Reporting cybersecurity breaches in India – Is it time to overhaul the law?

Friday, May 28, 2021

Article By
Aparna Gaur
Aarushi Jain
Gowree Gokhale
Dr. Mihir A. Parikh
Nishith Desai Associates

Related Practices & Jurisdictions
Administrative & Regulatory
Communications, Media & Internet
Criminal Law / Business Crimes
Corporate & Business Organizations
Election Law / Legislative News
Global
India
PRINTER-FRIENDLY
EMAIL THIS ARTICLE
DOWNLOAD PDF
REPRINTS & PERMISSIONS
Tweet
Like 9

Cyberattacks are on the rise worldwide and India is not left behind. Cyberattacks on Juspay, Unacademy, BigBasket, MobiKwik, Airtel and AirIndia are among the recent ones where personal data of millions of customers were stolen.[1] We have also witnessed massive cyberattacks on critical health infrastructure, including hospitals and vaccine makers.[2]

During the pandemic, digitization accelerated by manifold. While steps are being taken to ensure a smooth transition from physical to digital world, the focus on security measures to prevent cyberattacks is still lacking. Unfortunately, one weak link in the system can collapse the entire network.

Countering cyberattacks requires preventive actions by, immediate response from, and coordination among entities at various levels, including individual users, organizations, technology companies, data services providers, and governments. In several jurisdictions, one of the key aspects towards creating robust systems is to have timely knowledge and reporting of these attacks to the specialized government agencies which are responsible for alerting law enforcement agencies for quick action against the perpetrators.

In this article, we examine the insufficiency of the regulatory mechanisms put in place to bound businesses in India to report data breach incidents to their customers or to government agencies.

CERT-In and Its Limitations

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rule, 2013[3] ("**Rules**") provide for mandatory reporting of certain types of Cyberattacks to a national agency, the Indian Computer Emergency Response Team ("**CERT-In**") which remains functioning on 24-hour basis on all days of the year.[4] The role of CERT-In is to interact with and seek assistance from various stakeholders defined in Rule 10 of the Rules to collect, share and disseminate information and also to respond and prevent cyber security incidents.

While this is an important step toward, the Rules lack clarity on several aspects, such as time within which incidents must be reported, nature of incidents to be reported, the potential risk level, etc., This may result in inconsistent reporting of Cyberattacks.

Types of Cyberattacks

Reporting of certain types of "cyber security incidents" to CERT-In is mandatory.[5] However, little guidance is provided on what these incidents mean and what level of impact they can have. For instance, while the terms "spoofing", "phishing" are commonly used terms, there is no legal definition of the terms in the Rules or the Information Technology Act, 2000 ("**IT Act**"). Some of the listed incidents are vaguely identified, such as compromise of critical systems/information. Some of the listed incidents may be extremely common and even difficult to identify, such as targeted scanning/probing of critical networks/systems.

Ransomware type Cyberattacks are on the rise.[6] Here, attackers block access to certain database and demand users to pay a ransom, often in the form of cryptocurrency, to unblock it. They are expected to hit $6 trillion worldwide in the current year; double the damage since 2015.[7] Ransomware are becoming increasingly common and hurtful. However, ransomware do not fit directly in to any one or combination of the types of incidents listed in the Rules. While CERT-in has reported various instances of ransomware, there is a need to put a systemic mechanism in place that is not limited to not encouraging individuals or organizations to pay the ransom.

From a reading of the definition of "cyber security incidents"[8], it appears that the focus of the Rules is on incidents that violate security policies of an organization and involve some degree of unauthorised use/access of a computer resources/disruption or denial or services. Companies when faced with cyberattacks must therefore assess if the incident is a result of unauthorised use/access/disruption or denial or services. Incidents resulting in a data breach that have occurred due to internal errors, actions of employees authorised by the company, etc. may therefore not be within the scope of the Rules. This assessment must be done on a case to case basis.

Cyberattacks are happening not only on networks and databases but also on firms that develop security testing tools. When such security testing tools are compromised, cyberattacks go unnoticed and proliferate before huge damage across various companies surfaces. Such was the case in the SolarWinds cyberattack in which "Sunburst" malware was introduced into cybersecurity management software, Orion.[9] These types of cyberattacks do not fit well within the incidents listed by the Rules.

Critical Services

CERT-In provides various critical services in dealing with cyberattacks,[10] including responding to cyber security incidents, predicting and preventing them, undertaking their forensic analysis, information security assurance and audits. But it does not provide the service or mandating any requirement of reporting cyberattacks to customers whose data may have been affected. This gap in taking proactive steps to make crucial information

RELATED LEGAL HEADLINES
Digital June Part 5: Preferential Treatment & Exclusivity on Platforms [VIDEO]
By Vyapak Desai
International Investments Regulations Through the Lens of National Security: How the U.S. differs from India?
By Yashasvi Tripathi
Data Privacy Standards Issued in India – Legal Compliance or New Brand Differentiator?
By Purushotham Kittane
Going from SPAC to SPACtacular in India: Exploring Competition Law Exemptions & Relaxations Available to SPAC Structures
By Vaibhav Parikh
TRENDING LEGAL ANALYSIS
Amicus Briefs, OSHA, and the Sixth Circuit
By Squire Patton Boggs (US) LLP
Mexico's New Minimum Wage for 2022
By Ogletree, Deakins, Nash, Smoak & Stewart, P.C.
Present But Not Accounted For: NYSE Amends Treatment Of Abstentions In Certain...
By Nelson Mullins
ALERT: New State Privacy Requirements for Mortgages Funded After December 1, 2021
By Bradley Arant Boult Cummings LLP

immediately available to direct or indirect victims of cyberattacks can amplify the damage caused by them.

In addition, regular penetration testing and security audit are important weapons to prevent cyberattacks. Unfortunately, CERT-In has limited resources to undertake these activities. As per its latest available annual report, it had appointed only 90 technical IT security auditors.[11] These numbers are woefully small compared to the size and extent of IT infrastructure of the country. Also, there is no requirement of businesses to submit their own IT security audit reports and assess them.

The Rule 11(1) notes that CERT-In shall address all types of cyberattacks, but its level of support will vary depending on the type and severity of the incident, affected entity, and resources available with CERT-In at that time. It also prioritises the allocation of resources depending on the perceived impact of a cyberattack. While flexibility in the level of support is necessary, invariably, the full extent of the impact of a cyberattack is not known until the attack has already spread widely. There should be some minimum requirement for the level of support for all reported incidents and accordingly allocation of resources.

Coordination

Increasingly, cyberattacks are not limited to business network or data theft, but they are aimed at affecting vital infrastructure, such as power grid, power plant operations, water infrastructure, transit systems, government services, oil supply lines, etc. Recently, a cyberattack shutdown Colonial Pipeline system, which normally transports about 45% of fuel consumed on the East Coast of the US.[12] National Critical Information Infrastructure Protection Centre (NCIIPC) is the national nodal agency for the protection of Critical Information Infrastructure set up under Rule 2(n) of the Rules. NCIIPC is set up under National Technical Research Organisation, which is separate from CERT-In. Any delays in coordination between these two agencies and with infrastructure organizations can have devastating effects when the infrastructure faces a significant cyberattack.

Who Should Report?

The Rules provide that individuals, organisations or corporate entities affected by "cyber security incidents" **may** report such incidents to CERT-In.[13] There are many cyberattack cases, where multiple parties are 'affected' by a cyber security incident. For example, in case of a cyberattack affecting systems of a B2B service provider, it is possible that in addition to the service provider, the client is also "affected" by the incident. In such a situation, it is unclear which party needs to report the cyber security incident. Parties affected may choose to do joint reporting or contractually agree on who bears the obligation to report.

The Rules also specify that service providers, intermediaries, data centres and body corporates must report cyber security incidents to CERT-In "within a reasonable time of occurrence or noticing the incident". What is meant by "reasonable time" has not been clarified in the Rules and remains open for interpretation.

Reporting by Entities Outside of India

Section 75 of the IT Act provides that the provisions of the IT Act are applicable to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Therefore, with respect to offences being committed outside of India, it is clear that the provisions of the IT Act will be applicable if the offence involves a computer/ computer system/ computer network located in India. However, from a reporting perspective, the question remains whether the Rules are applicable in cases where both the entity and its computer resources outside of India, but the data of Indian customers is breached. It appears that in such a case, the mandatory reporting does not get triggered.

Consequence of Non-Compliance

The Rules do not provide any consequences for non-compliance with the reporting requirement. Non-compliance with the reporting requirement would attract a penalty of up to INR 25,000 as provided in the IT Act.[14] The IT Act does provide for a penalty of imprisonment of up to one year and a fine of up to one lakh rupees or both in case a service provider, intermediaries, data centres, body corporate or person fails to provide the information called for by Cert-In or if such service provider, intermediaries, data centres, body corporate or person fails to comply with any directions issued by Cert-In.

With respect to intermediaries, in addition to the abovementioned monetary penalty, non-compliance may result in loss of safe harbour provided under Section 79 of the IT Act. Reporting as per the Rules is an obligation imposed upon intermediaries under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[15] ("**2021 Rules**") and non-compliance with the 2021 Rules can result in loss of safe harbour.[16]

Key Takeaways

The Rules that provide mandate to CERT-In and NCIIPC were notified in 2014. A lot has changed in the last seven years. It may be time to review the Rules and update them. While the existing agencies are making the best efforts, the law in relation to cyber security may need an overhaul to address issues discussed above.

To avoid cyber security breaches, businesses must ensure implementing effective cyber security plans and policies. Nodal agencies need to continue to update standards required for such plans in response to continuously evolving cyber security landscape. Such plans should essentially include policies related to handling of proprietary information, use of personal devices by employees, training of employees dealing with sensitive and proprietary data, etc. Cyber security plans are essential not only for well-established businesses but also small businesses and start-ups which are often vulnerable to attacks due to poor cyber security infrastructures. Businesses should also have policies to follow if a cyber security breach has occurred. While India does not have a law requiring reporting of breaches to customers, some organisations voluntarily do so in good faith. The decision to voluntarily inform customers should be an informed decision as businesses may open themselves to the risk of consumer litigation.

With timely reporting of all attacks, CERT-In may be able to analyse information and take steps to prevent future attacks. CERT-In can also encourage organisations to conduct awareness programs to educate customers on methods to mitigate cyber security risks. It may be time to revisit the CERT-In Rules to clarify the reporting requirement, the timelines, etc. as well. Currently, CERT-In does not have powers to investigate cyber security incidents to identify the actors behind such attacks. Considering that CERT-In has the technical capabilities to analyse attacks, suggest guidelines to prevent future attacks, it may be the right time to bring in amendments to give more teeth to CERT-In by giving it the power to investigate cybercrimes by itself or assist the relevant law enforcement authorities in investigations.

---

[1] "India becomes favourite destination for cyber criminals amid Covid-19" By Shivani Shinde and Neha Alawadhi. *Business Standard*. 6 April 2021. https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html

[2] Indian Pharma Firms at High Ransomware Attack Risk in 2021. *National Herald*. 23 December 2020. https://www.nationalheraldindia.com/national/indian-pharma-firms-at-high-ransomware-attack-risk-in-

2021

[3] Rules: G.S.R. 20(E) – Available at https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf.

[4] Section 70(B) of the IT Act, 2000. https://indiankanoon.org/doc/80680324/

[5] See Annexure of the Rules.

[6] "Mounting Ransomware Attacks Morph Into a Deadly Concern" by Robert McMillan and Jenny Strasburg. *The Wall Street Journal*, 30 September 2020. https://www.wsj.com/articles/mounting-ransomware-attacks-morph-into-a-de...

[7] "The State of Ransomware in 2021." Blackfog. https://www.blackfog.com/the-state-of-ransomware-in-2021/

[8] Rule 2(1)(h) of the Rules

[9] "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president" Reuters. 14 February 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds...

[10] Rule 9 of the Rules.

[11] CERT-In Annual Report 2019. https://www.cert-in.org.in/

[12] "Restarting U.S. Pipeline Hit by Cyberattack May Not Be Easy" Bloomberg. https://finance.yahoo.com/news/restarting-u-pipeline-hit-cyberattack-025...

[13] Rule 12(1)(a) of the Rules

[14] 45. Residuary penalty.–*Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.*

[15] Rule 3(1)(l) of the 2021 Rules provides that an intermediary shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

[16] Rule 7 of the 2021 Rules states "Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Actshall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code."

National Law Review, Volume XI, Number 148

ABOUT THIS AUTHOR

Aparna Gaur
Senior Member IP & TMT Teams

Aparna is a senior member of the IP and TMT team at Nishith Desai Associates. She is integrally involved in IP transactional and advisory work and handles patent prosecution and IP litigation. She has vast experience in advising clients over a wide spectrum of industries in relation to protection and enforcement of their IP. Aparna has authored several articles on complex IP issues in India.

Aparna has represented clients in IP disputes before the Supreme Court of India, the Delhi High Court and lower courts, the Intellectual Property Appellate Board and the Indian Patents Office....

aparna.gaur@nishithdesai.com
+91 22 6159 5037
www.nishithdesai.com

Aarushi Jain
Education and Intellectual Property Group Co-Leader

Aarushi Jain co-leads the Education and Intellectual Property Groups at the multi-skilled and strategy driven international law firm, Nishith Desai Associates. With a niche focus on education sector, she has advised several clients, including pre-schools, K-12 schools and universities, Ed-Tech companies and strategic investors, both domestic and international, on legal, regulatory and tax issues. Her specialization includes advising foreign universities and platforms with their India business, from a legal perspective. In addition, she also assists clients in collaborations, pathways,...

Aarushi.jain@nishithdesai.com
+91 22 6669 5196
www.nishithdesai.com

Gowree Gokhale

A practicing lawyer for 24 years, Gowree Gokhale leads the IP, Technology, Media and Entertainment, data protection law practice of research and strategy driven international law firm, Nishith Desai Associates. She has assisted several international businesses in India entry strategy, corporate and strategic deals, litigation and arbitration in TMT and Pharma sector. She has spearheaded several policy initiatives for the TMT and Pharma industry including for online content companies, gaming industry, IT industry as also for privacy and data protection laws. She has also...

gowree.gokhale@nishithdesai.com
212-464-7050

www.nishithdesai.com

Dr. Mihir A. Parikh
Dr. Mihir A. Parikh Lawyer Nishith Desai Assoc. India-centric Global Law Firm

Dr. Mihir A. Parikh leads Research and Innovation as well as Strategic Legal Consulting Practice of Nishith Desai Associates—an India-centric global law firm, from the firm's Silicon Valley office in Palo Alto, California. He advises private equity and venture capital firms in investment decisions and creating value for portfolio companies by integrating technology and law as strategic assets. He helps companies understand and apply a strategic legal perspective to manage future business risks, defend competitive advantages, and create new growth opportunities....

Mihir.parikh@nishithdesai.com
650-460-0550
www.nishithdesai.com