

# Banking Security Summit 2008



(L-R) Dr K Ramakrishnan, Dr A M Pedgaonkar, Sanjay Saxena, Vijay Mukhi

Indian Banks' Association (IBA) and Finsight Media jointly organised a full-day Banking Security Summit 2008 at Hotel Intercontinental The Grand, Mumbai on November 25, 2008.

The purpose of the summit was to deliberate on the key security concerns of the financial services industry today and to present strategies for countering these threats from fraudsters through improved processes, employee surveillance, customer education and implementing advanced technology-based solutions.

Introducing the agenda, Dr K Ramakrishnan, chief executive, IBA in his welcome address informed the audience that Security Summit is an annual feature. He observed that with the advent of technology supported alternate delivery channels such as ATM, debit and credit cards, online banking and mobile banking for increasing customer convenience and reducing delivery costs, the Indian banking has undergone transformation during the past decade. However, the same innovations have exposed banks and customers to the associated whole new lot of security risks. While banks were exposed to various security risks earlier too, the technology used today has amplified the security risk with increased convenience and speed of transaction. The fraudster had to forge documents and signatures for identity theft earlier, but today he

accomplishes the task just by knowledge of a password or PIN of a customer. He emphasised on the need for extensive training to bank staff which was feeling insecure consequent to automation, so that they are made fully aware of technology and security risks. He also touched upon the threat emerging from banks resorting to outsourcing as well as from heavy personnel turnover which results in a loss of direct supervision and control on various activities. He observed that 'as the centre of economic gravity shifts to Asia, we need to gear up our defences against these threats before they hit us hard'.

In his keynote address, Sanjay Saxena, additional commissioner of police, economic offences wing, crime branch, CID, Mumbai, stated that his view of security is from the victim's standpoint. 'In good old days there was a mutual recognition between bankers and their customers, which has now become either non-existent or reduced to very limited personal interaction owing to the alternate delivery channels,' observed Saxena. He informed that 'nine out of ten phishing attempts are targeting the financial sector.' Fear of identity theft is the main driver for slowdown in the use of Internet banking. He emphasised the need for 'strong user authentication' and commended the Internet banking guidelines issued by the Reserve Bank of India (RBI). As the existing Information Technology Act in India does not fully address data protection issue, he

suggested adoption of legislation prevailing in developed countries. He exhorted banks to become more customer-centric in cases of cyber frauds and credit card misuse and report such instances to police without fear of adverse impact on their market reputation. Customer education and public announcements forewarning people about frauds was necessary in case of frauds that might have affected a large number of customers. According to Saxena, mobile phones, particularly in light of SIM and handset identity, were strong authentication tools for online banking and their utility as such can be enhanced by banks getting consent from the mobile phone using customer to make use of location information from mobile service providers. While cautioning banks against compromising the process of know your customer (KYC), Saxena concluded his address by appreciating the initiatives of IBA in issuing KYC and anti-money laundering (AML) guidelines with a list of suspicious activities to be watched.

The special address on 'Ensuring Public Confidence: Customer Data Protection' was delivered by Dr A M Pedgaonkar, chief general manager, Department of Information Technology, RBI. He observed that banks and financial institutions store sensitive personal information such as names, credit card details and other accounts data which identify customer in their files. If such information falls into wrong hands, it can lead to frauds, identity theft or other similar harmful consequences, ultimately resulting in loss of customer's trust and many times, in banks defending a lawsuit. When any outsourcing agency is using such information or when the data transmission on network takes place, these institutions should take utmost care to maintain the confidentiality of the information. He informed laws in many countries provide utmost protection rights for such personal data of individuals recognising it as basic civil right and an extension of right to privacy. There are various laws enacted for the purpose of protecting personal data of individuals in those countries. Pedgaonkar further observed that security is as effective as the weakest link in a chain and said that in his opinion the weakest link in the financial sector does not relate to the components of technology (which do have an implication although), but to the person who is part of the information supply chain, and is typically the insider in the organisation. He therefore advocated the need for putting IT vendors, customers, network service providers, employees, maintenance and support staff and outsourced agencies in the chain under the security cover. 'A substantial portion of the breach of security in financial institutions has occurred on account of, or has been triggered with the aid of internal exposures or internal controls being compromised,' he added. Referring to some recent frauds in real-time gross settlement (RTGS), Dr Pedgaonkar delved in detail on the security requirements in case of electronic funds transfer, RTGS, and other payment mechanisms. He also provided a

comprehensive list of security standards that the banks and financial institutions can adopt. He concluded his address with the advice that 'public confidence and customer trust in the banks is a prerequisite for the stability and reputation of the banking system. Hence, banks need to ensure the preservation, protection, security and confidentiality of customer information in their custody or in possession of the service provider.'

Vijay Mukhi, president, Foundation for Information Security & Technology, began his talk on 'Getting Inside the Fraudster's Mind: Ethical Hacking' with four live demos showing the tricks and tools that hackers use for keylogging, stealing passwords, and gaining unauthorised entry into computer systems. 'These programs are available free on the Internet,' he informed the spellbound audience, and added 'there are thousands of such hacking tools available on Internet'. He emphasised that the hacker of today is not a techie. He also drew the attention of the audience to the fact that there has been negligible conviction under the IT Act, and re-emphasised that banks must report cyber fraud cases to police. During question-answer session it was suggested that such reporting could be made generic (bank's name may not be made public).

Nandkumar Saravade, general manager, ICICI Bank, initiating the pre-lunch session, spoke on 'Financial Crime Surveillance'. Thomas Varghese, vice president, product management, Oracle, made an excellent presentation on 'Identity Management Challenges'. Sameer Ratolikar, chief information security officer, Bank of India, spoke on 'Addressing People, Process and Technology for Secure Banking', while Ananth Padmanabha, head, strategic business, Datacraft India made a useful presentation on 'Security Imperatives for Compliance'. Apurva Pandya, sales director, India, PortWise delivered a talk on 'Identity Theft: Eliminating the Threat' while 'Is the Mobile Phone Really a Threat in the Security Value Chain?' was the topic covered by Laurent Filliat, vice president, strategic business, CIDWAY Security SA, Switzerland. Vishal Salvi, senior vice president and chief information security officer, HDFC Bank presented a detailed account of 'Risk-based Transactions Authorisation'. Pradeep Sekar, senior vice president and head, information security, Citibank made a presentation on 'Stronger User Authentication: Security Need of Alternate Channels'. Geoff Haydon, executive vice president - Asia Pacific, RSA, The Security Division of EMC, and Andrew Namboka, chief technologist, Asia Pacific, business mobility, Nokia also made presentations at the summit. In the concluding session Ravikiran Mankikar, president, ISACA Mumbai Chapter and general manager, Information Technology, Shamrao Vithal Co-operative Bank spoke on 'Role of HRM in Banking Security: Employee Risk'. Rema Menon, senior vice president, IBA presented a vote of thanks.