PANORAMIC

CYBERSECURITY

India

LEXOLOGY

Cybersecurity

Contributing Editors

Edward R McNicholas and Fran Faircloth

Ropes & Gray LLP

Generated on: February 13, 2024

Contents

Cybersecurity

Recent developments and future changes

Contributors

India

AZB & Partners

Sumit Ghoshal	sumit.ghoshal@azbpartners.com
Aprajita Rana	aprajita.rana@azbpartners.com
Shagun Badhwar	shagun.badhwar@azbpartners.com
Suyash Tiwari	suyash.tiwari@azbpartners.com

LEGAL FRAMEWORK

Key legislation

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

While India does not have a dedicated cybersecurity law, there are several legislations and sector-specific regulations that, among others, regulate cybersecurity, and promote the maintenance of cybersecurity standards. One of the primary legislations dealing with cybersecurity, data protection and cybercrimes is the Information Technology Act 2000 (the IT Act), read with the rules and regulations framed thereunder. The IT Act not only provides legal recognition and protection for transactions carried out through electronic data interchange and other means of electronic communication, but also contains provisions that are aimed at safeguarding electronic data, information or records, and preventing unauthorised or unlawful use of a computer system. Some of the cybercrimes that are specifically envisaged and punishable under the IT Act are hacking, denial-of-service attacks, phishing, malware attacks, identity fraud and electronic theft.

In accordance with the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, the Computer Emergency Response Team (CERT-In) has been established as the nodal agency, which deals with cybersecurity incidents and responding to these incidents. It is tasked with performing certain functions including collection, analysis and dissemination of information on cyber incidents, issuing guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, response and reporting of cyber incidents. To perform these functions, CERT-In is empowered to call for information and issue directions to service providers, intermediaries, data centres, body corporates and any other person. Exercising such powers, CERT-In had issued the directions dated 28 April 2022 (CERT-In Directions) for strengthening cyber security in India. Clarifications to the Directions were issued by CERT-In by way of frequently asked questions on 18 May 2022 (FAQs).

In addition to the above, other relevant rules framed under the IT Act in the context of cybersecurity include:

- the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules), which prescribe reasonable security practices and procedures to be implemented for collection and the processing of personal or sensitive personal data. Once the Digital Personal Data Protection Act 2023 (DPDP Act), which has been notified but is yet to be made effective, comes into force the SPDI Rules will stand replaced. The DPDP Act stipulates that a data fiduciary is required to protect the digital personal data of an individual in its possession or under its control (including in respect of processing undertaken by it or on its behalf) by taking reasonable security safeguards to prevent personal data breach. However, unlike the SPDI Rules, the DPDP Act does not recognise any specific standards to be followed. Having said that, more clarity on specific security standards and safeguards to be implemented under the DPDP Act may emerge once the rules under the Act are framed and notified thereunder;
- the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018, which require specific information security measures

to be implemented by organisations that have protected systems, as defined under the IT Act; and

- the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (the Intermediaries Guidelines) require intermediaries to implement reasonable security practices and procedures for securing their computer resources and information contained therein. The intermediaries are also required to report cybersecurity incidents (including information relating to such incidents) to CERT-In.

Other laws that contain cybersecurity-related provisions include the Indian Penal Code 1860, which punishes offences, including those committed in cyberspace (such as defamation, cheating, criminal intimidation and obscenity), and the Companies (Management and Administration) Rules 2014 (the CAM Rules) framed under the Companies Act 2013, which require companies to ensure that electronic records and security systems are secure from unauthorised access and tampering.

In addition to the above, there are sector-specific regulations issued by regulators such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India, the Department of Telecommunication (DOT) and the Securities Exchange Board of India (SEBI), which mandate cybersecurity standards to be maintained by their regulated entities, such as banks, insurance companies, telecom service providers, and listed entities.

The proposed Digital India Act 2023 (DIA) that will replace the IT Act can be expected to bring a robust and dedicated law dealing with cybersecurity.

Law stated - 9 December 2023

Most affected economic sectors

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

Regulated entities operating in sensitive sectors, such as financial services, banking, insurance, and telecommunications, have exhibited higher standards of cybersecurity preparedness and awareness, partly because of regulatory intervention but also because of voluntary compliance with advanced international standards. Sectors such as e-commerce, IT and IT-enabled services that have seen an infusion of foreign direct investment have also proactively deployed robust cybersecurity frameworks and policies to counter the evolving nature of cyber fraud as they have borrowed advanced cybersecurity practices and procedures from their overseas parent entities in the United States, the European Union and other jurisdictions.

With the rise of digital payments, cybercrimes involving payment transactions in the online space have significantly increased and become complex. While the RBI has been active in requiring companies operating payment systems to build secure authentication and transaction security mechanisms (such as two-factor authentication, EMV chips, PCI DSS compliance and tokenisation), given that these payment companies often offer real-time frictionless payment experiences to their consumers, it leaves less time for banks and other entities operating in the payment ecosystem to identify and respond to cyberthreats. In light of the above, there is an increased need for such entities to identify and develop cybersecurity

standards commensurate with the nature of the information assets handled by them and evaluate the possible harm in the event of any cybersecurity attack, to ensure that these emerging risks are mitigated.

Moreover, the covid-19 pandemic has led to increased dependencies on digital infrastructure for many organisations, as employees are being given the option of working remotely. This has led to enormous cybersecurity-related vulnerabilities and challenges for large and small organisations alike and made them rethink cybersecurity preparedness, policies and budgets.

We have already witnessed large-scale cyberattacks (such as ransomware attacks) and disruption in sensitive sectors in India. For instance, in November 2022 a well-known public hospital in India was subject to a ransomware attack that crippled the services of the hospital, as access to the hospital management tool, which manages appointments, stores medical records, etc, being disrupted. Other, similar incidents have also been reported in the medical sector. The demand for remote work, new technologies and vulnerabilities resulting therefrom will continue to exist, and accordingly we expect cybersecurity standards to be given critical importance.

Law stated - 9 December 2023

International standards

Has your jurisdiction adopted any international standards related to cybersecurity?

Yes, the SPDI Rules require body corporates that handle sensitive personal data or information to implement 'reasonable security practices and procedures' by maintaining a comprehensively documented information security programme. This programme should include managerial, technical, operational and physical security control measures that are commensurate with the nature of the information being protected. In this context, the SPDI Rules recognise the International Standard ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements, as one such approved security standard that can be implemented by a body corporate for protection of personal information. All body corporates that comply with this standard are subject to audit checks by an independent government-approved auditor at least once a year or as and when they undertake a significant upgrade of their processes and computer resources.

The newly enacted, albeit yet to be notified, DPDP Act also puts an obligation on data fiduciaries to adopt reasonable security safeguards to prevent personal data breach. Unlike the SPDI Rules, the DPDP Act does not recognise any specific standards to be followed. Having said that, more clarity on specific security standards and safeguards to be implemented under the DPDP Act may emerge once the rules are framed and notified thereunder.

Sector-specific regulators have also prescribed security standards specifically applicable to regulated entities. For instance, the RBI guidelines mandate banks to follow the ISO/IEC 27001 and ISO/IEC 27002 standards for ensuring adequate protection of critical functions and processes. The Guidelines on Regulation of Payment Aggregators and Payment Gateways issued by the RBI require payment aggregators to implement data security standards and best practices such as PCI-DSS and PA-DSS and implement checks to ensure

that the merchants onboarded by them are compliant with such data security standards and best practices. Similarly, SEBI requires stock exchanges, depositories, clearing corporations, etc, to follow best practices of standards such as ISO/IEC 27001, ISO/IEC 27002 and COBIT 5, or their subsequent revisions, if any, from time to time.

Law stated - 9 December 2023

Personnel and director obligations

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

While there is no specific statutory provision that requires information security personnel to keep directors informed of an organisation's network preparedness, in the event of a cybersecurity breach, the persons in charge of an organisation will be required to demonstrate before regulators that they have implemented security control measures as per their documented information security programmes and information security policies. Therefore, it would be necessary for these persons to be aware of and updated about the information security preparedness of their organisation to effectively discharge their responsibilities.

Section 85 of the IT Act also specifically states that in case of any contravention of the provisions stipulated thereunder, any person who, at the time of contravention, was in charge of supervising the affairs of a company will be liable and proceeded against, unless he or she is able to prove that the contravention took place without his or her knowledge, or that he or she exercised all due diligence to prevent the contravention. Therefore, personnel can protect themselves from liability by being aware of and deploying adequate cybersecurity measures.

Separately, as per the CAM Rules, the managing director, company secretary, or any other director or officer of the company (as may be decided by the board) is responsible for the maintenance and security of electronic records. This person is required, inter alia, to provide adequate protection against unauthorised access, alteration or tampering of records; ensure that computer systems, software and hardware are secured and validated to ensure their accuracy, reliability, and accessibility; and take all necessary steps to ensure the security, integrity, and confidentiality of records. Any failure by such personnel in this regard may be construed to be a breach of their duties towards the organisation and is punishable with a fine. The CAM Rules also require an electronic voting system for companies with equity shares listed on a recognised stock exchange, and every company having not less than one thousand members to have adequate cyber security in place.

It is also important to note that the CERT-In Directions now require service providers, intermediaries, data centres, body corporate and government organisations to designate a Point of Contact to interface with CERT-In. All communications from CERT-In seeking information and providing directions for compliance are to be sent to the said Point of Contact. The information relating to a Point of Contact is required to be sent to CERT-In as well as kept updated from time to time. Accordingly, to demonstrate bonafide compliance

with the CERT-In Directions, the management and persons in charge are to ensure such a Point of Contact is appointed and such details are communicated to CERT-In.

Law stated - 9 December 2023

Key definitions

How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

Under the IT Act, 'cybersecurity' means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction. 'Cybercrime', on the other hand, has not been expressly defined under any central statute or regulations; however, the National Cyber Crime Reporting Portal (a body set up by the government to facilitate reporting of cybercrime complaints) has defined 'cybercrime' to mean 'any unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime'. Further, the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 define 'cyber security incident' as any real or suspected adverse event in relation to cyber security 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 in data, information without authorisation.

Under the CAM Rules, 'cyber security' is defined as protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosures, disruption, modification or destruction.

In November 2023, the RBI issued the Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices (Master Directions), applicable to regulated entities such as banks and non-banking financial companies (NBFCs), which define 'cyber security' as preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. As per the definition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved in cyber security. Further, the Master Directions define a 'cyber incident' as a cyber event that adversely affects the cyber security of an information asset, whether resulting from malicious activity or not. Also, the Master Directions define 'cyber-attack' as a malicious attempt (or more than one attempt) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorised access to assets. The Master Directions will come into effect from 1 April 2024.

The courts in India have also dealt with various instances of cybercrime over the years. The Gujarat High Court, in the case of *Jaydeep Vrujlal Depani v State of Gujarat* (R/SCR.A/5708/2018 Order), recognised a publicly available definition of 'cybercrime' to mean 'the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)'.

While the IT Act does not make any distinction between cybersecurity and data privacy, in our view, these issues are distinct but also deeply interconnected, as ensuring the privacy of any data (whether of an individual or a corporate) requires adequate cybersecurity processes to be implemented by organisations. Further, cybersecurity and information security frameworks are developed by organisations at a broader level to build resilience against various forms of cyberthreat, including cybercrimes that entail more extensive engagement with regulatory authorities depending on the extent of the harm caused, the nature of the information handled by the body corporate, sector sensitivities, etc.

Law stated - 9 December 2023

Mandatory minimum protective measures

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

As per the SPDI Rules, any body corporate that possesses, deals with or handles any sensitive personal data or information in a computer resource is required to implement prescribed security standards (ISO/IEC 27001 on Information technology – Security techniques – Information security management systems – Requirements). The newly enacted, albeit yet to be notified, DPDP Act also puts an obligation on data fiduciaries to adopt reasonable security safeguards to prevent personal data breach. While no specific standards are prescribed under the DPDP Act, more clarity may emerge once the rules are framed and notified thereunder.

Sector-specific cybersecurity measures have been made mandatory by regulators for some regulated businesses. For instance, in the banking sector, the RBI requires banks to undertake certain security measures, including, inter alia, logical access controls to data, systems, application software, utilities, telecommunication lines, libraries and system software; using the proxy server type of firewall; using secured socket layer (SSL) for server authentication; and encrypting sensitive data, such as passwords, in transit within the enterprise itself. The RBI specifically mandates that connectivity between the gateway of the bank and the computer system of the member bank should be achieved using a leased line network (and not through the internet) with an appropriate data encryption standard and that 128-bit SSL encryption must be used as a minimum level of security. The RBI also requires payment aggregators to implement data security standards and best practices like PCI-DSS, PA-DSS, latest encryption standards, transport channel security, etc. as per the Guidelines on Regulation of Payment Aggregators and Payment Gateways.

Additionally, in the telecommunications sector, the licence conditions imposed by the DOT require every licensee to implement the following measures:

- ensure protection of privacy of communication so that unauthorised interception of messages does not take place;
- have an organisational policy on security and security management of its network, including network forensics, network hardening, network penetration tests and risk assessment; and
-

induct only those network elements into its telecom network that have been tested as per relevant contemporary Indian or international security standards (eg, the IT and ITES elements against the ISO/IEC 15408 standards, the ISO 27000 series standards for information security management systems and the 3GPP and 3GPP2 security standards for telecom and telecom-related elements).

Further, critical information infrastructure (CII) is separately regulated by the National Critical Information Infrastructure Protection Centre (NCIIPC) and the 'Guidelines for the Protection of National Critical Information Infrastructure' (CII Guidelines). CII has been defined under the IT Act to mean any computer resource, the incapacitation or destruction of which can have a debilitating impact on national security, the economy, public health or safety. Under the CII Guidelines, certain best practices and controls are provided as minimum recommendations to be implemented by the CIIs at different stages of CII functioning, to maintain safe and secure operations. In addition to the CII Guidelines, the NCIIPC in April 2020 also issued covid-19 guidelines titled 'Building Resilience against Cyber Attacks during COVID-19 Crisis', which intend to provide guidance to CIIs on various issues, including managing email phishing risks, protection of organisational assets and enabling employees to work remotely. Further, the National Security Council Secretariat has released, 'Cyber Security Audit – Baseline Requirements' (CSA-BR) for Cyber information infrastructure prescribing minimum, common, and harmonised baseline criterion for cyber security audits, which is to be mandatorily followed by all CII.

Law stated - 9 December 2023

Cyberthreats to intellectual property

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

The IT Act and related laws are equally applicable to cyberthreats involving intellectual property and grant similar protection.

Law stated - 9 December 2023

Cyberthreats to critical infrastructure

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

As per section 70 of the IT Act, the government may notify any computer resource that directly or indirectly affects the facility of CII to be a ‘protected system’. CII means any computer resource of which the incapacitation or destruction can have a debilitating impact on national security, economy, public health or safety. Under the Information Technology (Information Security Practices and Procedures for Protected System) Rules 2018, specific cybersecurity practices are applicable in the context of a protected system, such as setting up an information security steering committee (Committee) to approve all information security policies relating to the protected systems, designating a chief information security officer (CISO) and carrying out vulnerability, threat or risk analysis on an annual basis and

on a significant change or upgrade in the system, under intimation to the Committee. Significant changes in network configuration would need to be approved by the Committee, and organisations would need to ensure timely communication of cyber incidents to the Committee.

Under the provisions of the IT Act, a nodal body – the NCIIPC – has been set up to work in the interest of CII protection. The NCIIPC is authorised to reduce vulnerabilities of CII against cyberterrorism, cyber warfare and other threats. Certain identified CIIs are in sectors such as transport, telecoms, banking, insurance, finance, power, energy and governance.

The recently notified Central Electricity Regulatory Commission (Indian Electricity Grid Code) Regulations 2023 prescribe measures to be taken by, among others, captive generating plants and energy storage systems to safeguard the national grid from spyware, malware, cyber attacks and network hacking, and also include requirements for a procedure for a security audit from time to time and a cybersecurity framework, among others.

Sector-specific cybersecurity regulations are also available for sectors such as banking, telecommunications, finance and insurance.

Law stated - 9 December 2023

Restrictions on cyberthreat information sharing

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

India does not have a dedicated cybersecurity law or regulation that restricts sharing of cyberthreat information. However, personal information and the right of privacy of an individual are protected under Indian law. In the judgment of *Justice KS Puttaswamy (Retd) and Anr v Union of India and Ors* (Writ Petition (Civil) No. 494 of 2012), the Supreme Court of India held the right to privacy to be a fundamental right that is an intrinsic component of the right to life and personal liberty under article 21 of the Constitution of India and therefore a basic right of all individuals. Although there are precedents where the courts have held private communications between individuals to be covered within the purview of 'right to privacy', there are also precedents where Indian courts have admitted recordings obtained without consent as valid evidence. Given that this issue is unsettled, the permissibility of recordings will need to be determined on a case-by-case basis.

In any case, the SPDI Rules require a body corporate to disclose personal data or sensitive personal information subject to prior consent of the data subject. However, this condition can be waived if the disclosure is to government agencies mandated under the IT Act for the purpose of verification of identity, or for the prevention or investigation of any offences, including cybercrimes. The SPDI Rules also permit disclosure without consent in cases where the disclosure is made pursuant to an enforceable order under applicable law.

The SPDI Rules also allow a body corporate to transfer data to any other body corporate or a person in India or in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, the transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject or where the person has consented to the data transfer.

Under the DPDP Act, any processing (including disclosure) of personal data will require consent accompanied or preceded by a notice by the data fiduciary to the data principal (except in certain cases identified under the DPDP Act as legitimate use). However, disclosure of information may be done to the state or any of its instrumentalities, for fulfilling any obligation under any law for the time being in force in India. Further, disclosure may also be done for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution. Such disclosure will be subject to processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force.

Certain laws, such as the Indian Telegraph Act 1885 (the Telegraph Act) and the IT Act, permit governmental and regulatory authorities to access private communications and personally identifiable data in specific circumstances. The Telegraph Act empowers the government to intercept messages in the interest of public safety, national security or the prevention of crime, subject to certain prescribed safeguards. In that scenario, the telecom licensee that has been granted a licence by the DOT is mandated to provide necessary facilities to the designated authorities of the central government or the relevant state government for interception of the messages passing through its network.

The IT Act also grants similar authority to the government and its authorised agencies. Any person or officer authorised by the government (central or state) can, inter alia, direct any of its agencies to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted, any information that is generated, transmitted, received or stored in any computer resource, in the event that it is satisfied that it is necessary or expedient to do so in the interest of sovereignty and the integrity of India, the defence of India, the security of the state, friendly relations with foreign states, public order or preventing incitement to the commission of any cognisable offence relating to the above, or for the investigation of any offence. In our view, the instances described in the IT Act can be relied on by the government agencies to intercept data for cybersecurity incidents if they relate to contravention or investigation of any crime.

Law stated - 9 December 2023

Criminal activities

What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

Cybercrime activities are specifically dealt with under the IT Act. It prescribes penalties ranging from fines to imprisonment for various types of cyber activities, including hacking; tampering with computer source code; denial-of-service attacks; phishing; malware attacks; identity fraud; electronic theft; cyberterrorism; privacy violations; and the introduction of any computer contaminant or virus. Further, the CERT-In directions also set out specific cyber security incidents, including targeted scanning/probing of critical networks/systems; attacks on internet of things (IoT) devices and associated systems, networks, software and servers; attacks on servers, such as database, mail and DNS, and network devices, such as routers.

Law stated - 9 December 2023

Cloud computing

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

CERT-In Directions are applicable to cloud service providers as well. The CERT-In Directions have imposed certain obligations on cloud service providers, vis-a-vis data retention, and reporting. For instance, as per the Directions, any attack or malicious/suspicious activities affecting systems/servers/software/applications related to cloud computing have to be mandatorily reported to CERT-In, within six hours of noticing such incident or being brought to notice about such incident. Further, cloud service providers are required to register and retain certain mandatory data for their subscribers.

Further, given that cloud computing services are rendered and received over the internet or through the digital medium, certain other provisions of the IT Act, the SPDI Rules and the Intermediaries Guidelines may be relevant to these services.

For instance, the SPDI Rules allow a body corporate to transfer data to any other body corporate or a person in India or in any other country that ensures the same level of data protection that is adhered to by the body corporate. However, the transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and the data subject or where the person has consented to the data transfer. Accordingly, in our view, any entity engaged in the cloud computing business will need to ensure that it maintains the same level of information security standards as that of the data controller (ie, the person collecting the information from the data subject).

Also, depending on the business model, a cloud services provider may fall within the definition of an intermediary under the IT Act (defined as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cybercafes). As an intermediary, the cloud service provider will need to observe due diligence measures to claim safe harbour protection from liability arising from the content stored by it. These due diligence measures include taking all reasonable steps to secure its computer resource and the information contained therein by adopting the security practices prescribed under the SPDI Rules.

The RBI also issued 'Guidelines on Regulation of Payment Aggregators and Payment Gateways' on 17 March 2020, and 'Regulation of Payment Aggregator – Cross Border (PA – Cross Border)' on 31 October 2023, where it is mandated for all payment aggregators, and payment aggregators – cross border, to adhere to the data-storage requirements applicable for payments data to ensure that all data is stored only in India for the RBI's unfettered supervisory access.

Law stated - 9 December 2023

Foreign organisations

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

As per section 75 of the IT Act also applies to any offence committed outside India if the act that constitutes the offence involves a computer, computer network or computer system in India. Hence, the applicability of this law is agnostic to the presence of foreign organisations in India so long as users in India can access the services provided by the organisations and the operation of the services amounts to the contravention of any provision described thereunder.

Further, in the context of applicability of the CERT-In Directions to overseas entities, the clarifications issued by CERT-In by way of FAQs, suggest that the CERT-In Directions will apply to all entities in the matter of cyber incidents and cyber security incidents as along as the service is catering to users in India. This seems to indicate that CERT-In is of the view that CERT-In Directions would continue to apply as long as catering to Indian users, irrespective of fulfilment of the requirements of section 75 of the IT Act. We will have to await clarity on the interplay between section 75 of the IT Act and the position indicated by the FAQs issued on the applicability of CERT-In Directions.

Law stated - 9 December 2023

BEST PRACTICE

Recommended additional protections

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

In addition to minimum statutory cybersecurity standards, various regulatory bodies have advised businesses to adopt more robust measures in areas of cybersecurity. For example, the Ministry of Communication and Information Technology released the National Cyber Security Policy in 2013, which recommended creating a secure cyber ecosystem, strengthening laws and creating mechanisms for the early warning of security threats, vulnerability management and the response to security threats. The policy intended to encourage all organisations to develop information security policies integrated with their business plans and implement the policies in accordance with international best practices.

Under the Digital India initiative, the Ministry of Electronics and Information Technology (MeitY) has set up the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), operated by the Computer Emergency Response Team (CERT-In), to work with internet service providers and product or antivirus companies to provide information and tools to users on botnet and malware threats. Similar proactive measures are deployed by sector-specific regulators from time to time.

Law stated - 9 December 2023

Government incentives

How does the government incentivise organisations to improve their cybersecurity?

In recent years, the government has rolled out some beneficial measures to incentivise both public and private sector organisations to improve cybersecurity standards. One example is the Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products notified by MeitY on 2 July 2018, which was further revised by the Public Procurement (Preference to Make in India) Order 2019 for Cyber Security Products notified by MeitY on 6 December 2019, wherein cybersecurity was named as a strategic sector, and government procurement agencies will give preference to domestically manufactured or produced cybersecurity products.

Law stated - 9 December 2023

Industry standards and codes of practice

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

In addition to the Information Technology Act 2000 and the applicable rules framed thereunder (including the CERT-In Directions which prescribe specific obligations for maintenance of logs, ICT clock synchronisation, and data retention requirements), industry-specific standards have been prescribed by specific regulators. Some examples are given below.

- Financial sector: the Reserve Bank of India has issued various guidelines for ensuring cybersecurity and the handling of cyber fraud within the banking sector. They can be accessed at www.rbi.org.in and include the following:
- Cyber Security Framework in Banks, prescribing standards to be followed by banks for securing themselves against cybercrimes;
- Basic Cyber Security Framework for Primary (Urban) Cooperative Banks, prescribing certain basic cybersecurity controls for primary urban cooperative banks; and
- Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices 2023 that incorporates, consolidates, and updates the guidelines, instructions and circulars on IT governance, risk, controls, assurance practices and business continuity/disaster recovery management. The Master Directions will come into effect from 1 April 2024.
- Insurance sector: the insurance sector is subject to the 'IRDAI Information and Cyber Security Guidelines 2023', issued by the Insurance Regulatory and Development Authority of India (IRDAI). These Guidelines are applicable to all insurers, including insurance intermediaries, brokers, corporate agents etc, regulated by IRDAI. The Guidelines apply to all data created, received or maintained by such entities in the course of carrying out their designated duties and functions, irrespective of the place of storage and form of such data. The Guidelines stipulate the organisational structure to be created for the governance, implementation and monitoring of information security.
-

Telecommunications sector: the licence conditions for a unified licence granted by the Department of Telecommunication (DOT) prescribe various cybersecurity obligations on the licensee entity. For instance, the licensee is obligated to ensure the protection of privacy of communication and that unauthorised interception of messages does not take place; the licensee is to be completely responsible for security of their networks and must have an organisational policy on the security and security management of their networks, etc. Due to the large surge in cybersecurity incidents fuelled by large-scale remote work adoption during the covid-19 pandemic, the DOT has been issuing, inter alia, various security-related circulars to update stakeholders, such as Best Practices – Cyber Security, which provides protocols to be followed by organisations; and Unsafe Practices to be Avoided at Workplace for Cyber Security, which describes unsafe workplace practices that may be avoided, such as using common passwords, leaving devices unlocked, ignoring operating systems and software updates and downloading files without scanning.

Law stated - 9 December 2023

Responding to breaches

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

Depending on the nature and the extent of the cybersecurity incident and the sensitivity of the sector, cyber incident response strategies may differ from one business to another. Some common measures that are recommended include:

- deploying a detailed information security policy to be approved by the board;
- conducting regular transaction monitoring;
- conducting information security risk assessments;
- setting up risk mitigation and transition plans;
- updating relevant stakeholders within the organisation on their role in advance; and allocating appropriate personnel to engage with regulatory authorities and to deal with clients, service providers, etc. For instance, the CERT-In Directions provide that service providers, intermediaries, data centres, body corporates, and government organisations must appoint a Point of Contact to engage with CERT-In for certain compliance related obligations of the entities.

Many companies also prefer to conduct regular assessments of the vulnerabilities in their systems, including by inviting focused hacking. Depending on the sector, organisations can also reach out to CERT-In and seek advice on incident recovery, containing the damage and restoring their systems to operation. From time to time, CERT-In also issues advisories on actions recommended for parties that have been affected by cybersecurity incidents.

Law stated - 9 December 2023

Voluntary information sharing

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

While there are mandatory reporting requirements under the CERT-In Directions, it is also possible for individuals and organisations to voluntarily report any other cybersecurity incidents and vulnerabilities to CERT-In and seek requisite support and technical assistance to recover from them. Whether timely and voluntary reporting will help mitigate the imposition of a penalty for failing to implement reasonable security practices will be a fact-specific assessment, given there is no formal guidance in this regard.

Moreover, Ministry of Home Affairs Ministry has operationalised a toll-free National Helpline number '1930' (previously '155260') and an online reporting platform, namely, the 'National Cyber Crime Reporting Portal' to enable persons to make immediate complaints of financial loss caused to such persons due to cyber financial frauds including debit or credit card fraud, e-wallet and internet banking related fraud, etc. Further, the platform can be used to report other types of cybercrimes.

In addition, the Securities Exchange Board of India (SEBI), in its 'Cyber Security & Cyber Resilience Framework' for Stock Brokers/Depository Participants, has mandated stockbrokers and depository participants to submit quarterly reports to stock exchanges and depositories with information on cyberattacks and threats experienced by such entities and the corresponding measures that were taken to mitigate the vulnerabilities, threats and attacks.

Law stated - 9 December 2023

Public-private cooperation

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

The government issues consultation papers to invite feedback and suggestions from the private sector, which aids the formulation of policies and laws in respect of cybersecurity. For instance, presently, the government is working with the private sector to develop its 2020 cybersecurity strategy. In addition, in 2019 the National Cyber Security Coordinator and the Data Security Council of India launched an online repository on cyber tech called 'Techsagar' to facilitate exchange and collaboration on matters of innovation and cybersecurity between businesses and academia. It is intended to provide an overview of India's cybersecurity preparedness and relevant stakeholders.

In a first of its kind public-private partnership, MeitY in 2018 launched 'Cyber Surakshit Bharat' to strengthen the cybersecurity ecosystem in India, by spreading awareness about cybercrime and undertaking capacity-building for CISOs and IT staff across all government departments. The founding partners of the consortium are IT companies Microsoft, Intel, WIPRO, Redhat and Dimension Data. Additionally, knowledge partners include CERT-In, NIC, NASSCOM and the FIDO Alliance and consultancy firms Deloitte and EY.

Law stated - 9 December 2023

Insurance

Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Cybersecurity insurance has gained momentum in India. It is aimed at shielding online users against the damage and loss that may arise as a result of unauthorised disclosure of or access to personal and financial data. Cyber insurance is prevalent and common in the banking, IT and ITES, retail and manufacturing sectors.

Furthermore, last year a task force set up by government submitted recommendations for formulation of a National Cyber Security Strategy 2023, which can be expected to provide certain guidance on cyber insurance. However, the Strategy has not yet been released.

Law stated - 9 December 2023

ENFORCEMENT

Regulatory authorities

Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Computer Emergency Response Team (CERT-In) is the nodal agency recognised under the Information Technology Act 2000 (IT Act) for the coordination of cyber incident response activities and the handling of cybersecurity incidents. Further, the government has also established certain authorities and agencies for according protection specifically to the critical infrastructure of India, such as the National Critical Information Infrastructure Protection Centre, which was created to assess and prevent threats to vital installations and critical infrastructure in India. As and when a cybersecurity incident is determined, individuals and organisations can seek remedy from the adjudicating authorities appointed under the IT Act.

Sector-specific regulators have also attempted to enforce compliance with their respective information security standards. For example, the Reserve Bank of India (RBI) imposed a monetary penalty of 26.6 million rupees on the Bank of Bahrain & Kuwait BSC, India Operations for non-compliance with the directions of the Cyber Security Framework in Banks.

In January 2020, the Union Minister for Home Affairs inaugurated the Indian Cyber Crime Coordination Centre (I4C) to deal with all types of cybercrime in a comprehensive and coordinated manner. One of the components of I4C is the National Cyber Crime Reporting Portal, which is a citizen-centric initiative that enables citizens to report all kinds of cybercrime online, with a specific focus on crimes against women and children – particularly child pornography, child sexual abuse material and online content pertaining to rapes, gang rapes and similar crimes. The complaints reported on this portal are dealt with by law enforcement agencies and police, based on the information made available in the complaints.

The Digital Personal Data Protection Act 2023 (DPDP Act) mandates a data fiduciary to have reasonable security safeguards in place to prevent breach of personal data. The Data

Protection Board of India established by the central government under the DPDP Act can impose a monetary penalty of up to 2.5 billion rupees for breach in observing this obligation.

Law stated - 9 December 2023

Extent of authorities' powers

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

Given that CERT-In is the national nodal agency responsible for cybersecurity, it has the authority to call for information and give directions to service providers, intermediaries, data centres, body corporates and any other person to perform their functions under the IT Act, the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, the CERT-In Directions. Failure to respond to CERT-In's information requests may lead to the imposition of monetary penalties as well as imprisonment for a term that may extend to one year or both.

Further, the adjudicating authorities appointed under the IT Act have the powers of a civil court to call for evidence and documents, and summon witnesses in connection with an inquiry into any contravention under the IT Act.

As per the provisions of the IT Act, for national security and for investigation of any offence (including cybersecurity offences), authorised government officers can issue orders to intercept, monitor or decrypt any computer resource, ask intermediaries to provide access to any information or to block access to any information stored, received or generated in any computer resource. Additionally, law enforcement agencies can be authorised to monitor and collect traffic data or information generated, received or transmitted in any computer resource, and can confiscate any computer resource in respect of which any contravention of the IT Act has been carried out.

Indian law also provides law enforcement authorities with various other mechanisms to pursue, investigate and prosecute cyber criminals. For instance, the Indian Penal Code 1860 (IPC) is a comprehensive code intended to cover most substantive aspects of criminal law. Criminal activities punishable under the IPC do extend to the online cyberspace infrastructure and will be dealt with in the same manner.

Under the DPDP Act, the Data Protection Board of India established by the central government can inquire into breach of personal data under certain circumstances and impose penalty.

Law stated - 9 December 2023

Most common enforcement issues

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

Regulators in India have relied on the provisions of the IT Act and the IPC to prosecute entities found to be non-compliant with mandatory information security requirements. However, from a practical perspective, enforcement agencies often face challenges in prosecuting

offshore entities that do not have a business presence in India, as well as affixing liability in multi-layered business outsourcing structures. The absence of a comprehensive data protection law that allocates cybersecurity responsibilities between all relevant stakeholders is also a concern. Over time, the private sector and the government have felt the need to develop more cybercrime and prosecution expertise among the police personnel responsible for prosecuting offences under the IT Act, and specific local cyber cells have been set up to address this gap.

Law stated - 9 December 2023

Regulatory and data subject notification

What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified? When is notice required?

There is no specific requirement under the IT Act to inform the data subject of a cybersecurity incident. However, as per the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 (Rules) and the CERT-In Directions specific types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, data breach, data leak, unauthorised access to social media accounts, attacks or incident affecting digital payment systems, attacks or malicious/suspicious activities affecting systems/servers/software/applications related to cloud computing, blockchain, virtual assets, virtual asset exchanges, etc) have to be mandatorily reported to CERT-In by service providers, intermediaries, data centres body corporates and government organisations within six hours of noticing the incident or being brought to notice about the incident. As per the FAQs issued for the CERT-In Directions, while the incidents specified in the aforementioned directions need to be mandatorily reported, it has been clarified that cybersecurity incidents not specified in the aforementioned directions or Rules also need to be reported considering the nature, severity and impact of the incident. If multiple parties are affected by a cybersecurity incident any entity that notices the cybersecurity incident must report it to CERT-In.

In addition, sector-specific regulators have their own reporting requirements. For instance, the RBI requires banks to comply with the Cyber Security Framework in Banks, which, among others, requires banks to report cybersecurity incidents to the RBI within two to six hours. The Guidelines on Regulation of Payment Aggregators and Payment Gateways issued by the RBI require payment aggregators to put in place a mechanism for the monitoring, handling and follow-up of cybersecurity incidents and breaches. These incidents and breaches must be reported immediately to the Department of Payment and Settlement Systems, RBI, Central Office, Mumbai, and reported to CERT-In.

As per the DPDP Act, a data fiduciary is required to notify the Data Protection Board of India (established by the central government) and the data principal affected by such breach. The form and manner of such notification will be prescribed in the rules to be formulated under the DPDP Act.

Law stated - 9 December 2023

Penalties for non-compliance with cybersecurity regulations

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

The IT Act provides for penalties for varied instances of cybersecurity breaches, some of which are described here. Section 43 of the IT Act provides that any person accessing a computer or a computer system or network without permission of the owner, downloading copies and extracting any data or causing disruption of any system will be liable to pay damages to the person affected. Section 66 of the IT Act also provides for punishment of imprisonment for a term up to three years or with a fine of up to 500,000 rupees if the person dishonestly or fraudulently commits the offence.

Section 66C of the IT Act provides that a person who, fraudulently or dishonestly, makes use of the electronic signature, password or any other unique identification feature of any other person will be punished with imprisonment of up to three years and will also be liable for payment of a fine of up to 100,000 rupees.

Additionally, the IT Act under Section 70B provides for imprisonment of up to one year or a fine of up to 100,000 rupees, or both, for any failure by an entity (service provider, intermediary, data centre, body corporate, etc) to provide requisite information requested by CERT-In. Furthermore, sector-specific authorities (such as the RBI) may also levy penalties for non-compliance with their respective cybersecurity standards.

Further, under the DPDP Act failure to have reasonable security safeguards in place to prevent breach of personal data can result in imposition on the data fiduciary of a financial penalty of up to 2.5 billion rupees.

Law stated - 9 December 2023

Penalties for failure to report threats and breaches

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

Any failure by intermediaries, service providers, data centres, body corporates and government organization, to mandatorily report a cybersecurity within the stipulated timelines, or furnish any information to CERT-In, as per the process provided under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 and the CERT-In Directions, is punishable by imprisonment of up to one year or a fine that may extend to 100,000 rupees, or both.

In addition, sector-specific regulators have their own reporting requirements. For instance, failure to report within the timelines prescribed for banks under the Cyber Security Framework in Banks may result in the imposition of penalties by the RBI. For the telecommunications sector, the unified licence conditions stipulate that any failure by the licensee to comply with the obligations provided therein, including reporting of any intrusions, attacks and frauds on the technical facilities, may render the concerned licensee liable to a monetary penalty of up to 500 million rupees per breach.

Under the DPDP Act, a failure to notify the Data Protection Board of India or affected data principal of a personal data breach can result in a penalty of up to 2 billion rupees.

Law stated - 9 December 2023

Private enforcement

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

The IT Act makes statutory remedies available to persons affected by a cyber security incident. Section 43A of the IT Act expressly provides that whenever a body corporate possesses or deals with any sensitive personal data or information, and is negligent in maintaining reasonable security practices and procedures that in turn cause wrongful loss or wrongful gain to any person, the body corporate will be liable to pay damages to the person affected. Therefore, the affected party may initiate a civil action against the negligent body corporate, making it liable to pay damages.

Further, a civil action may also be brought against any person who, without permission of the owner of a computer or a computer system or network, does any of the acts mentioned under section 43 of the IT Act, including but not limited to accessing or securing access to the computer or computer system or network, downloading or extracting any data from it, contaminating it with a virus or other malware, or causing any damage to it.

In addition, the Securities Exchange Board of India's Guidelines ('Cyber Security & Cyber Resilience Framework' for Stock Brokers/Depository Participants) have mandated stockbrokers and depository participants to draft their cybersecurity and cyber resilience policy document and ensure provisioning of alternate services or systems to customers in the event of any security incident.

The Ministry of Home Affairs has operationalised a toll-free National Helpline number '1930' (previously '155260') and an online reporting platform, namely, the 'National Cyber Crime Reporting Portal' to enable persons to immediately report financial loss caused to persons due to cyber financial frauds including debit or credit card fraud, e-wallet and internet banking related fraud, etc. This reporting platform can also be used by persons to report other kinds of cybercrimes, which include unauthorised access of data or data breach, ransomware, online and social media-related crimes, cryptocurrency related frauds, etc.

Under the newly enacted DPDP Act, a data principal has a right to readily available means of grievance redressal to be provided by the data fiduciary and/or consent manager. The right available to a data principal is for an act or omission by the data fiduciary and consent manager regarding the performance of their obligation under the DPDP Act or exercise of the data principal's rights under the DPDP Act. For instance, such acts or omissions can include failure to have reasonable security safeguards in place to prevent breach of personal data and failure to intimate the affected data principal of a personal data breach.

Law stated - 9 December 2023

THREAT DETECTION AND REPORTING

Internal policies and procedures

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

CERT-In Directions prescribe certain compliance requirements for service providers, intermediaries, data centres, body corporate, virtual private server providers, cloud service providers, VPN service providers, virtual asset service providers, virtual asset exchange providers, custodian wallet providers and government organisations (individually and collectively, 'Entities'). These compliance requirements include the following.

- Reporting of a cybersecurity incident: specified cybersecurity incidents are to be reported to CERT-In within six hours of noticing such incidents or of being notified of such incidents.
- Appointment of a POC: a point of contact (POC) is to be appointed to engage with CERT-In in relation to the CERT-In Directions. Details of the POC need to be provided to CERT-In and should be kept updated.
- Maintenance of logs in India: logs of information and communications technology (ICT) systems are to be maintained for a rolling period of 180 days.
- ICT clock synchronisation: entities must connect to a network time protocol (NTP) server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of the ICT systems clocks of such entities.
- Data retention: data centres, cloud service providers, virtual private server providers and virtual private network service providers are required to maintain certain data (such as name of subscriber, email address and IP address, address and contact number, ownership pattern, etc) for five years or a longer duration as mandated by law after any cancellation or withdrawal of registration.
- Virtual asset service providers: virtual asset exchange providers and custodian wallet providers must maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for five years.

The aforementioned compliance requirements, and more particularly the compliance requirement related to maintenance of logs and data retention, have been challenged in Delhi High Court via a writ petition. The petition is pending before the High Court, and based on public records will come up for hearing in March 2024.

In addition to the requirements mentioned above, CERT-In issued 'Guidelines on Information Security Practices for Government Entities' on 30 June 2023 for all the ministries, departments, secretariats and offices specified in the First Schedule to the Government of India (Allocation of Business) Rules 1961, their attached and subordinate offices, and all government institutions, public sector enterprises and other government agencies under their administrative purview. The Guidelines include guidelines prepared by the National Informatics Centre for Chief Information Security Officers (CISOs) and employees of central government ministries/departments for the purpose of enhancing cyber security and cyber hygiene.

In addition to the above, some specific requirements are mentioned below.

-

Information Technology Act 2000 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules): as per the SPDI Rules, all organisations handling sensitive personal information of natural persons (financial and health information, passwords, biometric data, etc) should, inter alia:

- have information security systems in place that are commensurate to the information assets sought to be protected;
- appoint a grievance officer to address any discrepancies and grievances of the provider of such information;
- have a privacy policy for providing information on how such information is used and disclosed, etc; and
- in addition, organisations are required to audit the reasonable security practices and procedures that have been implemented at least once a year, or as and when the body corporate or a person on their behalf undertakes significant upgrading of their process and computer resources;
- Companies (Management and Administration) Rules 2014: companies, when dealing with electronic records, are required to ensure the security of any such records, including:
  - protection against unauthorised access;
  - protection against alteration;
  - protection against tampering;
  - maintaining the security of computer systems, software and hardware;
  - protecting signatures; and
  - taking periodic backups; etc;
- The Reserve Bank of India (RBI) has issued a notification on 'Cyber Security Framework for Banks', which prescribes standards to be followed by banks for securing themselves against cybercrimes, including, for example, a mechanism for dealing with and reporting incidents, a cyber crisis management plan, and arrangements for continuous surveillance of systems and protection of customer information. A similar framework is applicable to non-banking finance companies. The Guidelines on Regulation of Payment Aggregators and Payment Gateways require payment aggregators to put in place a Board-approved information security policy for the safety and security of payment systems operated by them and to implement security measures in accordance with this policy to mitigate identified risks.
- The Insurance Regulatory and Development Authority of India (IRDAI) has issued 'IRDAI Information and Cyber Security Guidelines 2023', which, among others, mandate insurers to appoint a chief information security officer, formulate a cyber crisis management plan and conduct audits.

Law stated - 9 December 2023

Record-keeping requirements

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

CERT-In Directions prescribe that entities, such as service providers, intermediaries, data centres, body corporate and government organisations (Entity) are required to maintain logs of Information and Communication Technology (ICT) systems for a rolling period of 180 days. The logs to be maintained will depend on the sector in which an Entity is operating and may include firewall logs, event logs of critical systems, application logs, VPN logs, etc. Relevant logs need to be provided to CERT-In when cyber incidents are reported or when so ordered by CERT-In. The FAQs suggest that these logs can be stored outside India as long as a copy is retained within India. The FAQs also provide that logs for successful as well as unsuccessful events must be recorded.

The aforementioned directions and more particularly the requirement to maintain logs have been challenged in Delhi High Court via a writ petition. The petition is pending before the High Court, and based on public records will come up for hearing in March 2024.

Sector-specific regulators have prescribed storage requirements for regulated entities. For instance, IRDAI issued the 'IRDAI Information and Cyber Security Guidelines 2023', which require information and communications technology (ICT) to be maintained for a rolling period of 180 days and within the Indian jurisdiction.

Lastly, in accordance with the Securities Exchange Board of India Guidelines ('Cyber Security & Cyber Resilience Framework' for Stock Brokers/Depository Participants), stockbrokers and depository participants are required to ensure that records of user access to critical systems are identified and logged for audit and review purposes, and the logs should be maintained and stored in a secure location for a period not less than two years.

Law stated - 9 December 2023

Regulatory reporting requirements

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

Reporting under the IT Act

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 permit cybersecurity incidents to be reported by any individual organization or corporate entity to CERT-In. In addition, as per the CERT-In Directions specified types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, data breach, data leak, unauthorised access to social media accounts, attacks or incident affecting digital payment systems, attacks or malicious/suspicious activities affecting systems/servers/software/applications related to cloud computing, blockchain, virtual assets, virtual asset exchanges, etc) must be reported to CERT-In by service providers, intermediaries, data centres, bodies corporate and government

organisations within six hours of noticing the incident or being brought to notice about the incident. The 'Guidelines on Information Security Practices for Government Entities' issued by CERT-In also require such entities to report a cyber incident to CERT-IN within six hours of noticing the incident or being brought to notice about the incident.

The Intermediaries Guidelines require the intermediaries, as part of their due diligence obligations, to notify CERT-In of security breaches. CERT-In publishes the formats for reporting cybersecurity incidents on its website from time to time, which requires mentioning the time of occurrence of the incident, the type of incident, information regarding the affected systems or network, the symptoms observed, the relevant technical systems deployed, and the actions taken, among others.

Reporting in other sectors

In addition to the reporting requirements under the IT Act, separate reporting requirements are applicable for cybersecurity incidents occurring in regulated sectors. For instance, the Cyber Security Framework in Banks requires banks to inform the RBI of any cybersecurity incident within two to six hours of the breach and include details of it in a standard reporting template. Such report must include all unusual cybersecurity incidents (whether they were successful or were attempts that did not succeed). Similarly, the 'IRDAI Information and Cyber Security Guidelines 2023' require all insurers, including foreign reinsurance branches (FRBs) and insurance intermediaries regulated by IRDAI, to report cyber incidents to CERT-In within six hours of noticing or being brought to notice about such incidents, with a copy to IRDAI and other concerned regulators/authorities.

As per the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, all listed entities need to submit a quarterly report of the details of cyber security incidents or breaches or loss of data or documents to the recognised stock exchange.

In the telecommunications sector, every telecommunications licensee is required to create a facility (within 12 months of grant of authorisation) for monitoring intrusions, attacks and frauds on its technical facilities, and to provide reports of these intrusions, attacks and frauds to the Department of Telecommunications.

Law stated - 9 December 2023

Time frames

What is the timeline for reporting to the authorities?

As per the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 and the CERT-In Directions, specific types of cybersecurity incidents, such as target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, data breach, data leak, unauthorised access to social media accounts, attacks or incident affecting digital payment systems, attacks or malicious/ suspicious activities affecting systems/servers/software/applications related to cloud computing, blockchain, virtual assets, virtual asset exchanges, etc) must be reported to

CERT-In by service providers, intermediaries, data centres, body corporates and government organisations within six hours of noticing the incident or being brought to notice about the incident.

Separate reporting requirements are applicable for cybersecurity incidents occurring in regulated sectors. For instance, the RBI requires banks to report cybersecurity incidents within two to six hours. Similarly, the 'IRDAI Information and Cyber Security Guidelines 2023' require all insurers, including foreign reinsurance branches (FRBs) and insurance intermediaries regulated by IRDAI, to report cyber incidents to CERT-In within six hours of noticing or being brought to notice about such incidents, along with a copy to IRDAI and other concerned regulators/authorities.

Law stated - 9 December 2023

Other reporting requirements

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

Currently, there is no obligation to report cybersecurity threats or breaches to the general public or affected parties. However, under the Digital Personal Data Protection Act 2023 (DPDP Act), in the event of a personal data breach, the data fiduciary is required to notify each affected data principal of such breach. The form and manner of such notification will be prescribed in the rules to be issued under the DPDP Act.

Law stated - 9 December 2023

UPDATE AND TRENDS

Recent developments and future changes

What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Various factors have contributed to the delayed formulation of cybersecurity regulations in India, including the rapid advancement of technology, which continues to outpace regulatory response; intermittent and ineffective reporting of incidents; the private sector's inability to accurately assess the criticality of available information and the likely harm that may be caused in the event of an incident; lack of cross-functional expertise on the nature of cybersecurity incidents that may be experienced by varied sectors; and government and private sector hesitation to mandate minimum standards for all categories of businesses, in view of the time and expense involved.

In the past year, however, there has been a renewed focus on the adoption of robust cybersecurity practices in India, from both, the government and the private sector. Due to the covid-19 pandemic and the large-scale remote work and new technology adoption resulting from it, the private sector has been quite vigilant in adapting its processing, updating its budgets and responding to cyber threats in a timely and nuanced manner.

Several organisations, such as the Data Security Council of India, have proactively issued advisories and assisted other private sector organisations to seamlessly transition to safer digital processes. We expect these initiatives to guide the government in terms of the level of cybersecurity preparedness expected from organisations, how the private sector has responded to cybersecurity threats, a renewed focus on the revision of policies and the diversified skill-set of response stakeholders, and testing the efficacy of protective technologies and strategies. Timely and descriptive cybersecurity reporting by the private sector will bring in more collaboration and clarity on better practices. The varied experiences of regulated businesses regarding cyber incidents will help guide policy, as it is likely that sensitive sectors such as healthcare and social security will require a higher standard of compliance in view of the nature of their operations and risk assessment.

We expect some regulatory developments proposed by the government to further energise compliance. The National Cyber Security Strategy 2023 is a long-awaited policy initiative of the government, and it is hoped that better security standards and priority allocation will be the norm after it is notified. In 2023, a task force set up by government submitted recommendations for formulation of a National Cyber Security Strategy 2023. However, the Strategy has not yet been released.

The proposed Digital India Act 2023 (DIA) that will replace the Information Technology Act 2000 (IT Act) can also be expected to bring a robust and dedicated law dealing with cybersecurity.

The newly enacted Digital Personal Data Protection Act 2023 (DPDP Act) and the rules to be notified thereunder will also play a critical role in shaping the regulatory environment in relation to the protection of personal data, as they seek to prescribe certain obligations of data fiduciaries (persons who determine the purpose and means of processing of personal data), which include among other things the use of reasonable security safeguards to prevent personal data breach, deletion of data after the purpose for collection is served, having a grievance redressal mechanism in place and processing of personal data only for lawful purpose for which appropriate consent has been received. Further, the data fiduciary and data processor need to notify the Data Protection Board of India (proposed to be constituted under the DPDP Act) in case of breach of this personal data. The Data Protection Board may in the event direct the data fiduciary to remedy this personal data breach or mitigate any harm caused to data principals.

Law stated - 9 December 2023