September 28, 2022

CERT-IN'S SIX HOUR REPORTING RULE FOR CYBER SECURITY INCIDENTS

- Statutory Interpretation and Analysis

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA

Index

Introduction

Any person affected by a cyber security incident is required to mandatorily report such incident to the Indian Computer Emergency Response Team ("**CERT-In**") if it is of a specified type. With effect the June 27, 2022, the deadline for such reporting has been fixed at 6 (six) hours of the incident being noticed or being brought to the attention of the concerned person. This paper analyses this new rule and its impact and compares it against similar rules for reporting cyber security incident across the world.

The Indian Computer Emergency Response Team

The CERT-In is the national nodal agency for responding to computer security incidents as and when they occur and has been operational since 2004[1] though it was given statutory backing only in 2009.

On October 27, 2009, Sections 70A and 70B were introduced in the Information Technology Act, 2000 ("**IT Act**"). Section 70B of the IT Act provides that the Central Government shall appoint an agency of the Government to be called the CERT-In. The IT Act envisages the following functions for CERT-In:

a. Collection, analysis and dissemination of information on cyber incidents;
b. Forecast and alerts of cyber security incidents;
c. Emergency measures for handling cyber security incidents;
d. Coordination of cyber incidents response activities;
e. Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents; and
f. Such other functions relating to cyber security as may be prescribed.

Pursuant to the introduction of Section 70B in the IT Act, the government framed the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**Cert-In Rules**"). The Cert-In Rules state that CERT-In shall be a part of and under the administrative control of the Department of Electronics and Information Technology, Ministry of Communications and Information Technology. CERT-In shall be located at Electronics Niketan, 6, CGO Complex, Lodhi Road, New Delhi-110003. CERT-In is expected to function on a 24-hours basis on all days of the year including government and other holidays.

The Cert-In Rules provide a framework for the operation of CERT-In, the composition of its Advisory Committee[2] and Review Committee[3], its powers to collect or disclose information. They also impose an important reporting obligation on Indian entities that are at the receiving end of a cybersecurity attack, which is discussed below in detail and is the primary focus of this paper.

Obligation to report cybersecurity attacks

Rule 12(a) of the Cert-In Rules deals with incident reporting, response and information dissemination. Rule 12 requires CERT-In to operate an Incident Response Help Desk on a 24 hour basis on all days including government and other public holidays to facilitate reporting of cyber security incidents. Rule 12(a) reads as follows:

> *Reporting of incidents: Any individual, organisation or corporate entity affected by cyber security incidents may report the incident to CERT-In. The type of cyber security incidents*

[1] As per CERT-In's website (https://www.meity.gov.in/content/icert)

[2] The CERT-In Advisory Committee advises CERT-In on matters of policy and services related to cyber security and ensures that CERT-In can carry out its mandated roles and functions. The Advisory Committee comprises of the Secretary, Department of Electronics and Information Technology (in the capacity of Chairman) and representatives of various ministries of the Government of India, government departments and statutory organisations.

[3] A Review Committee has been formed under the CERT-In Rules to review any non-compliance with provisions of the CERT-In Rules including the rules for communication, seeking information under Rule 14 and directions issued under Rule 15. The Review Committee comprises of the Secretary, Department of Electronics and Information Technology as the Chairman, Group Coordinator (Cyber Law and e-Security) of the department as the Member-Convener as well as Joint Secretaries and equivalent officers of various ministries and departments of the Government of India.

as identified in Annexure shall be mandatorily reported to CERT-In as early as possible to leave scope for action. Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action.

Therefore, Rule 12(a) provides for two types of reporting, which are:

a. Any individual, organisation or corporate entity affected by a cyber security incident may, at its option and sole discretion, report the incident to CERT-In.
b. If any individual or organization, if affected by a cyber security incident which is of the nature as detailed in Annexure of the Cert-In Rules, such cyber security incident has to be mandatorily reported to CERT-In as early as possible to leave scope for action.

The requirement in Rule 12(a) states that, "*Service providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action*" could be interpreted to apply to both the voluntary and mandatory reporting or only to the mandatory reporting. The use of the word "*shall*" seems to indicate that the requirement to report "*within a reasonable time of occurrence or noticing the incident"* applies only to the mandatory reporting of cyber security incident which is of the nature as detailed in the Annexure of the Cert-In Rules. However, the absence of any reference to the Annexure of the Cert-In Rules could be interpreted to mean that the requirement to report "*within a reasonable time of occurrence or noticing the incident"* applies even to the voluntary reporting of incidents which are not listed in the Annexure of the Cert-In Rules. The words, "*to have scope for timely action*" at the end of Rule 12 (a) seem to suggest that even a voluntary report should be filed "*within a reasonable time of occurrence or noticing the incident"* or not filed at all. Though Rule 12 (a) of the Cert-In Rules does not say so expressly, it may be presumed that 'timely action' shall be from CERT-In and not from the affected entity.

The Annexure to the Cert-In Rules lists the following types of cyber security incidents which needs to be mandatorily reported to CERT-In:

a. Targeted scanning/ probing of critical networks/ systems;
b. Compromise of critical systems/ information;
c. Unauthorised access of IT systems/ data;
d. Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.;
e. Malicious code attacks such as spreading of virus/ worm/ Trojan/ Botnets/ Spyware;
f. Attacks on servers such as Database, Mail and DNS and network devices such as Routers;
g. Identity Theft, spoofing and phishing attacks;
h. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
i. Attacks on Critical infrastructure. SCADA Systems and Wireless networks
j. Attacks on Applications such as E-Governance, E-Commerce etc.

The various types of cyber security incidents do overlap and more importantly over a wide array of nefarious activities. The terms used in the Annexure are not defined, but even laypersons would be able to understand most of them. Terms such as "identity theft", "spoofing" and "phishing" are now everyday terms and there is little ambiguity about them. Denial of Service (DoS) and Distributed Denial of Service (DDoS) may not be so well understood and these mean as follows:

a. **Denial of Service (DoS):** A DoS attack is a type of cyber-attack in which a perpetrator attempts to render a computer resource dysfunctional, so as to make it unavailable for its intended users. This may also be done by temporarily or permanently damaging the services of a host connected to a network.

b. **Distributed Denial of Service (DDoS):** In a DDoS attack, the perpetrator renders an internet network unusable for genuine users and prevents them from accessing online services and sites available on such network by overflowing the network with internet traffic.

CERT-In's website details the incident reporting mechanism and provides a form to fill in while reporting an incident. The webpage detailing the incident reporting mechanism can be accessed here. The form on CERT-In's website can be accessed here.

Rule 11(1)(a) of the Cert-In Rules state that, "*CERT-In shall address all types of cyber security incidents cyber incidents which occur or are expected to occur in the country*". Though the Cert-In Rules do not expressly state whether reporting to CERT-In is required when pursuant to a global cyber security incident it is unclear if Indian operations have been impacted, it has become common practice to report global cyber security incidents to CERT-In where Indian data or Indian residents may have been affected, unless the affected entity is sure that Indian operations have not been affected or impacted.

Recent changes to reporting deadlines for cybersecurity attacks

On April 28, 2022, MeitY issued directions *vide* notification No. 20(3)/2022-CERT-In (**"Notification"**) which set out extensive compliances and reporting obligations for body corporates and increased the ambit of power of CERT-In. The Notification has now made it mandatory to report cyber incidents (listed in Annexure A of the Notification) within 6 (six) hours of the incident being noticed or being brought to the attention of the concerned person. The Notification, which will become effective from June 27, 2022, states that the compliances have become unavoidable to ensure effective response activities to cyber security incidents because the relevant information is very often not found or is not readily available with the concerned body corporate or service provider. This causes an unnecessary delay in analysing and investigating the incident.

The Notification has attracted extensive criticism. On May 26, 2022, industry associations and lobby groups which, *inter-alia,* including the US Chamber of Commerce (USCC), US-India Business Council (USIBC), The Software Alliance (BSA) submitted a letter to the director-general of CERT-In claiming that:

a. the Notification will create a fragmented cross jurisdictional approach towards cybersecurity. As a result, it will undermine India's security posture and will gradually make it difficult for businesses to continue operating in India.
b. 6 (six) hours is not sufficient for the entity to identify the nature of the crime and determine whether it falls under Annexure A of the Notification.
c. CERT-In ought to delay implementation of the directions and undertake a second and more detailed consultation with the wider public.

MeitY also received requests from various quarters to extend the timeline to 72 hours, which has been rejected by MeitY. MeitY stated that the nature and type of cybercrimes is not what it used to be and has become very complex, allowing these crimes to be committed from remote jurisdictions, without leaving any trace. This makes it imperative for the incident to be reported at the earliest for the response team to be able to take prompt action. At a meeting held between industry stakeholders and government officials on June 10, 2022, MeitY defended the 6-hour timeline on the ground that if people report robbery as soon as they get to know about it, they should do the same for a cyber security breach too.

The new time frame will require business entities to re-evaluate their internal mechanisms with respect to reporting cyber incidents and reallot resources towards that effect. Further, businesses

have already stated[4] that the new reporting deadline will make it difficult for them to operate in India. However, MeitY has refused to budge.

The Notification does not offer any clarity with respect to the reporting of global cyber security incidents where Indian data or Indian residents may have been affected. Would the six-hour period kick in from the time the global cyber security incident was noticed or from the time the possible impact on Indian data or Indian residents was noticed? In many instances, after a cyber security incident affecting an MNC with global operations, it takes many days to figure out which countries or regions and whose data is affected by such incident. It may be possible to argue that in such cases, the six-hour clock for the mandatory reporting to CERT-In shall ticking only after it is reasonably clear that India or data pertaining to Indian residents is affected.

Unlike in many other countries, the information sought to be obtained by CERT-In, through the CERT-In incident reporting form is basic in nature (type of incident, domain/ URL, IP address, etc.) and not very detailed. For instance, in Germany the report to be filed requires assessment information such as the number of users affected, duration of the incident and the detailed steps taken to minimise the damage. Relaxation in reporting is given to organisations who do not have access to such information. Interestingly there is no obligation under the CERT-In Rules to mandatorily file a detailed follow-on report when more information becomes available. However, it is possible that CERT-In may selectively seek more information at its discretion.

Vide a notification dated June 27, 2022, CERT-In extended the deadline of June 27, 2022 for compliance with the Notification to September 25, 2022 for certain specific entities, namely, (i) MSMEs which meet the criteria for MSMEs notified by the Ministry of Micro Small and Medium Enterprises *vide* its notification no. 2020 S.O. 1702(E) dated June 1, 2020 and (ii) Data Centres, VPS providers, Clous Service providers and VPN service providers, subject to their compliance with the requirement of registration and maintenance of validated names of subscribers/ customers hiring the services and validated addresses and contact numbers as provided in paragraphs (v) a. and f. of the Notification.

Impact of new deadline on incidents prior to June 27, 2022

The new 6 (six) hour deadline does not have retrospective effect and will apply only to cyber security incidents that take place on or after June 27, 2022.

However, new 6 (six) hour deadline has exposed CERT-In's thought process and it is now clear that CERT-In believes that it is possible for every organisation affected by a cyber security incident to report such incident to CERT-In within 6 (six) hours of noticing such incident. In light of this, it is interesting to see how CERT-In will view cyber security incidents that took place prior to June 27, 2022 and were required to be reported to CERT-In under the '*as early as possible standard*', but were reported to CERT-In without undue haste.

Let's assume that a cyber security incident (which is listed in the Annexure to the Notification) affected an Indian business organisation on June 10, 2022. This organisation took stock of such incident, carried out an assessment of its impact on its employees and customers and their data and reported such incident to CERT-In within 2 (two) weeks of noticing the incident, that is, by June 24, 2022. The Notification became effective from June 27, 2022. Is CERT-In now likely to take the view that the business organisation did not report such incident to CERT-In as early as possible to leave scope for action even though the new 6 (six) hour deadline for reporting cyber

[4] https://www.bsa.org/news-events/media/lobby-groups-write-to-govt-say-cert-in-directions-will-make-it-difficult-for-companies-to-do-business-in-india
https://economictimes.indiatimes.com/tech/technology/cert-ins-requirements-may-make-it-difficult-to-do-business-in-india-business-groupings/articleshow/91842557.cms?from=mdr
https://indianexpress.com/article/business/cybersecurity-norms-may-make-it-difficult-to-do-biz-in-india-11-industry-bodies-to-cert-in-7940437/

security incidents was not in force at the time of the incident or at the time of filing of the incident report? What if a cyber security incident affected an Indian business organisation on June 26, 2022 and was reported to CERT-In only after a week of such incident. If such incident had taken place a day later (on June 27, 2022), the new six-hour deadline would have applied. It is possible that CERT-In may take the view that entities who reported incidents that took place in the recent past, but before June 27, 2022, did not report them as "early as possible", if the reporting was not done within a day or two of the incidents.

Consequences of non-compliance with reporting obligation

Penalty for non-compliance

The Cert-In Rules do not prescribe any penalty for breach of the reporting obligation in Rule 12 of the Cert-In Rules. However, Section 70B(7) of the IT Act provides that any service provider, intermediary, data center, body corporate or person who fails comply with any direction issued by Cert-In shall be punishable with imprisonment for a term which may extend to 1 (one) year or with fine which may extend to Rs. 1,00,000 (Rupees one lac) or with both.

Procedure for imposition of penalty

It is noteworthy that the Notification has been issued under Section 70B(6) of the IT Act, which provides that Cert-In may issue directions to service providers, intermediaries, data centers, body corporates or any other persons for carrying out its functions as listed in Section 70B(4) of the IT Act. A similar power to issue directions has been provided to Cert-In under Rules 15 and 16 of the Cert-In Rules. The afore-mentioned Rule 16 enables the designated officer of Cert-In to submit a report to the Director General of Cert-In in case of any non-compliance with the directions issued under Section 70B(6) of the IT Act. This report is submitted to the Review Committee, which thereon may issue directions to the Director General to file a complaint before the court under Section 70B(8) of the IT Act.

When non-compliance is being adjudicated in a court of law, the party accused of non-compliance with the Notification shall be allowed an opportunity to be heard before the court. Thereon, the relevant court may impose a penalty which is proportionate to the breach committed by the party alleged to be non-compliant.

Need for express exceptions

The Cert-In Rules or the Notification do not expressly provide any exceptions in case of a failure to report a cyber security incident within the six-hour deadline. It is possible that due to a number of legitimate reasons, a party may fail to report a cyber security incident within the prescribed period of 6 (six) hours from the time such incident was noticed. For example, pursuant to or at the time of a cyber security incident, it may be possible that the senior management of the affected entity were in no position to report such incident within the prescribed period of six hours. The Notification has introduced one of the most stringent deadlines in the world for notification of cyber-security incidents, with failure to comply inviting not only a fine, but also imprisonment.

Even though the Cert-In Rules and the Notification do not expressly provide any exceptions, it is very likely that any court adjudicating on a report to comply with Rule 12 of the CERT-In Rules will take into account any extenuating circumstances before imposing any fine or other penalty. It is hoped that the Cert-In Rules shall be amended in the near future to incorporate specific exemptions to the obligation to report within 6 hours, such as a failure to report a cyber security incident within the prescribed deadline due to any injury or harm suffered during or in the course of the incident which resulted in the cyber security incident.

Filing an FIR alongside reporting to CERT-In

Sections 154 and 155 of the Criminal Procedure Code, 1973 ("**CrPC**") deal with the filing of a first information report ("**FIR**") with the police relating to the commission of cognisable and non-cognisable offences respectively. It is not mandatory to file an FIR even if one witnesses an offence being committed or is the victim of an offence. This position is in stark contrast with the mandatory requirement to report to CERT-In in the event of a cyber security incident. It may be argued that the government is justified in making it compulsory to report cyber security incidents to CERT-In in order to enable the government to monitor and ensure cyber security in India. However, it is possible to counter-argue that just as the government needs to monitor and ensure cyber security, it is equally important to monitor and control other offences. So, why isn't it mandatory to file an FIR if one is affected by an offence under the Indian Penal Code, 1860 ("**IPC**") or vice-versa, why should it be mandatory to report to CERT-In if one is affected by a cyber security incident? There is no easy answer to this question.

The next question arises whether it is possible for an FIR to be filed pursuant to any cyber security incident. In our view, it is definitely possible to do so if the cyber security incident has resulted in an offence under the IPC. In certain instances, local police authorities may be in a better position to take appropriate action faster than CERT-In, pursuant to a cyber security incident. However, filing an FIR would not satisfy the requirement to report to CERT-In under the CERT-In Rules.

On July 16, 2022, the Securities and Exchange Board of India ("**SEBI**") reported that a cyber security incident was noticed on SEBI's e-mail system which was undergoing a system upgrade and that SEBI had filed an FIR as well as informed CERT-In[5].

Deadlines and grounds for reporting cyber security incidents – an international round up:

Most countries now have detailed rules for the reporting of cyber security incidents. Here's a brief review of the position in a few countries across the globe.

USA

The United States` Government has introduced a series of new measures involving the notification and disclosure of major cyberattacks and cyber incidents. These measures were introduced after numerous ransomware attacks occurred on United States` companies and critical infrastructure.

The Cyber Incident Reporting for Critical Infrastructure Act, 2022 ("**CIRCIA**"), a key legislation akin to the CERT-In Rules, was signed into law by President Biden in March, 2022. The CIRCIA requires owners of critical infrastructure to notify the Department of Homeland Security's "Cybersecurity and Infrastructure Security Agency (CISA) of cyber-attacks that result in "unauthorised access or disruption of business or industrial operations". The definition of 'covered critical infrastructure' under CIRCIA is wide and even covers businesses which may not consider themselves to be infrastructure or 'critical infrastructure' providers. A timeline of 72 (seventy-two) hours after the covered entity reasonably believes that the covered cyber incident has occurred is prescribed under CIRCIA to report certain types of cyber incidents to CISA. However, ransomware payments are required to be reported within 24 (twenty-two) hours of the payment being made. The CIRCIA also allows for supplemental reporting by covered entities after making an initial report of a covered cyber incident or ransom payment. Such supplemental reporting is required to be done 'promptly' if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting the covered cyber incident report. The obligation to file

[5] PR No.23/2022 (https://www.sebi.gov.in/media/press-releases/jul-2022/sebi-files-fir-for-cyber-security-incident_60871.html)

supplemental reports is a continuing obligation and only ends after the covered entity has notified the CISA that the covered cyber incident has been fully mitigated or resolved.

Notification and reporting obligations have also emerged through various US Government decisions including reporting under the Cyber Incident Reporting for Critical Infrastructure Act, 2022, Securities and Exchange Commission (SEC) rules as well as Executive Order 14208 issued on May 12, 2021.

UK

The Security of Networks and Information Systems Regulations ("**NIS Regulations**") came into force in the UK in May, 2018. The NIS Regulations require organisations to notify the Information Commissioner's Office ("**ICO**") in the UK of any incident that has a substantial impact on the provision of such organisation's services. *Any event having an actual adverse effect on the security of network and information systems* has to be reported under the NIS regulations.

As per the NIS Regulations, the affected party is required to notify the ICO of any incident without undue delay and not later than 72 (seventy-two) hours of becoming aware of the incident. This 72 (seventy-two) hour requirement is broadly in line with the requirement prescribed under the UK's General Data Protection Regulation (UK GDPR). The information required to be provided includes (i) the name of the organisation which suffered the incident, types of digital services provided by such organisation, (ii) the time at which the incident occurred, (iii) duration of the incident, (iv) information about the nature and impact of the incident, (v) information about any cross-border impact that the incident may have had and any other information which may be helpful to the ICO.

The ICO generally shares incident notifications with the National Cyber Security Centre ("**NCSC**"). However affected parties are also advised to voluntarily report cyber security incidents to the NCSC if it is determined by the reporting party that NCSC's support will be required to manage the incident.

Australia:

The Security of Critical Infrastructure Act 2018 ("**SOCI Act**") of Australia classifies various types of assets as critical assets. Critical assets include telcos, internet service providers, data storage and processing organisations, banking, insurance and finance institutions and extends to fuel companies and food and grocery assets. The SOCI Act was brought into force on April 8, 2022 with a grace period of 3 (three) months for implementation, ending on July 8, 2022.

The Australian government also introduced expanded rules to the SOCI Act which provide for *mandatory reporting* of cyber security incidents to the Australian Cyber Security Centre ("**ACSC**") by regulated entities under Part 2b of the SOCI Act. As per the expanded rules, if an entity is a regulated entity and becomes aware of occurrence of a critical cyber security incident where such incident has had or is likely to have a relevant impact on the entity's assets, then such incident must be verbally notified to the ACSC within a period of 12 (twelve) hours upon becoming aware of the incident. Verbal notification, if any, should be followed by a written report to the ACSC within 84 (eighty-four) hours of verbally notifying the ACSC. Similarly, in case of other, non-*critical* cyber security incidents, the reporting must be done within 72 (seventy-two) hours of becoming aware of the incident. Verbal notification must be followed by a written record within 48 (forty-eight) hours of verbally notifying the ACSC.

A critical cyber security event is when the event has had or is having a significant impact on the availability of the asset. A significant impact is when the critical infrastructure asset is used in connection with the provision of essential goods or services and the incident has materially disrupted the availability of the essential goods or services delivered by the critical infrastructure asset.

Germany:

The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, in German which is abbreviated as "BSI") is the agency in Germany responsible for managing computer and communication security. The relevant reporting legislation, called the 'Act on the Federal Office for Information Security' (**"BSIG"**) provides incident reporting timelines for critical infrastructure providers and digital service providers. Critical infrastructure includes facilities belonging to the energy, information technology and telecommunications, transportation and traffic, health, water, nutrition and the finance and insurance sectors which are of high importance for the normal functioning of the community. The BSIG places a duty on the critical infrastructure operators to 'immediately' report to the BSI any IT disruptions relating to the availability, integrity, authenticity and confidentiality of their information technology systems which already have or may result in a malfunction or significant impairment of the functionality of the critical infrastructures.

With respect to digital service providers, Section 8(c)(3) of BSIG, requires them to 'immediately report' any security incident which materially impacts the provision of the digital services by the provider. The parameters taken into consideration while determining if a security incident is 'material', are:

a. number of users affected by the security incident,
b. duration of the security incident,
c. geographic area affected by the security incident,
d. extent of interruption of the provision of the service,
e. extent of the effects on economic and social activities.

It is important to note that Section 8(c)(3) of BSIG excludes the application of this provision to the service providers who do not have enough information to assess the impact of the security incident as per the afore-mentioned parameters. Hence, it appears that the timeline for immediate reporting gets triggered only after the digital service provider has evaluated the consequences of the incident.

EU Regulation no. 910/2014 on Electronic Identification and Trust Services for Electronic Transactions In The Internal Market (**"EU Regulation"**) enumerates the security requirements applicable to trust service providers throughout its member states. Trust service providers are those who provide services relating to the creation, verification and validation of electronic signatures website authentication and preservation of electronic signatures, seals or certificates.

Article 19 of the EU Regulation requires trust service providers to take measures to prevent and minimise the impact of security incidents. If a security incident occurs, the trust service provider is required to report it to the relevant authority within 24 (twenty-four) hours of becoming aware of it. It is notable that despite providing a maximum timeline of 24 (twenty-hours), Article 19 of the EU Regulation also encourages the incident to be reported 'without undue delay'.

France:

As per Article 33 of the European Union's General Data Protection Regulation (EU GDPR), there is an obligation on all data controllers to notify any incidents to the competent data controlling body unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In France, the competent authority is National Commission for Information Technology and Civil Liberties (**"CNIL"**) to whom the incident must be reported within 72 (seventy-two) hours of the discovery of the breach. The report must contain the following details:

a. description of the incident;
b. indication of the category of the affected data;
c. affected data subjects;
d. detailed description of the measures taken to remedy or mitigate negative effects; and

e. name and contact details of the data protection officer.

Article 83 of the French Data Protection Act provides that data service providers must notify any data breach to the CNIL 'without undue delay'.

The National Cybersecurity Agency of France (**"ANSSI"**) spearheaded the transposition of EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (**"NIS Directive"**) into French national law. The NIS Directive requires digital service providers and operators of essential services to report any incident having or likely to have a significant impact on the continuity of services to ANSSI 'without undue delay'.

Canada:

Canada does not have a unified, country-wide regulatory framework for the reporting of cyber security incidents. Instead, a heterogenous system imposing reporting requirements exists. This system is formulated at an industrial level, with statutory regulators for industries formulating rules that impose such requirements.

The Personal Information Protection and Electronic Documents Act, 2000 (**"PIPED Act"**) requires reporting of cyber security incidents impacting personal information collected by businesses for commercial purposes. Under Division 1.1 of the PIPED Act, organisations must report any breaches to the Privacy Commissioner 'as soon as feasible', upon determination of breach by the relevant organisation. Pertinently, this reporting requirement gets triggered when reasonable circumstances dictate that the breach poses Real Risk of Significant Harm ("**RRSH**") to any individual. The sensitivity of the personal information involved in the breach and the likelihood of the information being misused are weighed in while determining RRSH.

Financial institutions in the country are subjected to regulatory scrutiny by Office of the Superintendent of Financial Institutions ("**OSFI**"). In exercise of its powers, the OSFI formulated the Technology and Cyber Security Incident Reporting Advisory (**"Advisory"**) effective from August 16, 2021. The Advisory is applicable to Federally Regulated Financial Institutions (**"FRFI"**). As per the Advisory, FRFIs are required to make an initial report of any cyber security incident to OSFI's Technology Risk Division and their Lead Supervisor within 24 (twenty-four) hours of the incident, 'or sooner if possible'. The intimation to OSFI's Technology Risk Division must be made in the Incident Reporting and Resolution Form (**"Form"**). The Advisory provides that in the absence of specific information required to be filled in the Form, FRFI may specify 'information not yet available'. This gives the impression that the clock for reporting starts ticking as soon as the FRFI has noticed the incident, and it may take full stock of the incident after making the initial reporting. This is further evidenced by the subsequent reporting requirements where OSFI expects FRFIs to provide situation updates, including any short term and long-term remediation actions and plans until the incident in contained.

Reporting requirements also exist under the Investment Industry Regulatory Organisation of Canada ("**IIROC**"), which requires dealers to make an initial incident report to IIROC within 3 (three) calendar days of discovery of the incident. A 'dealer' is an investment dealer in accordance with securities legislation. The initial report is meant to reflect only a preliminary assessment of the cybersecurity incident, as per the best information available to them at the time of reporting. A detailed incident investigation report has to be filed with the IIROC after the dealer has undertaken a thorough investigation of the incident.

Conclusion

The new 6 (six) hour deadline imposed by CERT-In is way stricter than the deadlines prevalent in the developed world. It is stricter than the timeline of 72 (seventy-two) hours imposed in the US under CIRCIA and in the UK under the NIS Regulations. The requirement in Australia to verbally notify the ACSC within a period of 12 (twelve) hours upon becoming aware of the incident, followed by a written report to the ACSC within 84 (eighty-four) hours of verbally notifying the ACSC, also appears to be much less harsh than the new Indian deadline. In Germany, the requirement to 'immediately' report an incident under the BSIG applies only to critical infrastructure operators and digital service providers. The EU Regulation imposes a 24-hour deadline, but only on essential trust service providers. In France, only data service providers are required to notify any data breach to the CNIL 'without undue delay'. In Canada, the PIPED Act requires organisations to report any breaches 'as soon as feasible', but only when reasonable circumstances dictate that the breach poses Real Risk of Significant Harm to any individual. Further, Federally Regulated Financial Institutions must make an initial report of any cyber security incident within 24 (twenty-four) hours of the incident, 'or sooner if possible'. Investment dealers are given 3 (three) calendar days after discovery of an incident to file an initial incident report.

The biggest draw-backs of CERT-In's reporting deadline seem to be that (i) it is not selectively imposed on critical service providers or digital service providers but applies to all and sundry and (ii) follow-on reporting is not mandatory after full details of the cyber security incident become clear. Though CERT-In can selectively seek more information at its discretion, it is unclear as to what extent CERT-In can sieve through the flood of half-baked and premature reports received immediately after the occurrence of cyber security incidents and seek more information from the affected parties.

Contributors

Vinod Joseph, Partner
vinod.joseph@argus-p.com

Aryan Mohindroo, Associate
aryan.mohindroo@argus-p.com

Anushkaa Shekhar, Associate
anushkaa.shekhar@argus-p.com

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com