Guidance required for cyberspace security

By Priti Suri and Ashutosh Chandola PSA, Legal Counsellors

PSA
Legal Counsellors
14A & 14B Hansalaya, 15 Barakhamba Road
New Delhi 110001, India
Tel: +91 11 4350 0500
Fax: +91 11 4350 0502
www.psalegal.com
Email: p.suri@psalegal.com

Individuals and companies alike are becoming increasingly dependent upon the use of the internet for their daily activities. Cyberspace has become the standard means of communication and information transfer worldwide, with users ranging from people accessing social networking websites to companies using email to coordinate their global activities.

At the same time, there are few limitations on the accessibility of information in cyberspace, and this poses a serious threat to security. Incidences of corruption, theft of sensitive information and fraud in cyberspace have escalated in line with the immense increase in the ease of accessibility and volume of information exchanged online.

In India the protection and regulation of electronic information is governed under the Information Technology Act, 2000. The IT Act was recently amended by the Information Technology (Amendment) Act, 2008, notified on 5 February, which added new provisions for data protection and for enhancing cyber security throughout the country.

Section 2(1)(nb) of the IT Act defines "cyber security" as the protection of equipment, resources, communication devices and the information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. This definition also covers data protection in cyberspace.

Section 43 of the IT Act provides for compensation in the case of damage caused by a breach of cyber security. In other words, a person who breaches cyber security and thereby causes damage to another is liable to compensate the injured person. The term "damage" has been explained as destruction, deletion, modification or any kind of alteration of a computer resource (which includes a computer, computer system, network, data, database or software). The IT Act makes such a breach punishable as an offence, with penalties including imprisonment for up to three years, a fine of up to US$10,000 or both.

The amendment introduces section 43A, which requires companies handling "sensitive personal information" of individuals to maintain "reasonable security practices and procedures" to protect the information. Failure to meet these requirements makes such companies liable to compensate a person who suffers wrongful loss as a consequence of the company's breach of its security obligations.

Though the term "sensitive personal information" has not yet been defined, the tenor of the IT Act indicates that such information is likely to include medical records, contact information, bank account details, employee records and customer records (such as the customer records held by a bank or insurance company).

Another protective feature is set out in section 70B of the IT Act, which provides for the establishment of the Indian Computer Emergency Response Team (CERT-IN) to act as the national agency for incident response. The CERT-IN was established by the Department of Information Technology on 19 January 2004, and issues safety and security guidelines and alerts for the industry and the general public. Presently, CERT-IN is the only agency enabled to deal with computer-related incidents under the IT Act.

Despite the changes brought about by the IT Amendment Act and the penal provisions of the IT Act, there are still several practical gaps in relation to data security in India. For example, while section 43A requires a person handling sensitive information to safeguard it adequately, this is rendered ineffective by a lack of government guidelines. Regulators need to realize this and take action to rectify it.

Similarly, although CERT-IN issues guidelines and alerts as to best practice and system-specific security guidelines, it lacks teeth because compliance is not mandatory. This absence of meaningful legal sanctions puts data protection at serious risk.

To date, only the Reserve Bank of India has specified operational methods (its Internet Banking in India Guidelines, designed to govern the administration of online banking transactions) which qualify as "reasonable security procedures or protocols" under section 43A. There is a clear need for the government to suggest and outline the procedures and protocols that should be implemented by those who handle sensitive data in the IT-enabled services sector.

In addition to these shortcomings, there are certain factors affecting cyber security which the IT Act does not address. These include the easy and almost unlimited access and transferability of information over the internet, and the anonymity which typically makes it difficult to identify individuals who access or tamper with confidential information online. These factors underlie the main threats to data protection in cyberspace today.

Much remains to be done. While the IT Amendment Act represents progress, there is currently no effective implementation and so its objectives remain unfulfilled. There are still some prospects for improvement of the system. The Ministry of Information Technology has provided a few draft rules relating to blocking of websites and delegation of powers to the CERT-IN, and is in the process of drafting rules for the remaining changes introduced under the IT Amendment Act, which should be notified within the year.

Priti Suri is the proprietor of PSA where Ashutosh Chandola is an associate.