CYBERSECURITY

Making CERT-In More Certain


Anoop Narayanan & Priyanka Gupta

There have been media reports of a security and data breach of the Facebook-owned social messaging platform WhatsApp that, among other things, has affected about 1,400 WhatsApp users worldwide, and more than 100 Indians. These reports also indicate that WhatsApp did not adequately report the security breach to the Indian government.

The media has been busy discussing about NSO, the Israeli technology company focusing on cyber intelligence, which has been accused by WhatsApp of helping NSO's clients to break into phones via a spyware. But it would be important to understand certain legal aspects of such a reported breach.

A few questions arise. Has WhatsApp violated Indian laws? If yes, what are the applicable laws and what are the violations? And what are the penalties in Indian law for such violations? Further, from a public interest perspective, how do such legal provisions protect the public, and what are the remedies?

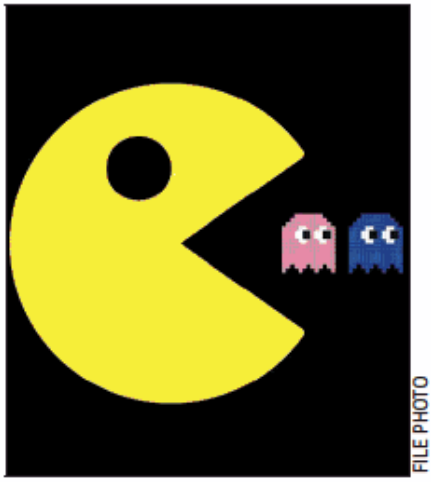
India's Information Technology (IT) Act, 2000 governs the reporting of data breach incidents, under which the government constituted the Indian Computer Emergency Response Team (CERT-In) as the nodal agency for cybersecurity. CERT-In Rules mandate service providers, intermediaries, data centres and body corporates (handling sensitive personal data) to report all cybersecurity incidents 'as early as possible'.

As to the reporting procedure, CERT-In prescribes separate forms for vulnerability and breach reporting. It appears from Cert-In's vulnerability note of May 17, 2019 relating to WhatsApp's reporting that the social messaging platform had reported a buffer overflow vulnerability that a remote attacker could exploit through a decoy WhatsApp call to target user phones and access information on the target systems.

The Cert-In report also reflects that the solution to patch the vulnerability was to upgrade to WhatsApp's latest version. Along with that, it provided web links to certain international online articles published a few days prior to the CERT-In report. These reported cases of exploitation of WhatsApp's vulnerability by attackers who had targeted a select number of users using NSO's Pegasus spyware.

Although it appears that WhatsApp has, prima facie, complied with its reporting obligations under the Cert-In rules, it is unclear whether the reporting was adequate and prompt. Further, Cert-In rules enable it to seek relevant information from any entity to carry out its functions. From the publicly available documents, it is unclear whether CERT-In had analysed WhatsApp's reporting, ascertained the inadequacy, and demanded additional information, despite rating the vulnerability severity as 'High' in its report.

While WhatsApp's compliance issue remains open now, and may be subjected to judicial analysis, one must understand the legal consequences. The law prescribes a penalty of ₹25,000 for non-reporting of a security incident, which is not even a trifle for large corporates. Further, one-year imprisonment and ₹100,000 fine is prescribed for not providing information called for by CERT-In. As regards imprisonment, there will be several open issues, specifically for companies operating in India from overseas jurisdictions without any people present in India. Similar issues are discussed in the traceability case before the Supreme Court.



FILE PHOTO

Careful now....

Further, from a public interest perspective, it is relevant to understand the key objectives of CERT-In. The purpose of reporting a cyber incident to CERT-In is to address and prevent data breach, and to develop security guidelines to prevent similar incidents in the future. The role of CERT-In and its objectives are critical. But it is unsure if CERT-In is reaching out to the general public other than through its website notifications. Additionally, we have not come across any provision or policy requiring CET-In to publish public notices alerting citizens about the vulnerabilities or breaches.

A larger concern that remains is about people affected by such cyberattacks. In the absence of any statutory provision to notify such persons and assess their loss, the reporting mechanism does not provide any direct benefits or remedies to them. Hopefully, the proposed privacy law containing notification requirements to the data subjects will bring some respite.

Millions of people use technology services like WhatsApp. However, it is impossible for the average user to understand cloud technology, never mind anticipate and detect such breaches, or protect themselves by adopting immediate remedial measures against cyberattacks. Considering the vast use of technology for personal, professional and financial transactions, the public must be immediately notified regarding such breaches, irrespective of whether all are personally affected or not.

Hopefully, GoI will introduce provisions for public notification of cyber and data security breaches to help citizens stay informed and protected.

The writers are lawyers at ANA Law Group, Mumbai