Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Cybersecurity

India
Anoop Narayanan, Priyanka Gupta and Shree Misra
ANA Law Group

chambers.com

2020

INDIA

Law and Practice

Contributed by:
Anoop Narayanan, Priyanka Gupta and Shree Misra
ANA Law Group see p.87

Contents

1. Basic National Regime

1.1 Laws

The Constitution of India guarantees the right to privacy (which includes right to data security) to all citizens as part of the right to life and personal liberty under articles 19 and 21, and as part of the freedoms guaranteed by Part III of the Constitution. This was also upheld by the Supreme Court of India (SCI) in 2017 in its landmark judgment of Justice K S Puttaswamy (Retd) and Another v Union of India and Others (2017) 10 SCC 1 ("privacy judgment").

India does not currently have a comprehensive cybersecurity law. Cybersecurity, data breach notification and incident response are governed under the Information Technology Act, 2000 (ITA) and the ITA rules in India. The ITA defines "cybersecurity" as "protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction".

Under the ITA, the Indian government has established the Indian Computer Emergency Response Team (CERT-In) as the national nodal agency for cybersecurity, to carry out the following functions:

- collection, analysis and dissemination of information on cyber-incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- co-ordination of cyber-incidents response activities;
- issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber-incidents;
- such other functions relating to cybersecurity as may be prescribed.

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules) prescribe that the CERT-IN will be responsible for responding to cybersecurity incidents and will assist cyber-users in the country in implementing measures to reduce the risk of cybersecurity incidents. The CERT-IN also has powers to issue directions to service providers, intermediaries, data centres, body corporates, etc, for enhancing cybersecurity infrastructure in the country.

The CERT-In Rules mandate the CERT-IN to operate an incident response help desk on a 24-hour basis on all days including government and other public holidays to facilitate reporting of cyber-authority incidents.

Further it is mandatory for the service providers, intermediaries, data centres and body corporates which handle sensitive personal data (SPD) to report all cybersecurity incidents to CERT-In "as early as possible". CERT-In has also set up sectoral CERTs to implement cybersecurity measures at a sectoral level.

The details regarding the methods and formats for reporting cybersecurity accidents, vulnerability reporting and remediation, incident response procedures and dissemination of information on cybersecurity are published on CERT-IN's website and are updated from time to time.

For critical sectors, the government has set up the National Critical Information Infrastructure Protection Centre (NCIIPC) under the ITA, as the nodal agency, and has framed the NCIIPC Rules and guidelines to protect the nation's Critical Information Infrastructure (CII) from unauthorised access, modification, use, disclosure and disruption to ensure a safe, secure and resilient information infrastructure for critical sectors in the country.

The ITA prescribes that any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for by the CERT-IN or comply with the CERT-IN's direction, will be punishable with imprisonment for a term which may extend to one year or with a fine which may extend to INR100,000 (USD1,406) or with both.

The ITA also prescribes deterrence in terms of compensations, penalties and punishments for offences, such as damage to computer system, failure to protect data, computer related offences, theft of computer resource or device, SPD leak, identity theft, cheating by personation, violation of privacy, cyber-terrorism, online pornography including child pornography, breach of confidentiality and privacy, breach of contract, etc.

1.2 Regulators

The ITA mandates the central government to appoint an adjudicating officer to conduct inquiries, and adjudicate matters (ie, contravention of any of the provisions of the ITA or of any rule, regulation, direction or order made thereunder including non-compliance of CERT-IN's direction), with claims for injury or damages valued up to INR5 crores (approximately USD701,881). Claims that exceed this amount must be filed before the competent civil court. Where more than one adjudicating officers are appointed, the ITA mandates the central government to specify the matters and places of jurisdiction of each adjudicating officer.

The inquiry and investigation procedure for the adjudicating officer is provided under the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of

Holding Enquiry) Rules, 2003. Any decision of the adjudicating officer can be appealed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

There are various sector-specific regulators engaged in supervising their relevant intermediaries on the progress of implementation and robustness of cybersecurity frameworks. They regularly conduct cybersecurity and system audits of the intermediaries, which are reported to the relevant regulators.

Sector-specific Regulators

Banking sector

The Reserve Bank of India (RBI) governs both public and private sector banks. The RBI's guidelines prescribe that the RBI can request an inspection any time of any of the banks' cyber-resilience. The RBI has set up a Cyber Security and Information Technology Examination (CSITE) Cell under the Department of Banking Supervision, to periodically assess the progress made by banks in the implementation of the cybersecurity framework (CSF), and other regulatory instructions and advisories through on-site examinations and off-site submissions. The RBI has an internal ombudsman scheme for commercial banks with more than ten branches as a redressal forum, and has proposed to set up an online portal to investigate and address cybersecurity concerns and complaints.

RBI has also released a discussion paper in August 2019, on Guidelines for Payment Gateways and Payment Aggregators, and has directed the payment aggregators to put in place adequate information and data security infrastructure and systems for prevention and detection of frauds, and has specifically recommended implementation of data security standards and best practices like PCI-DSS, PA-DSS, latest encryption standards, transport channel security, etc.

RBI has also obtained ISO 27001 Certification in August 2019 for three of its data centres to ensure administration and protection of key ICT infrastructure in consonance with globally accepted norms.

RBI regularly conducts audits and enquiries into the banks' security frameworks. For instance, RBI has recently imposed monetary penalties of INR3 crore (approximately USD421,000) on SBM Bank (India) Ltd., INR1 crore (approximately USD140,000) on the Corporation Bank and INR1 crore (approximately USD140,000) on the Union Bank of India, for non-compliance of certain RBI directions including non-compliance of cybersecurity framework in banks.

Insurance sector

The Insurance Regulatory and Development Authority (IRDA) is the nodal agency for governance and regulation of the insurance sector in India. The IRDA conducts regular on-site and off-site inspections of insurers to ensure compliance with the legal and regulatory framework. The IRDA also has guidelines on Information and Cyber Security for Insurers (IRDA Cyber Security Policy) that mandates separate information security audit plan for insurers covering IT/technology infrastructure and applications. Some other relevant guidelines issued by IRDA as IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, IRDAI (Maintenance of Insurance Records) Regulations, 2015, and the IRDAI (Protection of Policyholders' Interests) Regulations, 2017, which contain a number of provisions and regulations on data security.

Telecom sector

The telecom operators in India are governed by regulations laid down by the following regulatory bodies:

- the Telecom Regulatory Authority of India (TRAI) (to be renamed the Digital Communications Regulatory Authority of India);
- the Department of Telecom (DoT);
- the TDSAT;
- the Group on Telecom and IT (GOTIT);
- the Wireless Planning Commission (WPC); and
- the Telecom Commission (to be renamed the Digital Communications Commission) (DCC), which also includes information security requirements.

Further, the Unified Access Service Licence (UASL) extends information security to the telecom networks as well as to third-party operators. The regulator requires telecom operators to audit their network (internal/external) at least once a year.

Securities

The Securities Exchange Board of India (SEBI) has issued detailed guidelines to Market Infrastructure Institutions (MIIs) to set up their respective Cyber Security Operation Centre (C-SOC) and to oversee their operations through dedicated security analysts. The cyber-resilience framework also extends to stockbrokers and depository participants.

Health sector

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (IMCR) impose patient confidentiality obligations on medical practitioners. The Ministry of Health and Family Welfare had introduced a draft legislation in 2017, known as the Digital Information Security in Healthcare Act (DISH Act), to regulate the generation, collection, storage, transmission, access and use of all digital health data. The DISH Act also provides for the establishment of a National Digital Health Authority as statutory body to enforce privacy

and security measures for health data, and to regulate storage and exchange of health records.

The expert committee report and the Personal Data Protection Bill, 2019 (PDP Bill) prescribe central government to appoint a Data Protection Authority (DPA) to ensure compliance of the data protection laws, register data fiduciaries, conduct inquiries and adjudication of privacy complaints, issue codes of practice, monitor cross-border transfer of personal data, advise state authorities and promote awareness on data protection. In the case of significant data fiduciaries, the expert committee report and PDP Bill proposes appointment of a data protection officer (DPO) to address data principals' grievances.

1.3 Administration and Enforcement Process

The ITA provides for the appointment of an adjudicating officer to deal with claims of injury or damages not exceeding INR5 crore (approximately USD702,000). MeitY has appointed the Secretary of the Department of Information Technology of each Indian state or union territories as the adjudicating officer under the ITA. A written complaint can be made to the adjudicating officer based on the location of the computer system or the computer network, together with a fee based on the damages claimed as compensation. The adjudicating officer thereafter issues a notice to the parties notifying the date and time for further proceedings and, based on the parties' evidence, decides whether to pass orders if the respondent pleads guilty, or to carry out an investigation. If the officer is convinced that the scope of the case extends to the offence instead of contravention, and entails punishment greater than a mere financial penalty, the officer will transfer the case to the magistrate having jurisdiction.

The first appeal from the adjudicating officer's decisions can be filed before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), and the subsequent appeal before the High Court.

The PDP Bill prescribes filing the complaint before the data protection officer, which can be appealed before the adjudicating officer of the DPA, who will have the authority to impose penalties on the data fiduciary. The maximum penalty for violation of the PDP Bill's provisions is INR15 crores (approximately USD2 million) or 4% of the data fiduciary's total global turnover in the preceding financial year, whichever is higher. PDP also prescribes imprisonment of up to three years and/or penalty up to INR200,000 (approximately USD2800) against any persons who knowingly or intentionally and without the consent of data fiduciary re-identifies personal data which has been de-identified by a data fiduciary/data processor, or re-identifies and processes such personal data. The aforesaid offences under PDP are cognisable (ie, the police has the power to arrest the offender without a court warrant) and non-bailable.

The PDP Bill proposes the central government to establish an appellate tribunal to adjudicate on appeals from the orders of the DPA, and the SCI as the final appellate authority for all purposes under the PDP Bill.

1.4 Multilateral and Subnational Issues

India does not have state-specific cybersecurity laws or regulations. However, several state governments have taken initiatives to promote cybersecurity. For example, the Maharashtra State Government has launched the Cyber Safe Initiative in January 2020 to spread awareness regarding laws on cybercrime, bank frauds, child pornography, online gaming, cyberdefamation, false information sites, etc. Further, the Karnataka government had established a Centre of Excellence in Cyber Security to build awareness and facilitate innovation, standardisation and best practices for cybersecurity.

1.5 Information Sharing Organisations

The following non-governmental authorities assist the Indian government in cybersecurity measures:

- the Data Security Council of India (DSCI) – a not-for-profit industry body under the National Association of Software and Services Companies (NASSCOM) that engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity-building and outreach activities;
- National Cyber Safety and Security Standards (NCSSS) – a self-governing body to protect the CII from cyber-related issues;
- the Internet and Mobile Association of India (IAMAI) – a not-for-profit industry body that addresses the issues, concerns and challenges of the internet and mobile economy;
- the Cellular Operators Association of India (COAI) – an industry association of mobile service providers, telecom equipment, internet and broadband service-providers in India, which interacts directly with ministries, policy-makers, regulators, financial institutions and technical bodies;
- the Internet Service Providers Association of India (ISPAI) – the recognised apex body of Indian ISPs worldwide; and
- the Computer Society of India (CSI) – a non-governmental organisation of professionals, including software developers, scientists, academicians, project managers, etc, which contributes to the government's formulation of information technology strategy and planning.

1.6 System Characteristics

Similar to world CERTs, Cert-In is the national nodal agency for responding to computer security incidents as and when they occur. CERT-In operates on similar principles as other CERTs, such as:

- collection, analysis and dissemination of information on cyber-incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- co-ordination of cyber-incident response activities;
- issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber-incidents.

Further, the Indian cybersecurity laws follows the United Kingdom (UK) cybersecurity model. For example, the primary institutional authorities for critical information infrastructure (CII) in both jurisdictions are similar, such as the CIIPC in India and the National Cyber Security Centre in the UK. India and UK also have similar emergency response authorities, such as CERT-In and CERT-UK.

Additionally, the UK has a central authority, the National Cyber Security Centre, that co-ordinates between the UK government and its various industry stakeholders in cybersecurity matters. The MeitY is in the process of establishing a similar authority in India, known as the National Cyber Coordination Centre (NCCC), which will be implemented by CERT-In.

There are certain fundamental dissimilarities in the cybersecurity regimes of both India and the UK. For instance, the UK does not have a comprehensive legal framework in respect of information technology and cybersecurity, whereas India has a comprehensive legislation to govern information technology and cybersecurity (the ITA). Also, in the absence of all-inclusive cybersecurity framework, the various executive authorities in the UK function under separate laws (the Security Services Act, 1989, or the Civil Contingencies Act, 2004). Whereas, the central authorities for cybersecurity in India are established and operationalised under the ITA, and the various rules thereunder.

1.7 Key Developments

In September 2019, the RBI issued guidelines for payment gateways and payment aggregators to establish a mechanism for monitoring, handling and follow-up of cybersecurity incidents and breaches. The guidelines mandate all cyber-incidents and breaches to be reported immediately to the Department of Payment and Settlement Systems (DPSS) under the RBI, and to CERT-In. Under the guidelines, the Payment Gateways and Payment Aggregators are prohibited from storing the customer card credentials within their database or the servers accessed by the merchants. The Payment Gateways and Payment Aggregators must submit the System Audit Report, including cybersecurity audit conducted by CERT-In empanelled auditors, within two months of the close of their financial year to DPSS.

In August 2019, the RBI issued a Cyber Security Playbook (CSP) to provide a clear understanding of an incident response plan, and responsibilities of key persons towards cybersecurity standards and accepted practices before, during, and after a cybersecurity incident. CSP provides for aligning IT and business continuity plans, and specific communications, such as periodic situation updates, response options to proactively mitigate impacts of attempted and successful exploits.

In December 2019, the RBI has released a comprehensive cybersecurity framework for primary (urban) co-operative banks (UCBs).

In April 2019, the central government approved the National Policy on Software Products, 2019 (the Software Policy), which aims to develop India as a global hub for software products, and the information and communication technology sector. As part of its strategy to promote entrepreneurship and innovation for employment, the Software Policy provides establishing a common upgradable infrastructure for start-ups and software product designers to identify and plug cybervulnerability.

1.8 Significant Pending Changes, Hot Topics and Issues

The MeitY and Data Security Council of India (DSCI) had launched an initiative, the Grand Challenge for Cyber Security, to promote innovation and entrepreneurship by building key cybersecurity capabilities in India. The initiative seeks to provide impetus to the growth of Indian cybersecurity industry, and nurture start-ups which aim to diversify the industry and develop advanced solutions.

To address near-real-time situational awareness and rapid response to cybersecurity incidents in India, the central government has proposed to set up the National Cyber Coordination Centre (NCCC), a multi-stakeholder central authority, to provide an overview of cybersecurity breaches and threats in India. With the help of NCCC, the government proposes to scan the Indian cyberspace and generate near-real-time situational awareness. NCCC is being implemented in India by the Indian Computer Emergency Response Team (CERT-In). The government is, currently, operationalising the final phase of the NCCC.

2. Key Laws and Regulators at National and Subnational Levels

2.1 Key Laws

The ITA and the IT rules are applicable for the protection of data, computer systems, and infrastructures in India.

The ITA protects data which is defined as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer print-outs, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer".

ITA protects data and computer systems, including computers, computer resources and computer networks from unauthorised access, downloads, and extraction of data, database and information, computer contaminant or virus, damage, disruption, denial of access by authorised persons, theft, concealment, destruction and alteration of computer source code, etc. The ITA also provides compensations, penalties and punishments in respect of offences related to the aforesaid activities.

The DP Rules prescribes protection of personal information and SPD. The DP Rules define personal information as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person". Further, the DP Rules recognise the following as SPD:

- password;
- financial information, such as bank account, credit card or debit card, or other payment instrument details;
- physical, physiological and mental health condition;
- sexual orientation;
- medical records and history;
- biometric information;
- any detail relating to the above as provided to body corporate for providing service; and
- any of the information received from a body corporate in respect of the above, for processing, stored or processed under lawful contract or otherwise.

The CERT-In Rules require mandatory reporting of all cybersecurity incidents to the CERT-In at the earliest and in a prescribed format. The CERT-In is the central authority for reporting cyber-incidents, which analyses trends and patterns in intruder activities, determines the scope, priority and threat of a cyber-incident and develops preventive strategies against cybersecurity incidents.

The ITA, the NCIIPC Rules and guidelines prescribe protection of India's CII from unauthorised access, modification, use, disclosure and disruption, and ensure a safe, secure and resilient information infrastructure for critical sectors. The NCIIPC as the nodal agency under the NCIIPC Rules, essentially protects and delivers advices aimed at reducing vulnerabilities of CII against cyberterrorism, cyberwarfare and other threats.

The National Cyber Security Policy, 2013 aims to create a cybersecurity framework, which leads to specific actions and programmes to enhance the security posture of India's cyberspace. The Cyber Security Policy prescribes various objectives, which include:

- to create a secure cyber-ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy;
- to create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology and people);
- to strengthen the regulatory framework for ensuring a secure cyberspace ecosystem;
- to enhance and create national and sectoral level 24x7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions;
- to enhance the protection and resilience of the CII by operating NCIIPC, and mandating security practices related to the design, acquisition, development, use and operation of information resources;
- to enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizens' data and for reducing economic losses due to cybercrime or data theft;
- to enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

The Payment and Settlement Systems Act, 2007, mandates all information received by the RBI from payment system and system provider to be confidential, subject to certain safeguarding interests, such as: protection of the integrity, effectiveness and security of the payment system; the interest of banking or monetary policy; the operation of the payment systems generally, or in public interest.

The Companies (Management and Administration) Rules, 2014, mandate adequate cybersecurity in respect of an electronic voting system, which is used by members of a company to exercise their right to vote at general meetings.

2.2 Regulators
As India currently does not have a specific DPA, cybersecurity issues are adjudicated by an adjudicating officer appointed under the ITA, having the powers of a civil court.

2.3 Overarching Cybersecurity Agency
At present, there is no overarching cybersecurity agency for India similar to ENISA.

2.4 Data Protection Authorities or Privacy Regulators
Currently, the Indian laws do not prescribe for data protection authorities. However, the PDP Bill prescribes establishment of a DPA for addressing issues related to data privacy and protection. Under the PDP Bill, a complaint can be filed before a data protection officer, which can be appealed before an adjudicating officer of the DPA. The DPA will have the authority to impose penalties on any data fiduciary, with a maximum penalty for violation of the PDP Bill's provisions as INR15 crores (approximately USD2 million) or 4% of the data fiduciary's total global turnover in the preceding financial year, whichever is higher.

2.5 Financial or Other Sectoral Regulators
The RBI is the nodal banking and financial sector regulator in India. The sub-CERT for the banking and finance sector is the Institute for Development and Research in Banking Technology (IDRBT), which is an autonomous centre for development and research in banking technology set up by the RBI. The IDRBT owns the Indian Financial Network (INFINET), which is the communication backbone for the banking and finance sector in India.

The RBI's Regulations, and Guidelines on Information Security, Electronic Banking, Technology Risk Management, and Cyber Frauds (the RBI Cyber Security Guidelines), provide detailed guidance on information technology governance for banks in India.

The RBI has also issued guidelines on CSF in banks, prescribing banking companies to have an adaptive incident response, management and recovery framework to deal with adverse incidents and disruptions.

The Finance Minister has proposed to establish a CERT-FIN, which will act as an umbrella CERT for the finance sector. The RBI will be the lead regulator, until such CERT-FIN is set up.

SEBI has also issued guidelines on Cyber Security and Cyber Resilience for Stock Exchanges, Clearing Corporation and Depositories. Further, the IRDA has issued guidelines on Information and Cyber Security for Insurers, for cybersecurity protection of information in relation to the policyholders.

2.6 Other Relevant Regulators and Agencies
There are CERTs established under the Ministry of Power to mitigate cybersecurity threats in power systems, and four sub-CERTs for transmission, thermal, hydro and distribution to coordinate with power utilities.

The Information Technology (Intermediaries Guidelines) Rules, 2011, under the ITA, impose an obligation on any intermediary to report cyber-incidents to the CERT-In.

3. Key Frameworks

3.1 De Jure or De Facto Standards
The Information Technology (Reasonable Security Practices and Procedures ad Sensitive Personal Data or Information) Rules, 2011 (the DP Rules) prescribe reasonable security practices that should be supplemented by documented information security programmes and policies. One such security standard prescribed is the International Standard on Information Technology Security Techniques and Information Security Management System Requirements, such as the ISO 27001, and the use of codes of best practices created by self-regulatory bodies.

Further, in 2017, the RBI had announced a project to implement the RBI's guidelines for information security using COBIT 5 standards.

3.2 Consensus or Commonly Applied Framework
There is no consensus or commonly applied framework for reasonable security, and the regulators have recommended a sector-wise framework based on various factors, including risk-based elements.

CERT-In operates on the aspects of "identifying" the cybersecurity risks and the incidents, "containment" of the cyber-breach incident and minimise damage, "eradication" of cause of incident and "recovery" to restore normal operations.

Under the ITA, the reasonable security practices and procedures include the security practices that are designed to protect any information from unauthorised access, damage, use, modification, disclosure or impairment, and are specified in a contractual agreement, or any law or as prescribed by the central government.

The DP Rules prescribe the following criteria to comply with the "reasonable security" practices and procedures:

- the entities must implement the security practices and standards; and
- there must be a comprehensive documented information security programme and policies, containing managerial, technical, operational and physical security control measures, that are commensurate with the information assets being protected with the nature of business.

3.3 Legal Requirements

Written Information Security Plans or Programmes
The DP Rules prescribe the body corporates to have a comprehensive documented information security programme and security policies containing managerial, technical, operational and physical security measures.

Incident Response Plans
There is no statutory requirement under the cybersecurity laws to maintain an incident response plan. The Protected System Rules prescribe the central and state governments to implement a Cyber Crisis Management Plan for rapid identification, information exchange, swift response, and remedial actions to recover from malicious cyber-related incidents in the critical sectors.

The RBI requires banks to have a written incident response programme and cybersecurity policy to handle cyberthreats, and a cybercrisis management plan addressing detection, response, recovery and containment. The RBI requires mandatory reporting of cyberbreach incidents within two to six hours of the incident.

The IRDA requires the insurers to have an incident response plan.

Appointment of Chief Information Security Officer or Equivalent
The NCIIPC guidelines recommend that all CIIs have an information security department headed by a CISO.

The RBI's Cyber Security Guidelines mandate the appointment of a chief information security officer (CISO), along with a security steering committee in public/private sector banks, who must report any incident directly to the bank's head of risk management.

The IRDA also requires the appointment of a CISO for implementing a cybersecurity framework.

The DP Rules provide for the appointment of a grievance officer to redress the information provider's grievances.

Involvement of Board of Directors or Equivalent
The RBI and IRDA guidelines require involvement of the board of directors to approve cybersecurity policies and cybercrisis management plans, and take overall responsibility for information security governance framework.

Conducting Internal Risk Assessments, Vulnerability Scanning, Penetration Tests, etc
The DP Rules do not prescribe conducting internal risk assessments, vulnerability scanning, penetration tests, etc. The RBI mandates banks to have periodical vulnerability assessment and penetration testing exercises for all critical systems. The IRDA also has cybersecurity policy which recognises the need for testing programmes, vulnerability assessments and penetration tests.

Multi-factor Authentication, Anti-phishing Measures, Ransomware, Threat Intelligence
The RBI has issued guidelines for banks to implement two-factor/multi-factor authentication to protect the customer account data and transaction details' confidentiality, and in order to combat cyber-attacks by phishing, keylogging, spyware/malware, etc, that are targeted at banks and their customers.

Insider Threat Programmes
There is no insider threat programme or standards under the current Indian cybersecurity framework.

Vendor and Service Provider Due Diligence, Oversight and Monitoring
The DP Rules do not have any provisions for vendor/service provider due diligence or monitoring. The IRDA, TRAI and RBI respective sectoral guidelines on outsourcing and cloud services provide guidance for companies and banks to carry out due diligence, audits and regular monitoring on vendors and service providers.

Use of Cloud, Outsourcing, Offshoring
The MeitY guidelines for government use of cloud services prescribe that the service providers must store the data within India. If the data is located in one or more discreet sites in foreign countries, the conditions for data location have to be mentioned in an agreement with the service-providers.

The telecom regulations prohibit telecom companies from transferring customer account information outside India.

Training
The DP Rules do not prescribe any training requirements. The CERT-In prescribes stakeholders and other entities to conduct training on technical know-hows. The RBI and IRDA also prescribe regular training and security awareness to human resources on cybersecurity policies and programmes.

3.4 Key Multinational Relationships
India–US cyber-relationship (signed on 30 August 2016) (valid for five years): India and the US have signed a memorandum of understanding (MoU) to co-operate on cybersecurity mechanisms and information sharing.

India–Israel on cybersecurity (signed 15 January 2018): India and Israel have signed an MoU to develop, promote and expand co-operation in the field of human resources development (HRD) through platforms such as training programmes and skills development.

India–UK on cybersecurity (signed 20 May 2016): the CERT-In and CERT-UK have signed an MoU to promote co-operation for exchange of knowledge and experience in detection, resolution and prevention of security-related incidents.

India–Brazil on cybersecurity (signed 25 January 2020): India has signed 15 MoUs with Brazil on 25 January 2020 in respect of various issues, including co-operation in cybersecurity, and addressing information and communication technologies-related issues.

India has also signed MoUs with Australia, Bangladesh, Indonesia, Kenya, Portugal, Serbia, the UAE, Vietnam, France, Malaysia, Mauritius, Morocco, Qatar and Singapore on cybersecurity co-operation.

Further, India has signed mutual legal assistance treaties (MLAT) with nearly 35 countries for cross-border co-operation in respect of access to data in different countries.

4. Key Affirmative Security Requirements

4.1 Personal Data
The DP Rules requires all body corporates to implement reasonable security practices and standards, as well as to document their security programmes and policies.

Similarly, the RBI requires banks to classify data based on business complexity and risk levels, and the sensitivity criteria of a bank. The IRDA cybersecurity policy also provides that systems must be classified under different categories based on their criticality and severity.

4.2 Material Business Data and Material Non-public Information
There is no specific security requirement provision in respect of material business data and material non-public information.

4.3 Critical Infrastructure, Networks, Systems
The National Critical Information Infrastructure Protection Centre (NCIIPC) is the nodal agency for protection of Critical Information Infrastructure (CII), networks and systems in the country. The NCIIPC guidelines recommend that cybersecurity breach incidents must be reported to the NCIIPC. The NCIIPC regularly advices on reducing vulnerabilities of the CII, and against cyberterrorism, cyberwarfare and other threats.

The NCIIPC guidelines prescribe development of audit and certification agencies for protection of CII. The NCIIPC also exchanges cyber-incidents and other information relating to attacks and vulnerabilities with CERT-In and concerned organisations in cybersecurity in India.

4.4 Denial of Service Attacks
There are no specific provisions relating to security requirements to prevent denial of service (DoS) attacks, under the ITA or the DP Rules. The NCIIPC guidelines and the sectoral cybersecurity guidelines prescribe preventive and corrective measures to address DoS attacks and similar attacks on systems. Further, the NCIIPC regularly advices on vulnerabilities based on latest DoS attack incidents, which can be accessed on its website: https://nciipc.gov.in.

4.5 Other Data or Systems
There are no specific security provisions for other data or systems under the current cybersecurity regime.

5. Data Breach Reporting and Notification

5.1 Definition of Data Security Incident or Breach
The CERT-In Rules define a cyber-incident as "any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality integrity, or availability, of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a nega-

tive impact on the national economy, or diminishes the security posture of the nation".

The CERT-In Rules also define cybersecurity incident 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 for processing or storage of information or changes to data, and information without authorisation."

"Cybersecurity breaches" is also defined under the CERT-In Rules as "unauthorised acquisition or unauthorised use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource".

Cybersecurity incidents prescribed under the CERT-In Rules must be mandatorily reported, including:

- targeted scanning/probing of critical networks/system;
- compromise of critical systems/information;
- unauthorised access of IT systems/data;
- defacement of a website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites, etc;
- malicious code attacks such as the spreading of viruses/worms/Trojans/botnets/spyware;
- attacks on servers such as databases, mail and DNS and network devices such as routers;
- identity theft, spoofing and phishing attacks;
- denial of service (DoS) and distributed denial of service (DDoS) attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on application such as e-governance, e-commerce, etc.

5.2 Data Elements Covered

The data to be provided while incident reporting includes the sector details, location of the system, date and time of the occurrence, criticality, affected system/network, symptoms observed, and the relevant technical information such as type of incident, number of hosts affected, security systems deployed, actions to mitigate the damage, etc.

The PDP Bill also defines personal data breaches and mandates data fiduciaries to report any personal data breach that may cause harm to the data principal to the DPA.

5.3 Systems Covered

The ITA covers computer systems, and networks, resources, data and database.

5.4 Security Requirements for Medical Devices

Currently, there are no specific cybersecurity guidelines for medical devices, and the DP Rules and the NCIIPC guidelines apply. These include classifying data based on criticality, preparing a documented cybersecurity programme, appointing a CISO, etc.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

There is no specific cybersecurity framework and the security requirements under the DP Rules and CERT-In Rules are applicable to industrial control systems.

5.6 Security Requirements for IoT

There is no specific statutory provision that applies to security requirements for the internet of things (IoT). The data privacy principles under the DP Rules are applicable. However, MeitY's draft IoT Policy, 2015 (yet to be approved), proposes to appoint a nodal organisation for formalising privacy and security standards, and create a national expert committee for developing and adopting IoT standards in the country.

5.7 Reporting Triggers

Incidents specified under the CERT-In Rules must be mandatorily reported to CERT-In. Data breaches in certain specific sectors such as finance, insurance and securities must be reported to the respective regulators. Cybersecurity incidents must be reported to the CISO.

There is no statutory requirement to report a cybersecurity incident to other companies or organisations. Contractually, a body corporate may require the vendor or service provider to promptly report any incident to the company.

5.8 "Risk of Harm" Thresholds or Standards

There are no "risk of harm" thresholds or standards under the current privacy regime. The PDP Bill prohibits processing of such information that could cause harm or significant harm to the data principals.

6. Ability to Monitor Networks for Cybersecurity

6.1 Cybersecurity Defensive Measures

The relevant laws in India that govern network monitoring and cybersecurity defensive measures are:

- the ITA;
- the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the Interception Rules);
- the DP Rules;
- the CERT-In Rules;
- the NCIIPC Rules; and
- the Sectoral Cyber Security Framework Policies.

The ITA provides a legal framework to address hacking and security breaches of IT infrastructure and prescribes penalties for negligently handling SPD. Furthermore, to the extent that the data intercepted and monitored by a body corporate includes the SPD of its customers or employees, the body corporate must comply with the DP Rules.

The Interception Rules prescribe that no person shall carry out any interception, monitoring or decryption of any information generated, transmitted, received or stored in any computer resource, unless authorised by India's central or state governments. There is a lack of clarity on whether a company's interception and monitoring of its internal servers will conflict with the above restriction.

In addition, India does not have any specific laws relating to employee monitoring and thus companies can monitor their networks and servers.

In the privacy judgment and the expert committee report, the courts have ruled that monitoring of employee communications and employee surveillance must be handled carefully, and recommends maintaining a balance between an employee's privacy and the employer's legitimate need to safeguard the company's interest, until the new privacy law is enforced.

The sectoral cybersecurity policies for banks, insurance companies, telecom companies and CII permit body corporates, including banks, to monitor the secure status of each system and network, mobile and home-working procedures, and critical systems. These may include third-party providers.

The UASL obliges telecom companies to monitor all intrusions, attacks and fraudulent activity on its technical facilities and report to the DoT.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Intersection of cybersecurity and privacy is an important point of discussion, more so due to increasing unauthorised data access through cyber-attacks, third-party data sharing and data compromises.

Existing privacy laws and cybersecurity laws include data breach notification requirements. However, these breach notification requirements function directly at the intersection of security and privacy.

Data protection requires protecting against unauthorised data access, regardless of how it occurs, while simultaneously securing sharing of data.

The DP Rules mandate compliance with reasonable security practices and procedures by documenting information security programme and information security policies, and adhering to security standards, such as ISO270001, or to government-approved codes of best practices.

Despite the statutory mandate, various cybersecurity breaches have led to the exposure of personal data and SPD (as discussed in Section 8.4). In 2018, the personal data of more than 100 million users of the Indian business listing website, Justdial (www.justdial.com) was leaked and made publicly available from its old mobile application, which did not maintain adequate security on four application programme interfaces (APIs).

In 2019, WhatsApp was questioned by the government for not disclosing the cyber-attack by the Pegasus malware to Cert-In, which incident targeted many Indians' data. It is unclear whether the breach reporting by WhatsApp was adequate and prompt.

Further, it is unclear whether CERT-In had analysed WhatsApp's reporting, ascertained the inadequacy, and demanded additional information despite rating the vulnerability severity as "high" in its report.

A larger concern that remains is about people who are impacted with such cyber-attacks. In the absence of any statutory provision to notify the impacted persons and assess their loss, the reporting mechanism does not provide any direct benefits or remedies to the impacted persons.

Hopefully, the PDP Bill containing stringent provisions brings some respite to the situation.

7. Cyberthreat Information Sharing Arrangements

7.1 Required or Authorised Sharing of Cybersecurity Information

There is no statutory provision mandating the sharing of cybersecurity information with the government.

7.2 Voluntary Information Sharing Opportunities
Indian laws do not restrict or mandate any individual/body corporate to share voluntarily any information regarding cyberthreats with government agencies.

8. Significant Cybersecurity and Data Breach Regulatory Enforcement and Litigation

8.1 Regulatory Enforcement or Litigation
Please refer to **8.4 Significant Private Litigation**.

8.2 Significant Audits, Investigations or Penalties
Please refer to **1.2 Regulators**.

8.3 Applicable Legal Standards
There are no applicable legal standards. Instances of cybersecurity breach are adjudicated on a case-by-case basis.

8.4 Significant Private Litigation
There were no significant reported private litigations involving cybersecurity allegations or data security incidents/ breaches in India in the past year.

- India has reportedly witnessed 3.9 lakhs cybersecurity incidents in 2019, which is an 89% rise from the 2,08,456 cases reported in 2018.
- The RBI had reported more than 50,500 cybersecurity and banking frauds involving certain scheduled commercial banks in India in 2019, and had resulted in losses worth INR145 crores (USD 20,358,100 approximately).
- In 2019, the WhatsApp Messenger was attacked by a targeted snooping spyware, Pegasus, which gave the attackers unauthorised access to all the information stored on the users' mobile phones. This was one of the major cybersecurity breaches in 2019, and affected over 1,400 government officials, lawyers, journalists and civil rights activists all over the world, including in India.
- In May 2019, a cybersecurity breach involving the Swedish mobile application, Truecaller, leaked and sold the data of 300 million Indian users of the app in the dark web for USD2,100.
- Nearly 6.8 million users' personal and health data were stolen from an Indian healthcare website in February 2019.
- In October 2019, a North Korean malware had reportedly infected and extracted the data from the computer systems of an Indian nuclear power plant, Kudankulam Nuclear Power Plant.

8.5 Class Actions
Other than under the Companies Act, India does not have any laws enabling class action lawsuits. Under the Companies Act, shareholders or depositors can collectively approach the National Company Law Tribunal for redress where, for example, a company's affairs are not managed in its best interests.

9. Due Diligence

9.1 Processes and Issues
There is no prescribed procedure for conducting diligence in corporate transactions in relation to cybersecurity. The companies normally demand the target company's cybersecurity policy and framework, the annual audit reports on cybersecurity measures, and details of any past breaches and reporting in that regard.

9.2 Public Disclosure
There is no specific legal provision requiring mandatory disclosure of cybersecurity risk profile or experience.

9.3 Other Significant Issues
India is set to enforce the PDP Bill. There will be higher awareness and focus on data privacy and cybersecurity. The government and other organisations have been working on developing policies and frameworks in respect of machine learning and artificial intelligence for cybersecurity solutions, anomaly detection and response, and on IoT infrastructure for automation and efficiency, specifically for the CII. Government and the corporations will have to further secure the cloud-based model and the data stored in the cloud. Concepts such as blockchain to prevent data theft may also be in demand.

India is witnessing significant rise in instances of data breach and will need to set up more cyberdefence centres to address the issue.

On the other hand, India is facing a shortage of cybersecurity skills in the workplace. Certain authorities like CERT-In and RBI have been pro-actively conducting skill development activities and create awareness to deal with the increasing cyber-incidents.

ANA Law Group is a full-service law firm based in Mumbai, with a team of experienced professionals who have broad industry knowledge and specialisation across a wide spectrum of business areas. It has significant experience in counselling international clients on issues related to data protection and privacy in India, and regularly represents clients from industries such as banking and insurance, online gaming, finance, luxury goods, consumer goods, healthcare, payroll-processing, pharmaceuticals, telecommunications and internet service providers, credit research and employee screening. The firm also assists international companies with global privacy law involving Indian projects, the drafting and negotiating of contracts with Indian counterparts, and the preparation of data protection and privacy policies for international companies operating in India and their Indian subsidiaries. More specifically, it advises clients on permitted data processing, consent requirements, data collection, retention and disclosure, regulatory requirement compliance, transfers of sensitive personal data within and outside India, on security breaches and drafting security breach policies, on international compliance projects, and on prosecutions and offences.

Authors

Anoop Narayanan is the founder of ANA Law Group and has been in practice for more than 25 years. He has vast advisory and transactional experience in all areas of Indian law as well as being a distinguished employment, technology and intellectual property law expert. As regards employment law practice, Mr Narayanan focuses on a range of issues related to employment in information technology, manufacturing, retail, pharmaceuticals, etc. His clients include multinational corporations, law firms from around the world and Indian companies and individuals. He has regularly advised on the setting up of Indian employment platforms for overseas companies, compensation-structure-related documentation, legal assistance on complex senior-management terminations, strategies to handle sexual harassment complaints in India, structuring industry specific and substantially enforceable non-compete and non-solicitation obligations, ownership of employee developed intellectual property and data privacy. Mr Narayanan is a member of the International Bar Association (IBA), as well as the American Bar Association (ABA), and has spoken on Indian employment law issues at various international conferences organised by the IBA. Mr Narayanan consistently speaks at a number of Indian and international forums on his areas of practice and has also published many articles in leading national dailies touching upon several areas of Indian law.

Priyanka Gupta is a senior attorney at ANA Law Group who has been in practice for more than 12 years. She is qualified from a premier law school and has strong domain knowledge. She regularly advises on international TMT transactions and regulatory aspects of the Indian telecoms sector. Ms Gupta also advises multinational banks, financial institutions, technology businesses and other companies on data protection and privacy law issues. She has extensive experience in handling advisory, transactional and litigation projects in all areas of TMT and IP practice.

Shree Misra is an attorney with the firm's data privacy and intellectual property practice group. She is an LLM graduate from the University of New South Wales, Australia, with specialisation in innovation law and special focus on cybercrime, security and digital law enforcement. She regularly advises international clients on data privacy and cybersecurity-related issues in transactional, compliance and regulatory matters.

ANA Law Group

Indiabulls Finance Centre
Tower-2, 11th Floor
1103 Elphinstone Road
Mumbai – 400 013

Tel: +91 22 6112 8484
Fax: +91 22 6112 8485
Email: mailbox@anaassociates.com
Web: www.anaassociates.com