THE ECONOMIC TIMES

You are here: ET Home › Industry › Banking/Finance › Banking

Search for News, Stock Quotes & NAV's

Security breach: Time to build a strong security matrix

By *Pratik Bhakta* & *Saloni Shukla*, ET Bureau | Updated: Oct 26, 2016, 01.04 AM IST

Post a Comment

What keeps the chief executive of the world's most valuable lender JPMorgan Chase Jamie Dimon awake at nights is not a blow up in trading books, regulatory nightmares or shrinking bond markets, but cyber crimes that are becoming as routine an affair as daily trading. The US bank spends nearly $600 million a year on cyber security. Pose the same question to Indian banks, the top ones, including State Bank of India, ICICI Bank, HDFC Bank and Axis Bank, are not even willing to engage in conversations over the topic. Canara Bank is the only bank which replied saying that they have budgeted Rs 520 crore for IT security for the current financial year.

RELATED COMPANIES EXPAND

State Bank…

ICICI bank

HDFC bank

EXPAND TO VIEW ALL

Unlike the banks in the West, Indian lenders still do not appear to be sensitised to the threat from the cyber world, and their reactions to the possible theft of details of 3.2 million account holders in the biggest ever security attack reflect either their lack of seriousness or hesitation in admitting to the threat fearing dent to their reputation. Monetarily the damage from cyber attacks so far has been very limited, but it has the potential to get bigger and disrupt the nation's financial architecture and even result in the collapse of the system. Most of the crimes here have been aimed at disruption rather than to steal money on a large scale, unlike in cases like Bangladesh where $81 million was lost.

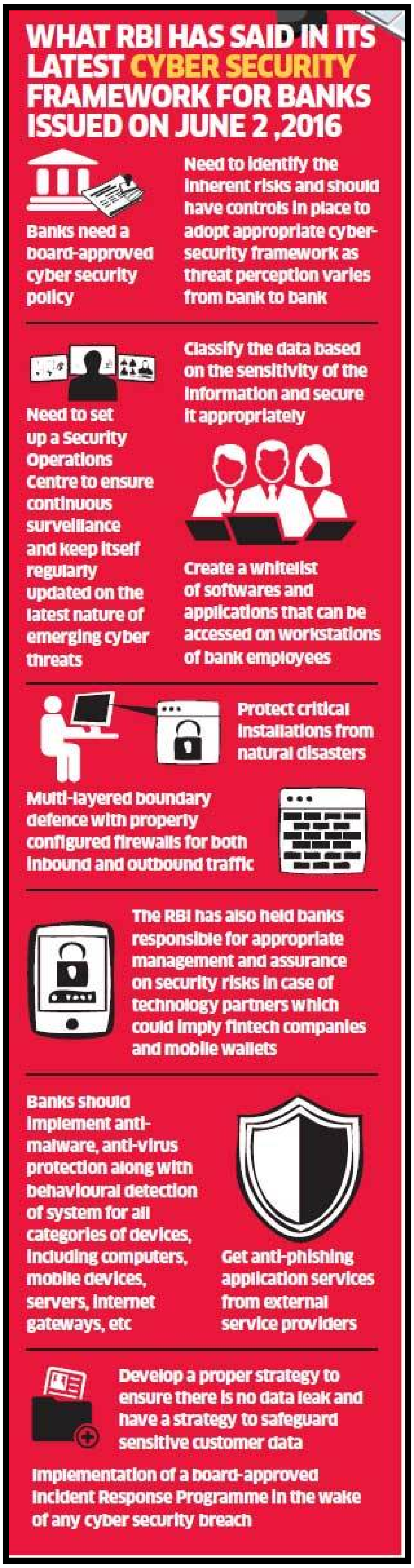
"Cyber crime is an issue that can actually bring down companies, and, at this point, banks need a more strategic approach in dealing with this," says Amit Jaju, executive director, fraud investigation and dispute services, Ernst & Young, India.

"It's important that they identify cyber crime as a key agenda for the board." Information from 19 banks were compromised with an estimated financial loss of Rs 1.3 crore in a mission that lasted for as long as six weeks before the banks woke up to the crime. While the regulator mandates that banks report any breach immediately, banks are reluctant to do so fearing damage to their reputation. The malware, reportedly introduced into the systems of Hitachi Payment Services, was lying undetected for weeks before consumer complaints exposed the technology deficiency of the banks and that of the service provider. No banker wanted to speak on record on this issue. Mails sent to many banks went unanswered. Police authorities that ET spoke with say that banks need to be more proactive in raising a red flag in such cases.

"Sometimes banks are responsive and sometimes they are not. I think banks need to be more proactive with these cases," said a senior police officer with Mumbai's cyber cell. "Banks don't report such incidents to us as they feel it harms their reputation. When we ask for information from the banks, they usually pass on the CCTV footage of the affected ATM." The recent spate of attacks that had happened on the banking system of Japan and Bangladesh had shown that India could have been the next target. In Japan, the hackers made away with around $13 million with credit card data stolen from a South African bank. A major card skimming act was also discovered in Bangladesh in February this year where media reports from the country pegged the affected numbers at six ATM booths and three banks. So, are we really facing a threat of such proportion? "To be able to track and detect such attacks beforehand, banks need their systems to be more intelligent to be able to do a diagnosis," says Atul Singh, regional director- banking, telecom and transport at Gemalto, a digital security firm.

"The bigger problem is this network of hackers and fraudsters is usually a global symposium and cards defrauded here have been found to be used in the US or China where they do not have a second factor of authentication." It is not just the technology installed in banks that would help detect such frauds, but the conduct of staff and internal policies and practices that are more important. In case of Bangladesh, for instance, the employees of the central bank were lured to visit certain websites and the moment an employee would visit a certain site, the malware would get downloaded into the bank's systems.

"Eighty per cent of the threats are coming from internal sources rather than external sources," says Manoj Kulkarni, managing director, Barclays Technology Centre, India. "The discussions that are happening internally is that how do we make our employees aware how to beef up internal securities. We are also figuring out the internal processes that how alarms are raised, how are they tracked and how they are dealt with." Indian banks are not the only ones exposed to cyber attacks, even the most sophisticated of the networks like the global payments messaging system SWIFT are also being attacked. With the interconnected nature of the industry, the financially weak state-run banks' ability to invest in technology is also being questioned.



WHAT RBI HAS SAID IN ITS LATEST CYBER SECURITY FRAMEWORK FOR BANKS ISSUED ON JUNE 2 ,2016

Banks need a board-approved cyber security policy

Need to identify the inherent risks and should have controls in place to adopt appropriate cyber-security framework as threat perception varies from bank to bank

Classify the data based on the sensitivity of the information and secure it appropriately

Need to set up a Security Operations Centre to ensure continuous surveillance and keep itself regularly updated on the latest nature of emerging cyber threats

Create a whitelist of softwares and applications that can be accessed on workstations of bank employees

Protect critical installations from natural disasters

Multi-layered boundary defence with properly configured firewalls for both inbound and outbound traffic

The RBI has also held banks responsible for appropriate management and assurance on security risks in case of technology partners which could imply fintech companies and mobile wallets

Banks should implement anti-malware, anti-virus protection along with behavioural detection of system for all categories of devices, including computers, mobile devices, servers, internet gateways, etc

Get anti-phishing application services from external service providers

Develop a proper strategy to ensure there is no data leak and have a strategy to safeguard sensitive customer data

Implementation of a board-approved Incident Response Programme in the wake of any cyber security breach

“Banks are already considering several cost reduction strategies to address cost pressures in managing non-performing assets and shrinking margins,” said consulting firm PwC in a report named RBI’s Circular on Cyber Security.

“In the wake of this, cyber security investment will not occur very easily. Banks will need to take a risk-based approach while building advanced capabilities. However, they may not be able to avoid baseline investments.” Regulator plays the most important role though in the wake of the recent fraud attack, it has only passed a statement instructing banks to adhere to its guidelines and review existing cyber security arrangements. In a country where banks are not willing to share even the list of defaulters to protect their own interests, to come out openly and share technology failures seems a distant dream. The RBI has issued guidelines for cyber security and it more or less covers all of it. What’s most important is how victims respond to such incidents.

In Europe, there is something called the Cyber Defence Alliance. This alliance ensures that there is information sharing among various banks because cyber security is an issue which is faced by all financial institutions. “Going forward, regulators need to continue focusing on enforcing policies and procedures and the top management of banks need to come together to battle cyber criminals,” says Jaju of Ernst & Young, India.

Live Market News Portfolio Mobile Live TV Newsletter Commodities Speed QnA Blogs Alerts RSS

Other Times Group news sites
Times of India | इकनॉमिक टाइम्स | ઈકોનોમિક ટાઈમ્સ | Mumbai Mirror
Times Now | Indiatimes

Living and entertainment
Timescity | iDiva | Zoom | Luxpresso | Gaana | Happytrips | Cricbuzz | Get Smartapp

Hot on the Web
Festival Guide 2016 | Gold Rate
Google expected to unveil Pixel smartphones | US Elections 2016
Live: India's surgical strikes on

Services
ads2book | Gadgetsnow | Free Business Listings
Simplymarry | Astrospeak | Timesjobs | Magicbricks | Zigwheels | Timesdeal | dineout | Filmipop | Remit2india | Gaana | Greetzap | Techradar | Alivear | Google Play