THE HINDU BusinessLine

'Non-disclosure of attack could be a violation'

Raghavendra Rao K
Mumbai, October 20:

Non-disclosure by listed banks to stock exchanges about issues such as cyber attacks on their systems or their ATM networks being infected by malware could amount to violation of SEBI regulations on listing obligations and disclosure requirements, say experts.

"As per the SEBI Listing Regulations, a listed company has to ensure timely and accurate disclosure of all material events to stock exchanges. Specifically, in terms of Regulation 30 of the said Regulations, a listed company has to disclose to the stock exchanges all such material events as soon as reasonably possible and not later than 24 hours from the occurrence of event or later along with an explanation for delay," said Tejesh Chitlangi, Partner IC Legal.

Material event

"Any fraud/material wrong perpetuating on a mass scale with respect to a product of a listed company may qualify as a material event. A violation may lead to regulatory warning, imposition of fines or other penalties depending upon the gravity of non-compliance," he added.

According to Vidya Rajarao, Partner Grant Thornton India LLP, the level of attacks is a fairly serious issue. "Hackers usually go after targets that are critical in nature so that the impact is maximum as it affects movement of money in the economy," she said. "This being close to warfare it is very difficult to achieve prevention and could be state sponsored/ or a group of criminals. Technology and /law enforcement is usually behind the curve in catching these criminals, she added.

Consumers should be wary

Consumers should also take adequate safeguards while transacting online, says Mukul Shrivastava, Partner, Fraud Investigation & Dispute Services, EY India.

"While companies are doing their part, consumers can also take certain precautionary measures at an individual level to combat online fraud. For instance, they can avoid sharing any private factual information, especially on social networking sites, use unique passwords and change them at regular intervals to mitigate surging cases of identity thefts," he said. "We have seen that technology — though it can be a double-edged sword — can minimise cyber-attacks and security breaches to a large extent."

Rajarao sums up: "This is not a problem of technology but one related to humans. Companies need to constantly check their cyber resilience and readiness by doing mock drills/ ethical hacking instead of waiting for something like this to happen. On its part SEBI may enact a regulation which would require companies to disclose their cyber-readiness."

(This article was published on October 20, 2016)

MORE FROM BUSINESS LINE

Coming soon to your wallet: ₹2,000 notes

Mukesh Ambani has no fresh investment plans

How US elections impact Indian stock markets