TRILEGAL

How to comply with CERT-In's new six-hour time frame to report cyber incidents

*By **Karthik Koragal** (Senior Associate) and **Pratibha Sharma** (Senior Executive)*

The Indian Computer Emergency Response Team (**CERT-In**) recently issued a set of new directions under the Information Technology Act, 2000 (**IT Act**), in relation to information security practices, procedure prevention, response and reporting of cyber incidents for safe and trusted internet (**CERT-IN Directions**), followed by Frequently Asked Questions (**FAQs**) dated 19 May 2022 issued by CERT-IN, to clarify the requirements under the directions.

CERT-IN Directions mandate service providers, intermediaries, data centres and body corporates (**Applicable Entities**) to mandatorily report cyber incidents (as defined under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (**CERT-IN Rules**)) within: (a) six hours of noticing such incidents; or (b) such incident being brought to such Applicable Entities. Prior to this update, CERT-In had stipulated reporting cyber security incidents (as defined under CERT-IN Rules) as early as possible, and within a reasonable time of occurrence or noticing the incident.

In addition to the Applicable Entities being mandated to report cyber incidents, within the prescribed time and in the prescribed manner, they are also required to report cyber security incidents (prescribed under CERT-IN Directions), on meeting the following threshold (as laid out in the FAQs):

(i) cyber incidents and cyber security incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant including ransomware) on any part of the public information infrastructure, including backbone network infrastructure;

(ii) data breaches or data leaks;

(iii) large-scale or most frequent incidents such as intrusion into computer resources, websites etc.; and

(iv) cyber incidents impacting the safety of human beings.

The new guidelines come in the backdrop of increasing cases of cybercrime in India – CERT-In has reported over 2.12 lakh cybersecurity cases within Jan-Feb 2022 in comparison to 14.02 lakh in total last year.

While the new guidelines are designed to tackle cybercrime effectively, they are likely to pose challenges to companies in terms of adhering to the six-hour rule. Some of these challenges are:

- **Inadequate infrastructure and resources:** Not all companies will be able to build capacities for largescale data collection, storage and management of consumer data to report cases within six hours.

- **Guidelines are aggressive compared to other global standards:** For instance, Singapore's data protection law stipulates reporting cyber breaches within three days - the same as General Data Protection Regulation's law.

- **Cybercrime is increasingly complex to detect:** It can take companies days and even months to discover a cyber security breach. Further, the new guidelines have expanded the list of

mandatorily reportable incidents from 10 to 20, including attacks on IoT devices. Currently, many companies lack an integrated technology and devices framework that can track breaches across platforms and devices, thereby amplifying the challenges in detecting and tracking incidents.

What businesses can do to report cyber breaches within CERT-In's six-hour time frame

Under the current circumstances, companies perceive the cost of compliance to increase in the near term while acknowledging that investments in cyber security could build consumer trust and loyalty in future. Below are some pointers to consider while relooking at one's cyber security readiness.

- **Reassess practices and procedures**: With CERT-IN Directions in force, practices and procedures pertaining to breach reporting require reassessment. These practices may include analysing the level of breach, deciding who is obligated to report when a cyber incident and/ or cyber security incidents affect multiple parties, and determining the road map in case of non-compliance with the regulatory guideline. If reassessed and handled appropriately, such factors may prevent delays in reporting cybercrimes.

- **Enhance organisational capabilities**: Applicable Entities need to develop or enhance appropriate mechanisms to effectively identify and report a cyber breach. These capabilities include training employees who deal with sensitive and proprietary data, conducting regular testing and security audits, and handling proprietary information and use of personal devices by employees. These cyber security imperatives are necessary not only for established businesses but also for small enterprises and start-ups, which are equally vulnerable to cyber attacks due to inadequate security infrastructure.

- **Enable logs**: CERT-In via CERT-IN Directions mandates Applicable Entities to enable logs of all their information and technology system for analysing cyber incidents. Further, such logs are required to be maintained for a rolling period of 180 days. The FAQs provide some guidance on the type of logs to be enabled, the logs stored to be finalised by the Applicable Entities depending on the sector it is in. Additionally, early identification of any cyber incident and/or cyber security incident (on meeting the threshold requirements) would depend on the kind of logs enabled by such Applicable Entities. Hence, to ensure such entities report cyber incidents and/or cyber security incidents (on meeting the prescribed threshold) within the prescribed six-hour time frame should enable and store as many logs as possible/required.

Repercussion for non-compliance with CERT-IN Directions

Non-compliance with the CERT-In Directions may result in imprisonment for a period of up to 1 year or a fine of up to INR 100,000 or both. However, in most cases, imprisonment is usually not resorted to at first instance.

Conclusion

Considering the ever-increasing preference for consumers to transact digitally, businesses must approach cyber risk holistically to manage and support their decision-making. Given the emerging standards like CERT-In's updated directions, integrating cybersecurity and regulatory compliance with business strategy can be beneficial.