IT (Amendment) Act 2008 and its effect on the Indian enterprise

By Dhwani Pandya, Principal Correspondent
29 Oct 2009 | SearchSecurity.in

According to a recent Ministry of Communication & Information Technology news release, the Information Technology (Amendment) Act, 2008 has come into effect in India from October 27, 2009. The Act has received mixed responses. While some are happy about the Indian government's attempt to curtail usage of the internet for terrorist activities, others feel that the surveillance powers received by government are prone to misuse.

The Information Technology (Amendment) 2008 Act has been debated since it was passed by the Indian Parliament in December 2008, about a month after the terrorist attacks in Mumbai. Certain sections like Section 69 which provides authority to the Indian government for interception, monitoring, decryption and blocking electronic data traffic have come under major criticism. "The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state," says Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India.

Vivek Kathpalia, the partner at Nishith Desai Associates observes that though the earlier IT Act provided the government with statutory powers to intercept information, it did not provide the power to monitor and decrypt digital information. Now it has the ability to monitor and seek decryption of communication over computer networks (such as email and IP telephony). The new IT Act empowers the Indian government to intercept, monitor and decrypt computer systems, resources and communication devices. This means that the government will be able to conduct surveillance on corporate networks and email systems.

According to Duggal, the new IT Act does not include sufficient checks and balances to prevent misuse of information. This raises corporate espionage and information leakage concerns.

While Kathpalia believes that the new IT Act provides good requirements from a national security perspective, information access misuse by unscrupulous parties may prove to be dangerous for enterprises (as well as individuals). "The government needs to keep an eye on how the Act is implemented. The rules framed under this Act should be very clear. Individuals and corporate bodies should be approached only if the matter relates to national security requirements. The Indian government should also ensure that the information gathered by them is kept confidential," says Kathpalia.

The Indian Computer Emergency Response Team (CERT-In) will act as a national agency to address cyber security incidents. CERT-In will have powers to monitor, collect, analyze, and block information. Kathpalia feels that very strict rules are required to govern the functioning of this agency.

At the moment, there is much ambiguity about the available safeguards for an enterprise if it is subjected to interception and monitoring under the new IT act. On this front, Kathpalia clarifies that the IT act prescribes procedures and safeguards under for interception, decryption or monitoring. The IT Act also mentions that the government's appointed agency (which has not been identified at present – possible agencies include those such as the Police Departments' cyber cells and the Central Bureau of Investigation) should record reasons in writing and issue an order. "If a company suspects foul play after receiving the order, it can always challenge the order by approaching the court. In cases of insufficient reasons provided by the authority, it can also get a stay order from the court," says Kathpalia. If the agency finds incriminating evidence during investigation, it will require a magistrate's order to take possession of the computer assets under question.

Data privacy issues

The new IT Act mentions that if an enterprise is negligent in implementing a reasonable information security procedure, then it's liable to pay damages to the affected party.

Earlier, there was no clarity over data security and privacy issues in India, since this issue was not governed by any Act. Much ambiguity existed when it came to the obligations of an enterprise which handles sensitive personal data (like credit card or medical information). With the new IT Act, the government necessitates that corporate bodies protect all personal data and information they are possess, deal or handle in a computer resource under section 43 (A), informs Kathpalia.

The new IT Act mentions that if an enterprise is negligent in implementing a reasonable information security procedure, then it's liable to pay damages to the affected party. It also tries to explain reasonable security practices and procedures. According to the Act, reasonable security means procedures and practices designed to protect sensitive information from unauthorized access, modification and disclosure. The Act tries to explain the nature of sensitive data, informs Kathpalia.

However, Duggal feels that the new IT Act does not provide adequate legal mechanisms for data protection and privacy. "Data protection and privacy cannot be given adequate coverage under a single section. Hence we need to

have dedicated data protection laws like other nations," Duggal suggests. On this front, Kathpalia feels that enterprises will need more guidance on sensitive data and reasonable security practices within the organization.

The new IT act lacks coverage of areas like social networking, user generated content, spyware and malware. "Emerging cybercrimes and mobile crimes have not been appropriately addressed. The definition of sensitive and personal data has been left to the government," says Duggal.

Yet another bone of contention in the new IT Act is the reduction in punishment tenures for cybercrime. Although the new IT Act rates cyber terrorism as a heinous offence punishable with life imprisonment, it is a cybercrime friendly legislation, claims Duggal. The IT Act has reduced its quantum of punishment and almost all cyber crimes are now bailable. "An offense such as online obscenity earlier received an imprisonment for five years. Now it has been reduced to a year," observes Duggal.

To sum it up, the new Indian IT Act tries to capture several aspects dealing with personal data privacy, Blackhat hacking and cyber terrorism. However, a strong and regulated implementation mechanism is required to mitigate possibilities of the Act's misuse.