Data deprivation makes cybercrime difficult to tackle

Author: Rameesh Kailasam & Priyanka Mathur are, respectively, CEO and manager, policy, at indiatech.org

Another emerging casualty of such cybercrimes is the emerging 'start-up' ecosystem.

In recent times, there have been many instances of the hard-earned money of Indians being taken out of bank accounts and charges loaded onto credit cards through online frauds. As a nation making a huge transition to a cashless economy, public faith in the digital system needs to be consistently reinforced. All the players involved, including banks, telecom companies, financial service providers, technology platforms, social media platforms, e-commerce companies and the government, need to play a responsible role in ensuring innocent citizens do not undergo the trauma of suffering losses. The customer also has a responsibility to maintain basic cyber hygiene, which includes following practices and taking precautions to keep one's sensitive information organized, safe and secure.

Another emerging casualty of such cybercrimes is the emerging "start-up" ecosystem. We are beginning to see multiple cases where customers of genuine start-ups, unicorns and Indian businesses have been subjected to online fraud, and these customers initially presume that it is the customer care departments of the companies that have conned them, as we see in many of the cases that get filed. This is a dangerous trend. Not only does it shake people's faith in digital systems, the scepticism vis-a-vis online transactions also hurts the potential of emerging companies, tomorrow's successes which could help take India to the $5 trillion economy that the country aspires to.

Let us look at the modus operandi of some of the recent internet-based financial frauds affecting companies in the digital and e-commerce space. Fraudsters usually start by creating various websites or accounts on social-media platforms that host some content to make them look deceptively similar to the authentic companies' websites or social media interfaces. Such websites and social media accounts list fake customer care numbers for the relevant brands. When a customer tries to search for a company name by using a search engine, the customer care numbers or email IDs that pop up as results (sometimes even the top search result, thanks to the bidding process for ad words in search engines) are often these fraudulent ones. It is easy to be taken in.

There could be worse to come. The customer, with little reason to suspect that the search result is not genuine, may end up calling such a fake number, and get entrapped by fraudsters into sharing his or her bank information (and sometimes even a one-time password), which enables the anonymous con artists to siphon off money from the customer's account. At times, these fraudsters send online links, asking customers to share their Unified Payments Interface details or other such information; in other cases, unsuspecting customers are asked to download screen mirroring apps, through which they take control of or gain access to information on mobile phones. Even the income tax department has not been spared, with people getting messages from a fraudulent source that masks itself as an income tax authority and sends a message asking them to claim tax refunds by sharing a link.

It is difficult to estimate the scale of the problem, as law enforcement agencies in different states are not fully equipped to understand and act upon complaints of such frauds. Also, some victims of fraud are too ashamed to admit that they have been conned, and often do not even tell their families. Yet, if the losses are large, the results can be devastating for fraud victims. While many cases aren't even reported, in cases that are, the investigations make little or no progress due to lack of access to data.

Despite multiple requests for data from Indian start-ups and unicorns that need action taken against online scammers, search engines and social media platforms have generally been unresponsive, taking cover under privacy principles or laws of the countries they are based in. Since most search engines and social media platforms have no “permanent establishment" in India, law enforcement agencies have hit a wall on data access for the purpose of solving cybercrimes. This has often raised calls for complete data localization, which could have been avoided had a collaborative mechanism for data access, based on agreed criteria, been put in place. The Srikrishna Commission recommended that data be stored in the country either directly or through mirror servers to serve law enforcement needs. The US Electronic Communications Privacy Act bars US-based service providers from disclosing electronic communications to law enforcement agencies of any country unless US legal requirements are met. The bilateral mechanism of the India-US Mutual Legal Assistance Treaty is a bit outdated and does not seem to work. The US Cloud (Clarifying Lawful Overseas Use of Data) Act, however, enables law enforcement authorities in India to request electronic content directly from US service providers under an executive agreement with the US government.

While privacy and data protection are necessary, and data localization may pose its own business challenges, India needs to work out a way to crack cyber frauds and crimes. For this, the country urgently needs a legally-backed framework for a collaborative trigger mechanism that would bind all parties and enable law enforcers to act quickly and safeguard Indian citizens and businesses from a fast-growing menace.