

Countering Online Frauds Through Secure Banking

PARTICIPANTS

Ajai Kumar
GM - IT, Bank of Baroda

Sudip Bandyopadhyay
Director and CEO, Reliance Money

P.A. Kalyansunder
GM - IT, Bank of India

B. R. Bhat
GM - IT, Corporation Bank

K.S. Harshan
Executive Director, Federal Bank

Sunil Dhaka
Head, ISG, ICICI Bank

B.R. Nath
CIO, State Bank of India

Murli Mohan
GM - IT, IDBI Bank

V. Subramanian,
CISO, IDBI Intech

P.R. Mutalik
AGM - Security, State Bank of India

Suresh Shanmugam
National Head-BITS, Mahindra Finance

Umesh Kumar Singh,
AGM - IT, Central Bank of India

Balkrishna Pipariya
GM - IT, Bank of Maharashtra

K. Unnikrishnan
Dy CEO, Indian Banks Association

Venkat Balan
Sr. VP and head, DBO, HDFC Bank

Kumar Saurav
Asst VP - IT, NCDEX

Ken Hunt
Founder Chairman and CEO,
Vasco Securities

Dan Dica
Regional Director - Asia-Pacific and
India, Vasco Securities

Manoj Kumar
Head, Financial Sector Sales - India
and Subcontinent, Vasco Securities

Venugopal Iyengar
Director, IOTM

Nitin Paranjape
CEO, MaxOffice



Participants at the roundtable

While Indian banks have deployed security systems with most exacting standards, the way Indian society works, the way Indian culture permeates, the purpose of security is defeated to a certain extent, says B.R. Nath, chief information officer, State Bank of India.

Participating in a roundtable discussion on 'Countering Online Frauds through Secure Banking' organized by Banking Frontiers in Mumbai, Nath pointed out that Indians generally lay much stress on mutual trust and 'what a person does is he just looks at how he is supposed to do the transactions and then carry it out without the least botheration.'

Nath told the participants: "I think what most of us lack today is in educating and driving our customers. Though we give them the kits, though we give them the forms, we intuitively make assumptions that most of these people will read and abide by them and adhere by them. But the reality is that most of them work on the basis of trust."

Citing the instance of PIN confidentiality, he said people tend to divulge it to others just based on mutual trust without realizing what the possible implications are. However, the internet banking is a different scenario, he said, adding: "In internet banking there are any

number of ways with which the fraudsters can lay their hands on passwords and transaction IDs. And it is a challenge to educate our own customers, what they are supposed to do and more importantly what they must not do."

He felt the most effective way to educate people is to make the educational material video-based. "The moment somebody sees how an inadvertent leakage of information can lead to personal monetary loss, it will immediately sink into his brain and will stay there for long that by just reading a list of dos and don'ts."

SECURITY TOKENS

Sudip Bandyopadhyay, director and CEO, Reliance Money, narrated the experience of his organization, where he claimed the issue was handled in a slightly different manner. Said he: "Customers are not interested in understanding the literature or going through the literature and following certain steps, because they work in different fields and their priorities are different. The entire business of Reliance Money is online. Customers can use our services offline but our systems, processes and backend function online and we have huge concern - hacking, phishing, pharming, etc. We actually scouted throughout the world for



Manoj Kumar Panicker

Ken Hunt

Dan Dica

a solution suitable for the people of India, majority of whom are not very technology savvy, and easier to adopt. What we did is, we picked up a unique security device. So when a person is accessing our portal or doing a transaction through our platform, he will have to have a login ID and a password and as an additional security layer, we introduced DigiPasses - security tokens. It's a two-factor authentication device which has got a six-digit number which changes dynamically every 32 seconds. Every customer of ours gets that security token which is small in size and easier to carry. So let's say somebody is trying to hack, somebody is trying to do any mischief. There is no way anyone can penetrate this security. In fact I must say with confidence that we are operating for last two and half years and there has not been a single incidence where security has been breached, very simply because of the security token. There is no link between our server and the tokens. It's an algorithm which is sitting in the server and sitting in the token which are matched for 5 years. So, the number which is randomly being generated, matches exactly to the number in the server and gives the customer access to the portal or any services."

Admitting that there has been lot of resistance, lot of questions and lot of discomfort that came in the way, Bandyopadhyay said today for Reliance Money customers, the token has just become a habit, the way a credit card or ATM card has become. "Yes, there are a lot of constraints, lot of problems, but you will have to keep on innovating ways. As we work in India, we have to work with Indian population, our core cultures."

Does he face any administration problems while adopting the tokens - like lost tokens or malfunctioning of the tokens? Bandyopadhyay said the whole process was structured in a manner that is convenient for the company and the customers. "We have a welcome kit for every customer, which contains a welcome

letter and the security token. There have been instances where the customer has forgotten to carry the token and he wanted to carry out certain transactions. So, we created some checks and balances and introduced a scheme whereby in some extreme cases the customer can contact the company's call center where the executives are trained to ask certain security-related questions to establish the identity of the customer and allow him or her to carry out the desired transaction. Through this process, one can only square up one's position and not take a fresh position. We are allowing you to exit your position and not create fresh positions. I must say that such instances were there only during our initial days and customers are very much used to the security tokens."

Bandyopadhyay also said Reliance Money had tested several systems including biometrics and found the security tokens to be most reliable and adaptable in Indian conditions. "Whatever you do, there is an electronic message which is going between the server and the device. We felt that there could be chances of interruption in the case of fingerprint verification so we consciously avoided that.

He also said cost was one consideration why Reliance Money adopted the security token.

IT CULTURE AS A GAP

Balkrishna Pipariya, general manager - IT, Bank of Maharashtra, felt that the Indian banking scenario is to a great extent different from what is prevailing abroad. "The biggest gap here," he said, "is the IT culture. Particularly in the banking industry which is almost 80% to 90% in the public sector, the employees are almost 50-55 plus. You can take the horse to the water but can't make him drink. That is the biggest bottleneck the Indian banks are going to face. Then there is the question of culture. Look at this scenario where there are employees who are suddenly having liberties to access anybody's account



Ajai Kumar

Nitin Paranjape

Manoj Agrawal



Umesh Kumar Singh

P.R. Mutalik

K.S. Harshan

through CBS, sitting in any branch. This is prone to frauds. Beyond that, there are serious issues with regard to business process re-engineering. In the earlier system there was a division between a clerk and an officer. Now, the load is more on the officers because everything needs authorization. This leads to vertical loading of jobs more on the clerical side. Now what could happen is an officer can allow a clerk to use his (officer's) password in order to get the work done. Such and other issues are needed to be discussed and resolved not only at the bank level but also at the industry level."

Pipariya said the need of the hour is to critically examine the systems, processes, business process re-engineering, IT culture, access controls and of course, the security issues involved in communications. Also there are issues like viruses, which takes weeks to even identify let alone find a solution. The intervening period is very critical. "All these emphasize the need for a strong IT culture so that you don't become a prey," he added.

He felt that as more than the vulnerability, one need to filter the size of the transactions. If a fraud takes place involving a demand draft issued from a branch which is connected to CBS to another bank there is no escaping the data process. "So, if a person passes a cheque or an instrument of a large value without complying with the systems and process then a whole lot of issues arise. In India we have good systems and processes but there is lack of compliance. I feel there should be filters for various levels of transactions. Another issue while considering implementation of security systems is vendor specifications. I feel IBA and RBI have a role here like setting up guidelines on outsourcing.

Speaking offline, B.R. Bhat said: "The primary implication of occurrence of online frauds on the customers is that they lose the faith in the system and would also tend to desist from using such facilities again on account of the fear of having affected once. But the important factor to be borne in mind is that

in many instances, online frauds would have resulted on account of the negligence of the customers themselves more than on account of any systemic or infrastructure deficiencies. This entails that the attempts to improve awareness of the customers on such matters also need to be accorded focused attention which would help prevent the customers from being coerced or misused to be a facilitator of such frauds themselves. This is very significant since in many instances of phishing, vishing, password misuse etc, the customers themselves facilitate the fraudsters to carry out the frauds by furnishing / parting with critical and sensitive account related information."

IMPLEMENTATION PROCESS

Sunil Dhaka, head, Information Security Group, ICICI Bank, felt that security issues need to be looked at from a point of view of implementation. Said he: "Let us start with a premise that no security is fool-proof. Apart from security issues at the customer level, there are hackers, hijackers and other online criminals always on the prowl. Even the best of security can be compromised. So, what is really required is an adaptive form of implementing security controls. I mean you are not going to a vault costing Rs one million just to put in Rs 10. We need to be very careful with what we are protecting and how we are protecting. Are these the only security mechanisms?"

Dhaka said he is of the opinion that the cultural issues that are being talked about are just going to vanish. "We have people who have migrated to a world of IT. But, the generation that is coming now is one that is born into the world of IT. So, I see the gap closing very very soon."

He cautioned that online fraudsters today are capable of using methodologies whereby even a genuine website can be injected with a malware that is capable of weaning away an unsuspecting customer visiting the genuine website and fill in personal information, which can be sent across to another data server which can make this information available to fraudsters. "The gangs out there are all so well organized that they do trading with the information so captured. It is available for a price country wise, organization wise, etc. It's a whole lot of commerce going on there, that there are concepts like 24x7 support, et al. I mean it might seem like a joke but definitely the online crime is highly organized today and it is only going to become worse. One can look at Triple D security systems - security through Design, security through Development and

security through Deployment.”

2 FACTOR AUTHENTICATION & BEYOND

Dan Dica, regional director - Asia-Pacific and India, Vasco Securities, explained the concept of two-factor authentication and said based on feedback his company has from some 1,200 banks across the world, he would say that this is an effective security system. Said he: “Two-factor authentication has two main lines of defense ...first the online password and second the dynamic password that is generated every 32 seconds, which ensures the person that is authorized to access the website or online banking applications is the genuine person. Yes, you are right when you say the session can be compromised and there are modes like man-in-the-middle attacks. We see this in several countries, including India. But it depends on what you want to secure. So I will give you one example. Most of the banks worldwide that we work with set up thresholds where they can say well first of all we want everybody or maybe not everybody to log on with a one-time password. Second if I see a transaction through an unauthorized account or a new account or \$300 or Rs 300 or Rs 5000, I would ask for challenge response. That’s the second type of obligations. If it’s a private bank it may even insist on a transaction signature. So it’s all possible and it all happening every day with all the major banks who have implemented our security system.”

Ken Hunt, chairman and CEO, Vasco Securities, said as far as strategy is concerned, his company has been to treat its customers as its partners. As far as security solutions are concerned, he explained that the security token has multiple functions and it can sit on one’s cell phone, Blackberry system or a PDA. “Security has a broad definition; we are simply one of the solution providers in that broad definition. Another strategy is using our middleware, which can be integrated into many vendors’ products to provide strong authentication to their products,” he said.

Venugopal Iyengar, director, IOTM, said he agreed that it is necessary for one to be clear on what is needed to be protected first before looking at solutions. “People talk about identity, verifications, validation, authorization, authentication, etc. They are all different, in different forms. The second thing is whether one wants to have device-dependent tokens or device independent tokens. Today, we are

working on indigenous platforms, we are working on different handheld devices, we are working towards international standards. The challenges are therefore many - if you opt for device-dependent tokens the vulnerability is very well known and you can easily exploit it. If you adopt device-independent tokens then the vendor needs to supply different types of tokens to handle that through different type of servers, through different type of channels. I feel security is more of strategy, you should know what tool to use, how to use, when to use rather than looking at the specifics. It’s not the risk assessment of your process, it’s the risk assessment of the various entities that are involved to authenticate.”

He added: “Today we need to look at how the tokens are going to be implemented, how the thresholds of these token are going to be put in, how these need to be deployed, which are the applications you want to deploy and then which are the clients who are going to use these kinds of tokens. Regulators are serious about thinking, fixing on something which is universally known rather than what is best.”

INCLUSIVE, ADAPTIVE PRACTICES

K.S. Harshan, executive director, Federal Bank, agreed with Dhaka saying inclusive or adaptive practices in banks and for customers are fundamental. “Human beings are brilliant enough to bring out any devices. Ultimately the human community is inclusive or adaptive of these. Now, if you look back in the last five years, we have seen an information or automation overload in the Indian banking system. As a result, most of the existing tellers have become more or less redundant. Now we have another crop of young people coming in who are well versed in IT but not in banking processes. So these two are the disconnects we are now facing. With this the issue now is how to break up literates on both sides, which is very difficult. Coming to the consumer side, in my bank I have



Kumar Saurav

Sunik Dhaka

V. Subramanian



Balkrishna Pipariya

Murli Mohan

B.R. Nath

operations and net banking. I think the importance of data security and other aspects will be covered in that."

ALIENS TOO

P.A. Kalyansunder, general manager - IT, Bank of India, said the bank has a data center in India for its domestic customers and a data center in Singapore for its overseas operations. "For our online banking, we have already implemented token-based solutions. We are also looking at implementing multi-factor applications in India for our domestic

several segments of processes. I segment them first and take the top risk areas to implement a solution so that adaptability will be better. Howsoever, we are told not to cross the roads on a non-pedestrian crossing."

He added: "Going by geography, we need to have devices with bottom up. Reliance can afford and can have a top down token for everyone but for banks like me we need devices with bottom up. For example a consumer in Bastar, who has to travel 15 to 25 kms to reach a bank branch, how I am going to address his or her needs? So we need to go by geographical segments and create devices suitable to them so that they achieve secure banking. It's a tough call though. But that is what we should practice."

NATIVES & MIGRANTS

K. Unnikrishnan, deputy chief executive officer, Indian Banks Association, participating in the discussion, talked about natives and migrants in the banking system and said in India there is a combination of new generation banks, old generation banks and public sector banks. "In private sector banks both the customers and the staff are the natives of these organizations. We have public sector banks where we have large segment of migrants both within and the customers. So, any security implementation poses different challenges. Talking about security, Sudip mentioned that he has implemented security tokens for customers number three million, I do not know why banks have not tried it."

He felt that banks should really look at it - maybe for transactions beyond certain levels. "Since the public sector banks are into the online area now, this is the time for them to look at it. But anyway there is always a cost benefit or quotient. From IBA's point of view, we see our role as that of creating awareness among the bankers because our resources may not permit us to reach out to the customers to create awareness among them. We have brought out a manual on preventive vigilance aspects some time back. That was at a time when the banks were on a branch computer environment. We are in the process of revising that to take into account the CBS

customers. Having said this, I must say that for an organization like Reliance Money, which came into existence just recently, implementation of security systems like tokens is rather possible because the technology was available and more so the customers were natives as they are called. For organization like ours, which is more than 100 years old history, we have a legacy. In fact, when we talk about technology, people usually talk about natives and migrants but we also have to remember that we have aliens in India. That is why the challenge gets more complicated. In fact, apart from migrating from people to technology how do we take care of aliens? I think that is the biggest challenge."

Ajai Kumar, general manager - IT, Bank of Baroda, said the bank's experience has been that it needs to study issues of security not only from the bank's perspective but from the customers' perspective as well. "When public sector banks they took up technology, they opted for the best technology in the world. They also opted for internet banking. This was something which was neither known to the bankers nor the customers. In spite of the best of efforts by us to educate our customers, there have been instances where they have lost money to fraudsters."

REGULATORS

Kumar Saurav, assistant vice president - IT, NCDEX, describing himself as a native customer be it for a PSU bank or private bank, felt that while banks would have efficient security polices, a customer often end up noting down the password for each bank. "That means I am vulnerable at the end of the day. Be it the first level of password or be it the transaction password. There is another password called the profile password for one of the banks. So I end up having three passwords for doing my internet banking transactions. But how safe am I?"

He said: "At NCDEX, customers are provided with a secure trading platform but at the end of the day we function as regulators for the members even when we have a regulator of



Suresh Shanmugam

Sudip Bandyopadhyay

B.R. Bhat

our own - the FMC - and I need to provide a secure trading platform, However, I admit and confess that we don't face the experience of my members being an alien. They are new generation members who are much aware of the security side, they have good controls built in at their end. But what I find typically is no matter how strong controls you build in terms of technology, the biggest thing is your people and the processes. If you don't follow the process, the security breaches get to happen at any moment. No security controls that you build are 100% fool proof. But, yes we need to build in a strategy, be it the risk assessment approach that you adopt, and you need to see the proactive approach and the reaction approach."

RURAL PERSPECTIVE

How about rural customers? Suresh Shanmugam, national head - Business Information Technology Solutions, Mahindra Finance, which has a rural focus, gave his perception that the rural customers are not very anxious about security. "We do have 13 lakh customers. We did a survey recently and found that 80% of the customers are happy if we reduce the interest rates. But surely I believe that security is a major concern and the regulators have to be very strict about ensuring that financial service organizations have an efficient and effective security system in place. Besides, awareness should be created about security issues. We have introduced handheld devices and this has been welcomed by the rural people. However, I feel the regulatory system has to come into the picture and play a major role which will enable other things."

Murli Mohan, general manager - IT, IDBI Bank, talked about the cost aspect in implementing sound security systems. Said he: "As far as cost aspect is concerned, it depends on the experience of the bank. What is the kind of hits they are presently taking from these online frauds? Probably that will drive the decision as far as the cost is concerned. That is one aspect. The other aspect is who is driving this whole initiative? In some banks it is risk that is driving this initiative, in some banks it is IT which is driving the initiative and in some banks

probably the business drives the initiative. I feel risk takes the lead. Probably it would be little bit easier for the businesses to get approval as far as cost is concerned."

SERVICE MODEL

V. Subramanian, chief information security officer, IDBI Intech, talked on the concept of authentication as a service. He said in the banking sector the onus of security falls on the banks, and not on the customer. So any cost on the security is borne by the bank and with millions of customers, this itself acts as a kind of deterrent for the management to go ahead with some of the implementations which don't have clear proof of concept in the country as of now. He suggested that if vendors come up with authentication as a service, there could be good response as it will be opex and not capex. The vendors can consider having number of transactions done by a customer for the charge. He also felt that as of today there is no proof of implementation of 2-factor authentication and no experience or stories of people who have implemented it successfully.

MaxOffice CEO Nitin Paranjape pointed out a couple of tricks to enhance risk. He said that every browser can be opened in a 'no-add on' mode and this disables any keylogger. Another thing he pointed out is that most new laptops come with a TPM chip that stores cryptographic key. Both these security features are relatively unknown and can be leveraged for improved security. One the customer education front, Nitin recommended an incentivization scheme so that customers get a discount or pay lesser interest for people who change their password frequently.

After two hours of discussions and deliberations, the roundtable concluded and several participants said that they found the deliberations very useful and interesting. Some of the participants had participated in earlier discussions, and promised to keep coming for future roundtables in view of the value they derived from them.



K. Unnikrishnan

P.A. Kalyansunder