KHAITAN &CO ADVOCATES SINCE 1911

NEWSFLASH

ERGO

Analysing developments impacting business

INDIAN COMPUTER EMERGENCY RESPONSE TEAM DIRECTION: PARADIGM SHIFT IN CYBER INCIDENT REPORTING

30 April 2022

Introduction

The Indian Computer Emergency Response Team (CERT-In) has issued a direction on 28 April 2022 (Direction) under Section 70-B(6) of the Information Technology Act 2000 (IT Act) relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe and trusted internet. This is an ongoing effort on the part of CERT-In to further strengthen cyber incident reporting, internet security and allied topics.

CERT-In had earlier issued Advisory CIAD-2021-0004 dated 20 January 2021 (Advisory), which *inter alia* required affected entities to immediately notify users/customers who could be affected with details of information breached, actions being undertaken by such affected entities to address the problem and how they can reach out to CERT-In for any queries.

Key highlights of the Direction

- ***When does the Direction come into effect?***

  The Direction is to come into effect after 60 (sixty) days following the date of its issuance.

- ***Reporting of cyber incidents***

  Certain specified types of cyber incidents (such as targeted scanning/probing of critical networks/systems, compromise of critical systems/information, unauthorised access of IT systems/data etc) as identified under Annexure I of the Direction are to be mandatorily reported to CERT-In by service providers, intermediaries, data centres, body corporates and government organisations (Covered Entities), within 6 (six) hours of noticing such incidents or being brought to notice about such incident. Notably, some of the cyber incidents (such as data breach, data leak, attacks on internet of things (IoT) devices and associated systems etc) that are to be mandatorily reported, are in addition to those set out under the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 (Rules) issued under the IT Act.

- ***Synchronisation of information and communication technology (ICT) system clocks***

  All Covered Entities are required to connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks.

  Entities having ICT infrastructure spanning across multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC.

- ***Enabling and retention of logs***

  All Covered Entities are to mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 (one hundred and eighty) days within Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered or directed by CERT-In.

- ***Retention of Information by data centres, virtual private server providers, cloud service providers and virtual private network service providers***

  Data centres, virtual private server providers, cloud service providers and virtual private network service providers are required to register the following information accurately: (i) validated names of subscribers/customers hiring the services; (ii) period of hire including dates; (iii) IPs allotted to/used by the members; (iv) email address and IP address and time stamp used at the time of registration/on-boarding; (v) purpose for hiring services; (vi) validated address and contact numbers; (vii) ownership pattern of the subscribers/customers hiring services.

  The above-mentioned information is required to be maintained for a period of 5 (five) years or longer duration, as mandated by the law, after any cancellation or withdrawal of the registration (as the case maybe).

- ***Compliances for the virtual assets industry***

  Virtual asset service providers, virtual asset exchange providers and custodian wallet providers are to mandatorily maintain records of the following, for 5 (five) years:

  - All information obtained during the process of conducting Know Your Customer (KYC) for users; and

  - Records of financial transactions, including information relating to the identification of the relevant parties involved in the transactions such as IP addresses, along with 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 transactions, and the amounts transferred.

- ***Information regarding appointment of Point of Contact***

  The format in which information about the appointment of a point of contact needs to be conveyed to the CERT-In by the Covered Entities has been provided through the Direction.

- ***Penalty for non-compliance***

  Any failure to furnish the information as required under the Direction or any non-compliance with the same may invite punitive action under Section 70-B(7) of the IT Act and other laws, as applicable. Section 70-B(7) of the IT Act provides for punishment with imprisonment for a term which may extend to 1 (one) year or with fine which may extend to INR 100,000 (Indian Rupees One Hundred Thousand) or with both.

Comment

While there have been a slew of developments in the cyber incident reporting space, this Direction is more comprehensive in its ambit and includes publication on several aspects of cyber incident reporting and cybersecurity. One of the new aspects of the Direction is inclusion of mandatory retention periods for certain records, as indicated above. The Direction enhances the legal obligations on cyber incident reporting than was originally envisaged under the IT Act and the Rules. This is a particularly interesting development and may also indicate a wider effort to overhaul the existing IT Act, given its limitations on regulating aspects such as internet and cybersecurity.

It will also have to be seen how the Direction will blend in with the data breach reporting obligations under the new data protection law, as and when it is enacted, as well as the revamp of the IT Act which is envisioned.

- *Harsh Walia (Partner), Supratim Chakraborty (Partner), Shobhit Chandra (Counsel), Sumantra Bose (Principal Associate), Tashi Gyanee (Associate), Sanjuktha A. Yermal (Associate), Shramana Dwibedi (Associate)*

For any queries please contact: editors@khaitanco.com