December 10, 2015

Low Cyberattack Reporting Leaves India Vulnerable

From Bloomberg Law: Privacy & Data Security

By Amrit Dhillon

Dec. 4 — Over a year ago, a large Indian bank faced a major cybersecurity breach and was forced to replace 24 million credit cards. But news of this only trickled out to the public.

No one knew if the bank took remediation measures, leaving open the possibility that a breach might happen again. The Reserve Bank of India didn't reveal anything about the case or whether it had moved to changed the regulatory rules to help ensure that it wouldn't happen again.

Although the scale of the credit card breach may have been large, analysts told Bloomberg BNA that data breaches happen all of the time in India. But these cybersecurity incidents are rarely reported by companies to the regulatory authorities and news of the breaches rarely appear in the media, they said.

The lack of disclosure to regulators of breaches in India leaves companies with little incentive to improve security and consumers without any understanding of whether their data is safe, the analysts said.

Under-Reporting of Breaches

“If this kind of breach were reported, it would not only force other banks to follow suit” in making such incidents known “it would also result in the setting of new standards for others in the banking/financial services sector to follow,” Pavan Duggal, a New Delhi lawyer who specializes in cybersecurity law, said. “When cyber security is comprised and this is revealed, it puts pressure on the company or bank to fix the problem instead of hiding it.”

Duggal said that, under India's Information Technology Act—which was last updated in 2009 to include data security measures (209 Privacy Law Watch, 11/2/09)(8 PVLR 1574, 11/2/09)—there is no mandatory requirement for companies to generally report data breaches to privacy regulators or affected individuals.

Data security rules that took effect in April 2011 (88 Privacy Law Watch, 5/6/11)(10 PVLR 687, 5/9/11) haven't had a major impact on general notification. But a later rule does require reporting to India's Computer Emergency Response Team of certain kinds of cybersecurity intrusion data breaches.

All the Indian framework data protection statute says is that companies should report breaches, but there is no mechanism for reporting to regulators or monitoring what is reported and no penalty for failing to report, he noted.

Sivarama Krishnan, a partner for PricewaterhouseCoopers LLP Risk Advisory Services, said companies are wary of acting on security breaches. “They do not like to go to the police station to report a breach because they feel the police are not trained to deal with cybercrimes and because they don't want the news to get into the papers,” he said.

Duggal echoed the point. “We have a situation of gross under-reporting which is the norm. As a result, a false sense of complacency exists in the corporate India that everything is fine regarding the security of their businesses and their data,” he said.

Mukul Shrivastava, a partner in Ernst & Young's Fraud Investigation & Dispute Services division, said that nobody in the government or outside has a database of what is happening. “Most companies tend to suppress such information since they fear it could lead to a loss in valuation. However, if the information is public, other organizations would be in a position to protect themselves,” he said.

“Just like the Companies Act in India states that you have to report every fraud, you need a system in place where every cybercrime that happens gets reported to a

central agency," Shrivastava said.

The lack of intelligence sharing encourages attackers to try the same techniques to target other companies, he said.

Cyberattacks on Increase

There are no accurate figures available for corporate cyber-fraud. The only official statistics available are for small crimes reported by private individuals at police stations. 'Estimating cyber crimes in corporate India is a matter of approximation and guesswork,' says Krishnan.

In the absence of reporting, analysts and consulting companies conduct surveys to get an approximate idea of the level of cybercrime. A November survey report by PwC India said that previously developed nations were prime targets but Indian organizations have been barraged by attacks and are now on a par with other global companies at the receiving end of cyberattacks. PwC found that cybercrime more than doubled over the past year

Given that the financial services sector is the most at risk from security breaches and data theft, the Reserve Bank of India (RBI) mandates that banks report security breaches to the RBI. It has also created a platform where banks can share their experiences and expertise. Once a breach has happened, banks have to report their remediation measures to the RBI. However, neither the breach nor the remediation are made public.

The Securities Exchange Board of India (SEBI), the other primary financial regulatory body in India, has issued guidelines on cybersecurity for the stock exchanges.

"SEBI law does not provide for any specific disclosures to be made by an Indian listed company to the stock exchanges or SEBI for any cybersecurity breach," Shrivastava said. However, if a breach involves "material information" it must be disclosed to the stock exchanges, he said.

Since 2012, the National Association of Software and Services Companies has been asking the government to create the post of national cybersecurity coordinator, but the appointment of Gulshan Rai to that role only happened last March. The government has yet to set up the approved in principle National Cyber Coordination Centre to deal with cybercrime.

The Data Security Council of India has criticized the government for continuing to use software that lacks proper security safeguards and for having no proper legal framework to ensure security in software procurement. The lack of adequate information technology infrastructure to test and certify IT products is also alarming the group reported as there is a large amount of sensitive data is being transmitted among government departments.

Ransomware Threat

Cybercrime in the corporate world is growing, the analysts said, with the most common threats being malicious code, phishing, website intrusion, spam, network scanning and probing and malware propagation. Ransomware is another big issue, according to an April report by security company Symantec Corp.

Mumbai-based independent cybersecurity lawyer Prashant Mali said that digital extortion is on the rise with companies being held ransom after their data has been locked by hackers. “Ransomware is the biggest threat facing corporate India today. Some companies are under regular cyberattack and they have set aside huge ransom amounts without their books of account showing the figure,” he said. “They fear their business getting affected so they make budgetary provisions for international hackers,” Mali said.

Analysts said that information technology and business outsourcing companies in India that do work for U.S. companies are far ahead of the curve because they work according to global standards of security and data privacy and these standards are audited and monitored.

Although increasingly companies are implementing Internet usage and privacy policies and conducting Internet audits as part of their workforce plans, that is still the exception rather than the rule, the analysts said.

“This weakness is a function of the maturity curve at which Indian businesses stand. As they grow and become larger, formal structures will be put into place to deal with cybercrimes,” Nandkumar Saravade, chief executive officer of the Data Security Council of India, said.

Need for Legislation

Many analysts said that the only way India's cybersecurity preparedness will improve is if a law dealing specifically with cybersecurity is enacted. India has no dedicated law on cybersecurity.

Duggal said that companies operating in India need to be aware that Indian law has the unique concept of an "intermediary" under the Information Technology Act. Intermediaries are all legal entities who on behalf of another person receive, store or transmit any electronic records or provide any service with respect to that record.

"Since a large number of businesses provide networks to their employees" as well as to their "business partners, they qualify as intermediaries," Duggal said. As such, they must "exercise due diligence while discharging their obligations under the law," he said. "But most companies in India are in breach of the due diligence parameters," Duggal said.

Violation of the law can expose businesses and their top management to potential legal liability, both civil and criminal. "Further, the Indian IT law applies to any legal entity whose services are available or impact, computers, computer systems and computer networks, physically located in India. As such, American and foreign CEOs who are outsourcing some of the business operations to India must ensure that their business operations comply with Indian law," Duggal said.

Shrivastava agreed it is important for companies operating in India to use a "loose" definition of intermediary in the IT Act so that telecommunications service providers, Internet service providers, cyber-cafe operators and search engines are included.

"Given the wide definition, subsidiaries of foreign companies, while complying with other laws, should also comply with cyber law due diligence requirements as applicable in India under the IT Act," he said.

To contact the reporter on this story: Amrit Dhillon in New Delhi at correspondents@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com

LEGAL & BUSINESS

TAX & ACCOUNTING

ENVIRONMENT, HEALTH & SAFETY

HUMAN RESOURCES & PAYROLL

RELATED NEWS

Legal Mandates Fuel Cybersecurity Insurance Growth

General Data Protection Regulation, Safe Harbor Dominate EU Outlook

Slow Philippines Privacy Law Uptake Raises Concerns

Lack of Injury Dooms Michaels Breach Class Suit

Cybersecurity Insurance Explosion Poses Challenges

Application Developers Settle COPPA Violation Charges