SOURABH ISSAR
CHIEF EXECUTIVE OFFICER, CLOUDSEK INFORMATION SECURITY PVT LTD

Security

"A BREACH Directly AFFECTS The BRAND NAME"

Indian banks and enterprises are on a mission to strengthen their security systems against the ever-evolving cyber threats. Sourabh Issar, chief executive officer, CloudSek Information Security Pvt Ltd, tells Paromik Chakraborty of *Electronics For You* how digital risk management solutions ensure a safe online environment for businesses

Q. How vulnerable are banks and enterprises to cyber threats today?

A. In mature markets like the US, every breach costs a company around US$ 7.6 million. In India, we are reporting at least two to three vulnerabilities every day to our customer enterprises, each of which can turn out to be catastrophic.

Top private banks in India have matured perception and good readiness for cyber security. But the moment we go to tier 2 banks, some are doing well, while the rest have no idea about what they should do. They do not have a strong budget or strategy for security.

The hacker community is getting interested in the Indian financial sector because of the high amount of money being put into circulation. The truth is, everyone will get breached at some point of time. The most important differentiator between a secure company and an unaware one is how quick it is to detect a breach and respond to it.

The concerning matter is that, in India, there are a lot of local communities that are ready to buy what the hackers steal. Sensitive data like user account information of various websites, employee and agent details, and so on are available for sale on the dark Web. We even detect counter-deals for such data from India-based IP addresses.

Q. How critical is the situation?

A. The reality in India is that while B2C channels (like credit and debit cards, Aadhaar cards, etc) get breached the most, the real money is lost to hackers through B2B medium. The massive breach of Cosmos Bank is a big example.

The dark Web has many corrupt and untraceable sources with complete tutorials on how to hack an ATM, change locations and convert money into cryptocurrency.

While there is abundant information about the importance of cyber security in the informed media, the sense of importance is still low among the masses. Banks nowadays are aware about the possibility of breaches and are taking necessary actions. But each is at a different stage of maturity. A breach directly affects the brand name of a bank or an enterprise.

Q. How do digital risk management services improve business security?

A. Traditional digital security for banks included an antivirus and firewall setup. At present, it is essential for companies to know the loopholes in their networks, close these, and be able to detect and react to breaches quickly.

Digital risk management companies like CloudSek provide something more advanced than just making the firewall stronger. With due permissions from the clients, they help them assess their security posture in real time from the perspective of an attacker. They monitor the surface Web and the dark Web, and scour thousands of sources on the clients' behalf to detect cyber threats, data leaks, identity thefts and so on.

They let the clients know about impending risks, enabling them to take immediate action against these. Measures could include changing passwords, altering potentially-leaked data, if possible, and so on.

Q. What are the underlying technologies used by such solutions?

A. Machine learning algorithms and artificial intelligence (AI) coupled with big data handling capability enable the platforms to store and search multiple gigabytes of incremental data in minutes. AI enables the platforms to analyse millions of data within a few hours.

These platforms are capable of correlating clients' assets to threat data in less than three minutes, which would have taken at least a week to complete if done manually.

The platforms can also record 10GB to 15GB of raw incremental data every day.

Q. What legal regulations need to be followed in implementation of such solutions?

A. One should sign non-disclosure agreements and a contract of approval for the processes while getting into a deal. The primary intention should be to listen and observe on such forums on behalf of the customers.

Q. What subscription model does your solution offers?

A. Ours is a Software as a Service model, where customers can access the portal for one-time assessment of security breaches or continous monitoring of their assets. Charges are dependent on the scale of engagement. We calculate the scale based on the number of assets the client needs monitored. Assets can be anything from IP addresses and domain names to keywords. EFY