity risk are detected. The risk management actions must also be made a part of the annual report of the companies.

In fact, the SEBI guidelines specifically require that the listed companies should disclose instances of data breach or cybersecurity being compromised to the stock exchanges under the "Material Events or Information" reporting.

Similarly, the RBI also mandates the reporting of significant Incidents of data breach or cybersecurity issues at the earliest opportunity and most certainly include the same in the Annual Reports of the Banks along with the risk mitigation measures taken by the Banks.

6. Litigation

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

While there are no specific private remedies available, the IT Act and Rules allow for statutory remedies for affected persons including civil actions under Section 43. Please refer to responses in section 1 and 2.

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

There have been some instances of data breaches that have come to light in the past few years, such as the data of Air India being compromised and order details of Domino's Pizza being leaked online. There was also a case of the COVID-19 vaccination data being leaked online due to the hacking of some Government portals and websites. However, to date, there are no reported instances of companies having been penalised for data breaches in India.

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

The latest legislation, such as the DPDPA, is a step towards defining the roles and responsibilities of the Data Processor and Data Fiduciary. There are serious penalties prescribed under the Act in the event of failure on the part of the Data Fiduciary or Data Processor to prevent the occurrence of instances of a data breach. However, the details of how [illegible] mented will become clear once the Rules under this Act are notified.

7. Insurance

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

Yes, they are. Cybersecurity insurance has now started to become almost mandatory, given the value and volume of fines being levied in different laws.

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

In India, there are typically no specific regulatory restrictions preventing insurance coverage for types of losses like business interruption, system failures, cyber extortion, or digital asset restoration.

Insurance companies in India generally have the freedom to offer policies that cover a wide array of risks, including those associated with cyber Incidents and digital assets. However, the terms and conditions of these policies are subject to the regulations and guidelines established by the Insurance Regulatory and Development Authority of India (IRDAI).

The IRDAI may issue guidelines or regulations governing the structure and terms of insurance policies, including those related to cyber insurance. These guidelines could encompass requirements for disclosing information, policy language, coverage limits, and procedures for filing claims.

7.3 Are organisations allowed to use insurance to pay ransoms?

Organisations are not allowed to use insurance to pay ransoms.

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. anti-terrorism laws) that may be relied upon to investigate an Incident.

Investigatory powers under the various laws

The investigatory powers of the applicable laws are mentioned in various places in the IT Act, read along with the CERT-In guidelines. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:

- collection, analysis, and dissemination of information on cybersecurity Incidents;
- forecast and alerts of cybersecurity Incidents;
- emergency measures for handling cybersecurity Incidents;
- coordination of cybersecurity Incident response activities; and
- issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity Incidents.

The IT Act also envisages a CAT (now merged with the TDSAT) wherein any person aggrieved by the orders from the Controller or adjudicating officers can prefer an appeal. The CAT is not bound by the CPC and instead is at liberty to regulate its own procedures, limited only by the principles of natural justice and the IT Act itself. The CAT has the same powers as vested in a civil court under the CPC and, while trying a suit, such powers shall include:

- summoning and enforcing the attendance of any person and examining them under oath;
- requiring the discovery and production of documents or electronic records;

- reviewing its decisions;
- dismissing an application for default or deciding it *ex parte*; and
- any other matter as may be prescribed.

Further, Section 80 of the IT Act allows the police the power to enter-search and arrest any person in contravention of the Act and having reasonably been suspected to have committed or of committing or being about to commit any offence under this Act.

The current DPDPA also envisages that the Data Protection Board will similarly function and shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in respect of matters relating to:

a. summoning and enforcing the attendance of any person and examining her on oath;

b. receiving evidence of an affidavit requiring the discovery and production of documents;

c. inspecting any data, book, document, register, books of account or any other document; and

d. such other matters as may be prescribed.

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?

Yes, Section 69 of the IT Act allows the Central Government or appropriate agency on its behalf to order the subscriber or person in charge of said computer resource to extend all facilities and technical assistance to intercept, monitor or decrypt the information on a computer resource if the Central Government or agency authorised is satisfied that it is necessary or expedient to do so in the interests of:

- The sovereignty or integrity of India.
- The security of the State.
- Friendly relations with foreign States.
- Public order.
- Preventing incitement of the commission of any cognisable offence – for reasons to be recorded in writing, by order, any agency of the Government is to be directed to intercept any information transmitted through any computer resource.

Section 69-A and 69-B of the IT Act provides for more such powers. Section 69-A talks of blocking of public access of any information through any computer resources, while Section 69-B talks of the power to monitor or collect traffic data or information generated transmitted, received or stored in any computer resource.

Contributors