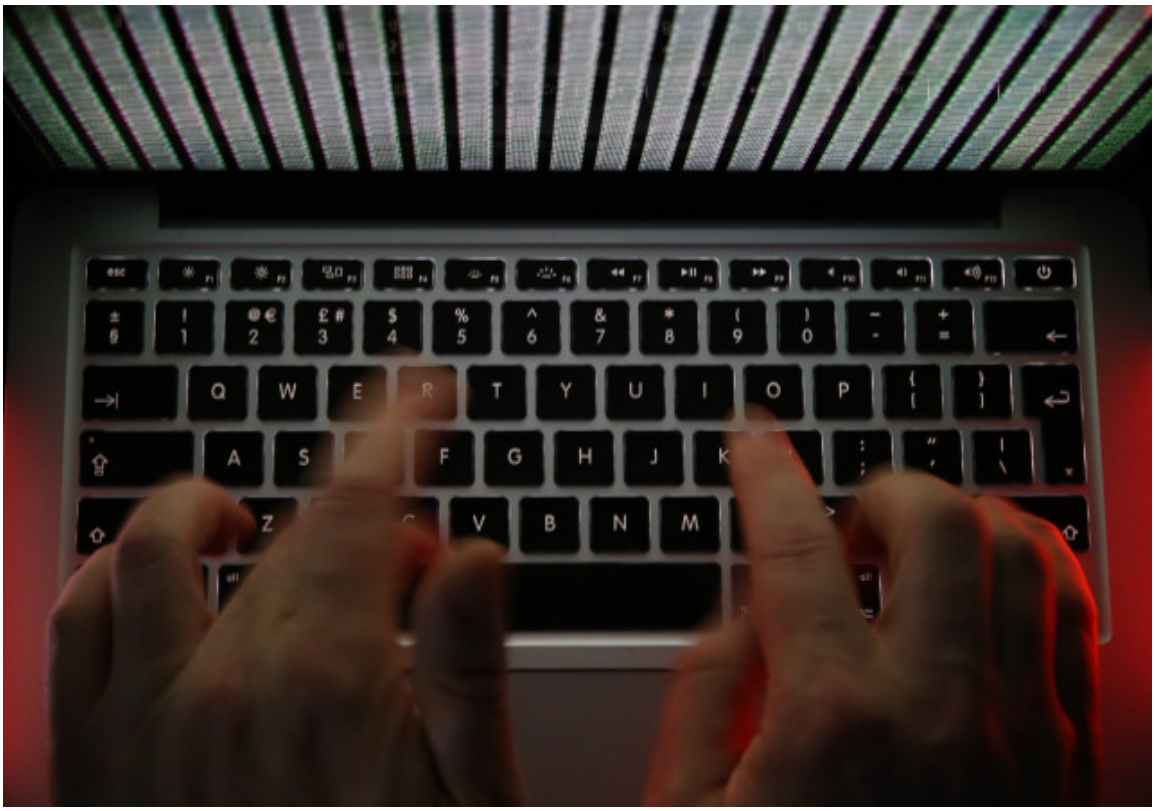

Photo by Chris Ratcliffe/Bloomberg

Global Law Firms May Have India Cybersecurity Chances

February 11, 2016

By Amrit Dhillon, Bloomberg BNA

Using lawyers to tackle cybersecurity issues, data breach response and cybercrime recourse is uncharted territory in India. The field is wide open, with only a handful of law firms specializing in cybersecurity cases for corporate clients, analysts told Bloomberg BNA.

Since there is no dedicated law in India to tackle cybercrime and no mandatory requirement that a company or institution that has faced a data breach must report it, the demand for law firms to handle such cases is feeble.

Currently, when companies suffer a data breach, they don't go to the police, much less consult a lawyer. Since the breach has already happened, their main aim is to identify and deal with the person — usually an insider — who hacked into their systems. For this purpose, they often hire private detectives or technical specialists to understand how the breach happened, identify the source and put in place mechanisms to stop any further attacks, the analysts said.

The need for a lawyer usually doesn't arise because the company has no intention of reporting the matter to the police for fear that the news will get out into the public domain, damaging its reputation and stock value. Even if they aren't concerned about embarrassing publicity, the fact remains that India offers little or no effective legal remedies for data breaches.

Since the law isn't an effective threat, it doesn't act as a deterrent. There hasn't been a single exemplary conviction for a cybercrime. "If we want companies to opt for the legal path, we need to give them effective legal remedies otherwise why should they bother taking legal action? We need more focused laws that are effective," New Delhi-based cybersecurity and Supreme Court attorney Pavan Duggal told Bloomberg BNA.

In-House Generalists

Most large corporations retain in-house counsel but these legal experts are generalists. When a cybersecurity breach takes place, these lawyers, not being specialists in technology, often engage the services of one of the few cybersecurity legal specialists in the country to handle the case.

In short, as an area of jurisprudence cybersecurity has barely taken the first few baby steps in India. The Indian National Bar Association has a Cyber Law & Security Committee comprised of a group of cybersecurity enthusiasts, but not much else is happening to develop the speciality.

The subject doesn't feature in the curriculum of Indian law schools. Even if they wished to specialize in the subject, law firms wouldn't be able to recruit the right people, analysts said.

Since there is no dedicated law in India to tackle cybercrime and no mandatory requirement that a company or institution that has faced a data breach must report it, the demand for law firms to handle such cases is feeble.

"Most lawyers trying to specialize in this field are commerce or arts graduates with a cyber law diploma," Prashant Mali, Cyber Security and Cyber Law Specialist in Mumbai, told Bloomberg BNA. "I prefer computer science or engineering graduates with law qualifications as they understand the client's issues better," he said.

Nonetheless, the few specialist cybersecurity legal firms that exist are beginning to send out tentative feelers to foreign law firms to explore possible professional ties.

For Sunil Abraham, executive director of the Centre for the Internet and Society in Bangalore, it is understandable that cybersecurity jurisprudence is embryonic. "As distinct from data protection jurisprudence, cybersecurity jurisprudence is every undeveloped, not just in India but elsewhere too," he said.

"Even if more corporations reported breaches and took legal action, it's not clear how jurisprudence will develop—the issues of jurisdiction, along with procedural incompatibility across jurisdictions, are complicated. So taking legal action doesn't necessarily mean that it will lead to the culprits being caught and punished," he said.

Potential Explosion of Representation Opportunities

There isn't at the moment a strong cybersecurity law environment in India and only a handful of qualified specialists in country. Nonetheless, the few specialist cybersecurity legal firms that exist are beginning to send out tentative feelers to foreign law firms to explore possible professional ties.

Analysts said the reason for these overtures is the conviction that legal work in cybersecurity is poised to explode in the next few years for three reasons.

First, the government is under pressure to introduce a standalone cybersecurity law. Cybercrime comes under the Information Technology Act and analysts said is both inadequate on its face to deal with the problem but is also hopelessly outdated since it was passed seven years ago.

Second, there is an expectation that mandatory reporting of cybersecurity breaches will expand as the government takes measures to protect the economy, businesses and critical infrastructure, which will create work for law firms.

At present, 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. Another regulator, the Securities Exchange Board of India (SEBI) which looks after the country's stock exchanges, requires an Indian listed company to report a breach if it involves "material information."

"We're poised at the threshold of a new phase. The government is actively considering making mandatory reporting a must in other sectors. It will happen first in certain selected, important sectors such as finance, insurance and medical data by around the end of the year. Once mandatory reporting comes in, it will open up huge vistas of work for law firms. Mandatory reporting will be the catalyst," said Duggal.

Third, breaches are expected to rise sharply. "As more and more Indians go online and as the government moves more of its transactions online as part of the Digital India campaign, the incentive for criminals increases because of the value of an attack goes up,' Abraham said.

Seeking Global Ties

The kind of law firms that are gradually moving into cybersecurity are those that were working on matters related to technology. But telecommunications lawyers haven't moved into the cybersecurity field, instead working on tariff and network issues.

Given the nascent state of cybersecurity law and the fact that India prohibits foreign law firms from practicing in the country, the potential for foreign law firms with expertise to establish ties with Indian lawyers is considerable.

Given the nascent state of cybersecurity law and the fact that India prohibits foreign law firms from practicing in the country, the potential for foreign law firms with expertise to establish ties with Indian lawyers is considerable.

"Because this field is so new, clients also feel comfortable knowing that the Indian firm they hired has enlisted the help of a foreign legal specialist," Duggal said.

Mali too says tie-ins with foreign law firms makes sense, but says such efforts are in the early stages. "There are some big international firms that have set up shop in India but they are here to support their international clients in India. A few leading international law firms have asked me for tie ups to handle cybersecurity work but we're still at the talks stage," he said.

Abraham said that "collaboration is already happening in cases where there are cross-jurisdictional concerns, say, for example, over trade secrets with Europe being stolen. Collaboration is a necessity when multiple jurisdictions are involved."

Even if more companies were to report cybersecurity breaches to the police and hire specialist lawyers to fight the case in court to convict the culprit, the state of the Indian legal system itself presents a huge difficulty. With an estimated backlog of 25-30 million cases winding their way through the courts, it can take 10-15 years to reach a verdict— hardly a deterrent for cybercriminals.

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