

# The Indian BANKER

THE MONTHLY JOURNAL PUBLISHED BY THE INDIAN BANKS' ASSOCIATION

**Financing Micro and Small Enterprises**

Page 22

**Bank Credit Portfolio Composition**

Page 30

**Data Security and Privacy in Banks**

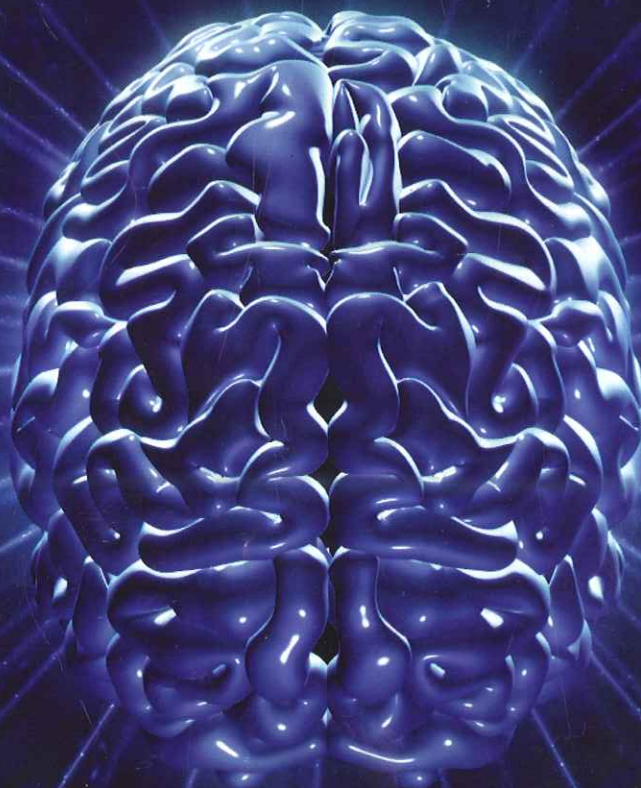
Page 34

**Various Risks in Banking**

Page 48

## Information Overload

How To Deal With It?



Indian Banks' Association



# Data Security and Privacy in Banks

## Challenges and Solutions

**B Venkateswaran**

With the advent of dynamic technological transformation in each and every field of operation, the resultant fruits of technology have been reaped by all segments of the economy and the banking sector is no exception to this. In fact, the banking sector has been one of the major beneficiaries although in some cases it was also an adventurous one. While banks in India, particularly the new generation private sector banks, have been at the forefront of seizing the advanced technological tools at an aggressive rate of knots to improve the quality of deliverables to their clientele-base, to keep pace with some of the international banks, the old private sector banks and the state owned banks had to follow suit to retain their market share lest they would befall as non-competitors and lose their preeminence in resources mobilisation and credit delivery.

Today banks need to improve their business performance management (BPM) techniques and business intelligence tools through performance accountability, process value enhancement, operational visibility, and compliance in global environment. To achieve this, banks need to redefine their core focus areas in the context of better customer delivery and reinvent themselves by optimum utilisation of their resources including human capital and technology.

### **Complex ecosystems of operations**

In view of the ever increasing cyber crimes being perpetrated on banks, it has become imperative for them to tighten their security systems in the context of huge and valuable database at their disposal; and to plug all possible loopholes to avoid pilferage, thefts and abuse by vested interests from both within and without.

Online banking channels are under threat of sophisticated and sustained attacks from malicious sources. According to annual figures released by the UK Cards Association,

'phishing' attacks in the UK rose by 16 percent in 2009, resulting in the total amount of online banking losses hitting £59.7 million, up 14 percent year-on-year. One particularly prevalent type of fraud that is responsible for these numbers is the so-called 'man-in-the-browser' attack. Following on from basic Trojans that existed for many years, online banking became susceptible to 'man-in-the-middle' attacks, where the hackers would place themselves between the customers' machines and those of their banks, intercepting and modifying online instructions from the customers for their own ends.

However banks were earlier able to tackle these frauds since the messages from the hacker came from an IP address different to the customer, making the fraud detectable. Unfortunately this is not the case with man-in-the-browser attacks. Here the Trojan embeds itself in an Internet browser application on the user's computer. When a user logs on to specific online banking sites, the Trojan is activated and intercepts and manipulates data as it is being communicated from the legitimate user's PC to an online banking system. All the while, this appears to be coming from the user's legitimate IP address.

While banks have vied with each other in implementing surveillance systems in their operations mostly through outside agencies over a period of a decade or so, very little thought has gone into the ominous area of data safety and security. As a result, this has become quite vulnerable and perhaps could be equated to a massive and latent time-bomb which may lead to a colossal financial catastrophe. HSBC Private Bank (Suisse) reported and apologized on March 11, 2010 for an incident in which a former IT employee stole account information for 15,000 Swiss-based accounts. Emerging threats to the database and a plethora of complex regulatory requirements for managing data are forcing organisations to rethink the way they secure their

structured data stores. With so many financially motivated attackers looking for easy paths to valuable data—and a growing panoply of vulnerable web-based applications connected to those databases—organisations can no longer set up a firewall around their data stores and call it a day. Data protection has to be strengthened from the inside out if we are to have any hope of properly mitigating these security risks.

## **Data protection systems (DPS)**

### *Basic issues*

There exist larger gaps in the data privacy and data protection management which arise due to:

1. Threats from insiders
2. Outsourcing of sensitive data to third parties
3. Not protecting customer data from all possible angles
4. Negligent and belligerent users

In most of the cases which have been reported in the recent past with regard to losses suffered by the consumers or the financial institutions, the role of insiders has been responsible for the calamity to a large extent. Bank managements obviously, do not have either time or inclination to monitor the behaviour pattern of the employees once they are absorbed. They take them for granted and repent only after an untoward incident takes place which, many a time, proves to be quite daunting. Irrespective of the cadre of the employees, it is essential that the management has an effective and preventive surveillance system in banks. Here data entrustment to the personnel of proven and undisputed integrity and frequently monitoring their functions is essential. Job rotation seen as an integral part of the HR policy is vital.

Sometimes proxy drills need to be enacted to test the vulnerability and susceptibility of the key employees to such ominous temptations. 'The basic idea behind a social engineering attack is that you can harden your IT systems to any conceivable degree and there will always be a weak point, which is that those IT systems need to interact with humans,' explains Tim Callan, vice president of product marketing for Mountain View, California-based VeriSign. 'If (hackers) can trick the humans into letting them in, it does not matter how strong the security system is.'

## **Outsourcing**

Similarly, while outsourcing jobs to outside agency, a comprehensive legal contract needs to be drafted and

signed by the banks taking into consideration the layers of people who would access such data at the other end and the resultant risks involved in this. It should be ensured that accountability on one or two key persons and penal clauses for breach are made specific and should serve as a deterrent.

Protection of clients' data including their identity, financial worth etc, is an integral part of the business responsibilities of banks and hence impermeable systems and devices should be in place at banks. Today when you open an account with a bank, the data gets captured by outside agencies and you start getting numerous telecalls from many service providers like credit card sellers, personal loan providers etc. It is an open secret that such data is collected and sold by such agencies to such users. Customers in India, being not quite aware of their rights to enjoy privacy, tolerate and sometimes silently suffer from such pernicious perpetrators. Banks need to consciously strengthen this area by suitable tools and systems.

## **Unholy nexus**

We also come across cases where the outsiders and consumers of banking services often operate with a malicious design of intruding into the space of other customers by just opening modest accounts and gain access and confidence of the bank often to the peril of the bank and its valued constituents. The banks quite often wake up only after the horses have left the stable. Here again a thorough study of the antecedents of prospective customers through KYC norms becomes imperative not only from the anti-money laundering point of view but also from the otherwise vulnerable and pernicious operations. Banks have to be constantly aware of the vulnerable areas like risks leading to data breach resulting in diminishing customer loyalty and trust.

## **Technology upgradation**

Over the years the banking industry maintained a near monopoly on safeguarding customer funds and facilitating transactions. This is now being challenged with industry convergence which has brought on new competition from other financial services entities and non-bank enterprises such as telecoms and software firms. To stem further erosion of their core businesses and navigate through a myriad of new regulations, banks are now finding themselves constrained by their old technology. These new non-bank entrants can rapidly adapt and offer customers the financial products and services that match their lifestyles. Banking industry's collective need for modern, agile systems has never been greater than now. Technology upgradation is required for agility necessary to respond more quickly not only to the evolving market conditions

and competition, but also to a rapidly changing regulatory landscape.

Quite a few surveys and research done internationally amply demonstrate that the senior management of banks do not sensitise themselves to the extent required to the safety and security issues, data theft, and impending cyber crimes. While funds are being generously released for installation of new systems and technology through budget and off-the budget, less or no provision of funds is consciously made for security of data and/or prevention of cyber crimes. It is in the interest of the banks to chalk out both short-term and long-term data protection plan.

### Credible client servicing

From the clients' point of view, more protective devices need to be put in place and relevant education extended to them to save them from the losses that they are vulnerable to due to their ignorance. With both retail and corporate customers expecting reliable 'anywhere, anytime, anyplace' access to their funds and financial information, a bank's operations are no longer contained within the confines of the traditional branch network.

And, with critical financial and identity data moving among multiple players who operate outside of the bank's own network, it is more important than ever to monitor and secure the flow of data.

### Solutions

The software systems used by banks are being reviewed, modified and improved from time to time by external agencies who are entrusted with such tasks and hence the data going into the hands of unscrupulous persons cannot be ruled out. Banks will have to do masking and sub-setting of data before handing over the assignment for development and testing. Sensitive and confidential personal information and business data need to be protected from piracy, especially when they are transferred across inter/intra offices by reliable persons. User access rights are to be periodically verified and documented for surveillance. Banks in the future may look to use 'multi band' authentication, requiring use of a secondary device (such as a smartphone) to confirm online banking transactions. One of the most successful and widespread security strategies developed to combat data theft is 'one time password' (OTP) technology. It adds on an extra layer of protection that can help stem the tide of fraud.

Data loss prevention of business records and that of customers are the prime focus of data security. The banks need to build customers' loyalty, trust and confidence not only in terms of their product brands but also their data

security concerns. They may be authorised to view and correct their personal information and have in place a redressal mechanism through mediation, arbitration etc. Helpline for customers to seek clarification and report abuse may be thought of. All employees may be gently monitored at random, through surveillance methods particularly new ones while they operate emails and inter-offices correspondence.

It is also suggested that banks take up security mechanisms such as 'whole disk encryption' to prevent consumer and business data on laptop and portable devices from being stolen or lost. It is therefore necessary for banks to secure their network and enterprise systems and test their sensitivity from time to time. While transacting records of information with outside business partners, extraordinary care and caution need to be exercised while drafting legal documents fixing the onus on them in case of any pilferage or leak or abuse of data by incorporating relevant covenant for malfeasance or misfeasance.

### Conclusion

The battle against payments fraud is as old as money. But while some of the latest efforts borrow from past scams, most of today's fraud schemes are as sophisticated as banks' most advanced payments systems. And stopping them is a real challenge. The top management of banks should assess the risk profile of security data for the bank as a whole and entrust the job to a senior level executive for effective control and monitoring. Martyn Jones, chairman, corporate governance services group, Deloitte, says, 'It is clear that financial institutions are investing more heavily in risk management, but some are struggling with the integration. The fundamental issue is around behavioural changes - without changes in attitudes and behaviour no framework will be truly effective.' Banks may jointly set up a research wing exclusively on 'cyber crimes' with the help of technical experts and police officers, to devise tools and processes to avert data and identity theft and financial fraud.

#### About the Author



**B Venkateswaran** is a professor in Rai Business School, Chennai. An experienced banker, Venkateswaran has served Bank of Baroda as chief faculty in its staff training college, and thereafter Lakshmi Vilas Bank Ltd as assistant general manager for 4 years. A science graduate with post graduation in management from Annamalai University, he has been a regular contributor for 'Business Standard', share market advisor at 'Sun TV-Sun News' channel, and was a member of editorial committee of IBA bulletin.