2022 CERT-In Directions on Reporting Cyber Incidents

04 May 2022

Partners: *Rahul Matthan, Nikhil Narendran, Jyotsna Jayaram,* ***Counsel:*** *Jishnu Sanyal,* ***Senior Associates:*** *Thomas J. Vallianeth, Puja Saha,* ***Associate:*** *Shantanu Mathur*

On 28 April 2022, the Indian Computer Emergency Response Team (**CERT-In**) issued new directions (**2022 Directions**) under Section 70B (6) of the Information Technology Act, 2000 (**IT Act**) incorporating a host of cyber-security, breach reporting, and record maintenance requirements. In India, the CERT-In is appointed as the national agency for performing various functions in the area of cyber security as per provisions of section 70B of the IT Act. The CERT-In is also empowered to call for information and give directions to any service provider, intermediary, data centre, body corporate and Government organisation. The 2022 Directions have been issued to augment incident response measures. This update provides a brief overview of the new requirements imposed by the 2022 Directions.

The CERT-In has issued fresh directions mandating compliances in relation to cyber security incidents, ranging from the requirement to report incidents within six hours to storing system logs locally in India. These directions are likely to bring sweeping changes to the law relating to cyber security and data breaches in India.

1 Six Hour Timeline for Reporting and Expanded List of Reportable Cyber Security Incidents

The Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013 (**CERT-In Rules**) had not prescribed a timeframe within which cyber-security incidents must be reported and only required reporting within a reasonable time frame. The 2022 Directions, on the other hand, make this requirement more stringent by requiring cyber security incidents to be reported within six hours of noticing or being brought to notice of such incident to the CERT-In. Given the short time frame, organisations would need to reassess their practices and procedures in relation to breach reporting, and ensure that appropriate organisational capabilities are deployed in order to identify and report cyber security incident in this time frame.

Further, under the CERT-In Rules only those cyber security incidents specified as mandatorily reportable were required to be reported. However, the 2022 Directions expand this list to include: (i) data breach; (ii) data leak; (iii) attacks on Internet of Things (**IoT**) devices and associated systems, networks, software, servers; (iv) attacks or incidents affecting digital payment systems; (v) attacks through malicious mobile apps; (vii) unauthorised access to social media accounts; (viii) attacks or malicious/ suspicious activities affecting cloud computing systems/servers/software/applications; (ix) attacks or malicious/suspicious activities affecting systems/servers/networks/software/applications related to big data, block chain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, drones; (x) attacks or malicious/suspicious activities affecting systems/servers/software/applications related to Artificial Intelligence

and Machine Learning. There is no clarity on the specifics of what these incidents entail, and no impact threshold has been specified presently.

2 Information Requests

Under Rule 14 of the CERT-In Rules, the CERT-In can seek information from regulated entities in specified formats and time frames for responding to cyber incidents, however this power could only be exercised by an officer of the rank of Deputy Secretary or higher. The 2022 Directions however prescribe a broad ranging power to call for information without any such safeguards.

3 Maintenance of System Logs within India

The 2022 Directions require entities to maintain logs for all their information and communications technology (ICT) systems for 180 days and to store these logs in India. These logs are also required to be provided to CERT-In while reporting a cyber incident, or when sought by CERT-In pursuant to a direction. At present there is no clarity on what these logs are required to comprise.

Further, given the generality of this requirement, it would mean that a wide range of service providers and intermediaries, such as cloud based/application layer service providers would also need to maintain localised system logs in India, even if they do not otherwise have a physical presence in India.

4 Subscriber Data Collection and Retention

Specified entities, namely Data Centres, Virtual Private Server (VPS) providers, cloud service providers (CSPs) and Virtual Private Network (VPN) providers will be required to record certain information accurately in relation to its subscribers, similar to the Know Your Customer (KYC) requirement imposed by other sectoral regulators. This information needs to be maintained for at least five years after the cancellation of the user registration, or a longer period when mandated by law.

The CERT-In is empowered to call for this information in case of any 'cyber incidents' or 'cyber security incidents'. The information required to be maintained includes: (i) validated names of subscribers/customers; (ii) subscription period including dates; (iii) IPs allotted to/being used by the members; (iv) email address, IP address and time stamps used at the time of registration; (v) purpose for subscribing to the services; (vi) validated address and contact numbers; and (vii) ownership pattern of the subscribers/customers using service.

5 Know Your Customer Information and Financial Transaction Record Retention

The 2022 Directions require all *'virtual asset service providers, virtual asset exchange providers and custodian wallet providers'* to maintain KYC and financial transaction records. This appears to create a new requirement for these entities to carry out a KYC function - which was till now only required for entities regulated by Indian financial service regulators, such as those operating in the banking, securities and insurance sectors. The retention requirement in this regard is also for a period of five years. While the directions refer to the definitions by the Ministry of Finance (MoF) for these entities to determine application, there is presently no guidance from the MoF on these definitions. Apart from being an entirely new obligation, this lack of guidance will evidently make it difficult to determine which entities will be required to comply with this obligation.

As such, the directions require the retention of identification information of the parties (including IP addresses, timestamps and time zones), transaction ID, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred.

Financial transaction records must be maintained such that individual transactions can be reconstructed from them.

6 Synchronised System Clocks

The 2022 Directions require all entities to synchronise ICT system clocks to the Network Time Protocol (**NTP**) of the National Informatics Centre (**NIC**) or National Physical Laboratory (**NPL**) or with other NTP servers traceable to those maintained by NIC or NPL. While global entities are permitted to use a different time source that is in sync with the NTP, they need to ensure that their time source shall not deviate from NPL and NIC.

This may be difficult to practically implement for entities, as the number of such servers maintained by the NIC are limited, potentially making such syncing unreliable.

7 Penalty

Non-compliance with the 2022 Directions, which would include requests from CERT-In to provide information, can invite punitive action under Section 70-B(7) of the IT Act, which can extend to imprisonment for up to a year, and/or a fine upto INR 100,000. Other penal laws, where applicable, may also be invoked in cases of non-compliance.

Conclusion

The 2022 Directions greatly widen the compliance net for entities in these sectors. The ambiguity with regard to its scope and applicability, combined with an intention to invoke penal provisions for non-compliance may make requirements such as six hour reporting, localising system logs and syncing all systems to Indian NTP fairly onerous for various entities, such as cloud service/storage providers to operate in a legally compliant manner in India.

It is noteworthy that several provisions of the 2022 Directions appear to be in excess of or in deviation from the provisions of the CERT-In Rules and the IT Act itself, as explained above, and thus the interpretation that will be taken by the courts and regulators in such cases are yet to be seen. However, both the CERT-In Rules and the 2022 Directions will need to be considered by entities while scoping for compliance. As such, while the directions envisage an effective date of 60 days from notification, it remains to be seen how the regulator and the industry will respond to the new regime.