Data security and breach notification in India

Global, India | October 29 2018

Use the Lexology Navigator tool to compare the answers in this article with those from other jurisdictions.

Data security and breach notification

Security obligations

Are there specific security obligations that must be complied with?

Section 43A refers to 'reasonable security practices and procedures', which have been defined as reasonable security practices and procedures as determined by a law in force (of which there is none) or as agreed to by the parties and, in the absence of both, the rules framed by the government (ie, the Privacy Rules). Accordingly, the parties are free to decide on the security standards to be adopted.

The Privacy Rules do not prescribe a particular security standard (although this is was what the rules were meant to do). Instead, they suggest that the International Standards Organisation/International Electrotechnical Commission 27001 or a code prescribed by an industry association and approved by the government can be used. Thus far, the government has approved no codes.

The banking regulations on the other hand require banks to follow ISO/IEC 27001 and ISO/IEC 27002. Similarly, the securities exchange regulations require stock exchanges, depositories and clearing corporations to follow standards such as ISO 27001, ISO 27002, COBIT 5.

Breach notification

Are data owners/processors required to notify individuals in the event of a breach?

The IT Act or the Privacy Rules do not require data owners or processors to notify individuals in the event of a breach.

Are data owners/processors required to notify the regulator in the event of a breach?

There are two scenarios under which data breach notifications are required to be made to the regulators. First, the banking regulations require banks to intimate the RBI in case of any cyber security incident within two to six hours of the breach.

Second, there are certain rules relating to notification of breaches to the Computer Emergency Response Team (CERT). The law is unclear as to whether such notifications are mandatory. Past enquiries with the CERT have resulted in a view that such notifications are voluntary. However, the CERT has recently taken the stand that such notifications are mandatory.

Separately, certain regulations that provide a safe harbour from third-party liability for intermediaries require the intermediaries, as part of their due diligence obligations, to notify the CERT in case of security breaches. The definition of 'intermediary' is wide and includes telecoms, ISPs, network service providers, web hosts, search engines, online payment and auction sites and online marketplaces. However, in practice, such a requirement would be relevant only to those organisations that might be held liable for third-party content.

The data breach regulations define 'cybersecurity incident' to mean any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, and information without authorisation. There is a further definition through a description of various incidents that constitute cybersecurity incident:

- targeted scanning or probing of critical networks and systems;

- compromise of critical systems and information;
- unauthorised access to IT systems and data;
- defacement of website or intrusion onto a website and unauthorised changes(eg, inserting malicious code or links to external websites);
- malicious code attacks (eg, spreading viruses, worms, Trojan horses, botnets and spyware);
- attacks on servers (eg, database, mail and DNS) and network devices (eg, routers);
- identity theft, spoofing and phishing attacks;
- denial of service and distributed denial of service attacks;
- attacks on critical infrastructure, SCADA systems and wireless networks; and
- attacks on applications such as e-governance and e-commerce.

The above list includes not just breaches, but also cyberattacks which do not result in actual breaches.

Click here to view the full article.

Kochhar & Co - Stephen Mathias and Naqeeb Ahmed Kazia