Date: 16.6.2016	**Publication**: The Times of India
Page number: 19	**Editions**: Delhi, Mumbai, Pune, Chennai, Kolkata, Chandigarh, Ahmedabad

India Inc scrambles to check cybercrime

Cos' Boards Fast-Track Preventive Security Measures, Buy Cyber Insurance Covers

Lubna.Kably@timesgroup.com

Mumbai: Boards of directors across India Inc are increasingly concerned about the growing menace of cybercrime. Loss of funds is just one facet, as theft of sensitive information is perceived to be more damaging in the long run.

In PwC-India's latest survey, 61% of the 480 respondents mentioned that boards were actively involved in cyber security issues, against a global average of 41% (*see graphic*). Several companies are putting in place holistic processes to mitigate cyber security threats and cyber liability insurance is gaining traction. "The uptake of insurance policies covering cybercrime was largely limited to the IT-ITeS sectors, or e-commerce companies. Now we are seeing an increase in demand from the manufacturing sector," says Tapan Singhel, MD & CEO, Bajaj Allianz General Insurance. Its cyber liability cover, introduced last year, has seen a gradual growth in demand of 25%.

Sanjay Datta, chief (underwriting and claims) at ICICI Lombard General Insurance, agrees. "With emergence of new threats such as ransomware (a malware which prevents users from accessing their system till a ransom is paid), companies across sectors, including banks, retailers and IT, are showing an interest in our new product — a cyber liability insurance cover (which also covers cyber extortion)," he says. Another product, crime insurance policy, has seen 30% growth in customer interest over the past few years. This policy covers internal and external crime, including fraudulent fund transfers.

While the premium payable is fact-based, typically for a Rs 25-crore cover, the industry norm is in the Rs 15-30 lakh range. But with only 200 'pure cybercrime' policies sold by general insurance companies, India Inc has a lot of catching up to do.

Companies are reluctant to share their own experiences and not all cybercrimes are reported as it could dent brand image, say experts. Jayant Saran, forensic partner at Deloitte-India, says, "In the past 18 months, we have seen companies incur losses ranging from Rs 10 lakh to Rs 150 crore. The last six months have shown a spike in external attacks, such as ransomware and phishing-based wire transfers."

The mechanics of cyber attacks are varied — malware enables cyber attackers to gain unauthorized access to a company's system and transfer funds. Others are more ingenious. In case of a large insurance company, the fraudster impersonated as a group CFO and passed on fund transfer instructions. "The impersonation attack had signatures of malware and a command-and-control to a remote location outside the country," says Atul Gupta, partner (cyber security), KPMG-India. Dhruv Phophalia, MD and head of Alvarez & Marsal's forensic practice, says, "Cyber theft resulted in a north India-based company losing sensitive information on critical operations and key business performance metrics."

Sivarama Krishnan, leader (cyber security) at PwC India, says, "Recently, we helped a marquee PSU respond to a defacement of over two dozen websites running on the same server, which were hacked primarily due to an exploit in an outdated application development framework (Drupal). This attack was politically motivated involving hackers from another country."

Access to a company's system via a multitude of platforms and evolving technological arsenal gives cyber criminals an added edge. Rather than plugging in loopholes post an attack, cyber security experts advocate having a holistic process in place as a preventive measure. KPMG recently launched 'Cyber-KARE' — a mobile app which enables a self-assessment of a company's cyber security to be carried out. The results are quantifiable and key potential actions are then recommended. "Cyber security is not purely an 'IT-issue'. A prevention strategy must focus not only on technology but also on improving processes and sensitizing users of the causes and consequences of cybercrime," says Krishnan.

Saran advocates awareness workshops, especially for senior management personnel who often end up as targets of attacks for ransomware.

Phophalia sums up, "A partnership between corporates and law enforcement agencies, that will help in disseminating information quickly on reported corporate cybercrime cases, will create awareness and will be useful."

GROWING PROBLEM

- PwC & KPMG recently surveyed more than 480 and 250 respondents respectively on cybercrime
- PwC found 61% of cos' boards have been actively involved in cyber security, and KPMG reported 41% actively discuss cyber threats as well as cyber defense strategies
- There is also keen interest in cyber security insurance with nearly 55% having purchased such policies or plan to in future, according to PwC
- About 44% said in PwC's survey that cyber attacks caused loss of customer records and almost 36% suffered financial losses, while KPMG found 63% suffered financial losses and 55% mentioned theft of sensitive info

GETTY IMAGES