Measures taken by public sector banks to prevent the cyber crimes and measure the level of awareness of Bank Customers

Asst. Prof. Shreyas Dingankar IMED, Bharati Vidyapeeth University, Pune

Abstract:

"Are Banks Protected"

One hundred percent security isn't possible for anyone in this world. Banks are skeptical and are unavailable for certain risks like human risk where they're dealing with a lot of confidential data of the customers, the account opening procedures and the KYC norms which are part of the RBI. Those are the areas where banks need to improve upon. But as far as the technology and infrastructure are concerned, I think banks are fairly secure. They have double authentication after the August 2009 notification from the RBI, and they're also now initiating one-time bank passwords and IVR-based passwords. You get one-time passwords on your mobile phone, where you register, get an SMS and a password pin. As far as the banks are concerned

I think they're very well protected. The only thing is the human element which needs to be improved upon.

Objective:

Objective of the paper is to ask the user "**Are You Protected**" and also advice them the scale to check their protection level. There is a lack of knowledge on the subject, lack of responsibility on where this issue is because people don't want to accept their role in this security domain. Questions represented by the associates vary from those who are ready to very fundamental concepts, definitions, attributes, prevention and intellectual property when it comes to corporate and those related to practical applications.

Every person who uses internet or mobile services, as far as India is concerned. It's generally used for academia purposes, for educating the officers in IT security for the states of India. We educate auditors, the Bollywood industry and a lot of intellectual property that's being used. But there are a lot of risks which are associated with it. We have industries; we have chambers of commerce and so and on and so forth. As I said it's for everybody who uses technology because there are many definitions and explanations that are very confusing.

Top Cyber Risks to Banks

Human risk is a big problem for Indian financial institutions, says Mr. Vishwas Paradkar Deputy Manager SBI (2) and banks need to start proactively educating their employees and customers to prevent cyber threats from persisting. "Banks need to work on how to have affective customer awareness programs as far as cyber fraud and banking fraud are concerned".

- **Top Cyber Risks to Indian Banks**

The Basic Question Which I came up with was ***what do we see as the top cyber risks to Indian banks today?***

With the advances in IT, most banks in India have migrated to core banking firms and have moved transactions to payment cards, debit/credit and to electronic channels like ATM, Internet banking and mobile banking.

There was a study released by the Ministry of Finance in 2009 where only 340 companies were registered in India and the loss was around 15.6 cores. I'm sure this status only talk about the crime which is reported, and the crimes which aren't reported there's no data available as to how much financial loss was there.

Often in the press and media we find once or twice a month there are instances of banking fraud because of the lack of user awareness and security. A lot of the finances and funds are getting lost.

Also, IT governance from the bank perspective and the information security audit which a new amendment that's come into place which mandates that the audit has to be done annually and bi-annually for specific processes. The outsourcing job of bank operations, like KYC norms, has further documentation.

The human element is a big, big risk in Indian banks today because people are collecting and handling the information of customers - they are the biggest challenge. That's why I keep on saying human behaviour is the biggest risk in security, specifically in bank security. In a nutshell, the banks need to work on how to have affective customer awareness programs as far as cyber fraud and banking fraud are concerned in order to reduce this thing.

Instances of banking fraud are frequent and mostly underling causes after investigation were established as lack of user awareness and security. A lot of the finances and funds are getting lost. Also, IT governance from the bank perspective and the information security audit which a new amendment that's come into place which mandates that the audit has to be done annually and bi-annually for specific processes. The outsourcing job of bank operations, like KYC norms, has further documentation. The human element is a major risk in Indian banks today because people are collecting and handling the information of customers - they are the biggest challenge. That's why author feels that human behaviour is the biggest risk in security, specifically in bank security. In a nutshell, the banks need to work on how to have affective customer awareness programs as far as cyber fraud and banking fraud are concerned in order to reduce security threats due to lack of awareness.

- **Methodology:**

Checking the customer awareness level,

Data is collected from following Banks

STATUS OF INDIAN BANKS WEBSITES

In this paper I take five Indian banks and try to find out the security features using by the bank for online transactions. The data is collected by various reports from web, newspaper and media. For every security feature I have provide 5 points.

The banks are-

- State Bank of India (SBI)
- Punjab National Bank [PNB]
- Central Bank of India [CBI]
- Bank of Baroda [BOB]
- Allahabad Bank

POINT TABLE

Bank	PE	VKl	SSL	SMS	UAP	Total
SBI	5	5	5	3	0	18
PNB	5	5	5	3	0	18
CBI	5	5	5	3	0	18
BOB	4	4	5	2	1	12
AB	3	3	3	1	0	10

PE- Password Encryption, VK- Virtual Keyboard, SSL Secure Socket Layer, SMS- Short message service alerts, *UAP- User Awareness Program

How you will identify Threats of cyber crime to selected public sector banks?

a) Unauthorized access & Hacking:

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

b) By hacking web server taking control on another person's website called as web hijacking

c) Trojan Attack: The program that acts like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans.

d) Virus and Worm attack: A program that has capability to infect other programs and make copies of it and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms.

Findings on Cyber Fraud:

- The fraudsters have started sending mail which is more personal in customizing them and changing the value to the specifics.
- Financial frauds, the variation of financial frauds in terms of income tax refund and your phishing banking frauds are common, innovative ways we are getting the funds from the transfers of shares. A lot of financial fraud is coming. These are the new trends which are coming up.
- E-mail spoofing currently brings fraud because it looks deceptive, and people are being victimized by such fraud where a person intercepts the e-mail IDs of party A and B and then the transactions happen. A lot of financial fraud is out there in multiple variations. These are the new trends now.

• Most retail cyber frauds and electronic banking frauds would be of values less than Rs.1 core and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is recommended that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values.

• The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent fraud risk management group in the bank. The group should be adequately staffed and headed by a senior official of the bank, not below the rank of General Manager/DGM.

• Fraud review councils should be set up by the fraud risk management group with various business groups in the bank. The council should consist of the head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet at least every quarter to review fraud trends and preventive steps taken that are specific to that business function/group.

• Various fraud prevention practices need to be followed by banks. These include fraud vulnerability assessments(for business functions and also delivery channels), review of new products and processes, putting in place fraud loss limits, root cause analysis for actual fraud cases above Rs 10 lakhs, reviewing cases where a unique modus operandi is involved, ensuring adequate data/information security measures, following KYC and Know your employee/vendor procedures, ensuring adequate physical security, sharing of best practices of fraud prevention and creation of fraud awareness among staff and customers.

• No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process

needs to be analyzed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.

• Banks have started sharing negative/fraudulent list of accounts through CIBIL Detect. Banks should also start sharing the details of employees who have defrauded them so that they do not get hired by other banks/financial institutions.

• Quick fraud detection capability would enable a bank to reduce losses and also serve as a deterrent to fraudsters. Various important requirements recommended in this regard include setting up a transaction monitoring group within the fraud risk management group, alert generation and redressed mechanisms, dedicated e-mail id and phone number for reporting suspected frauds, mystery shopping and reviews.

• Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which alarms can be triggered. This unit needs to have the expertise to analyze transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitization for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques**.**

- Cyber crime can be recognized in two ways:

I. The Computer as a Target:-using a computer to attack other computers. Ex: Hacking, Virus/Worm attacks, DOS attack etc.

II. II. The computer as a weapon:-using a computer to commit real world crimes. Ex: Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc

- **Analysis:**

a) The Bank & General public has only a partial awareness on the cyber crimes and different types of cyber crimes for which they are susceptible. They know about compute virus and not on email address hacking. They don't take much attention to the protection of their password particularly younger children. They forget to "put-off" the option of "remember the password for future use" and end up in giving away their password for unscrupulous hands. The use of face-book, twitter and similar social sites are commonly observed. There is gross lack of knowledge on e-commerce and e-banking cyber crimes among most of the internet users.

b) The cyber police have not visited these centers even once in the present year.

c) Most of cyber centers have put internet virus protection packages

d) Except one centre all other nine centers out of sample of ten have login system adopted where the user has register his name, email address and personal details to use the internet, but some time they are bypassed to browse the internet only by entering name.

e) Most of the centers (eight out of ten) insist on personal identity to be entered into the register. Two centers don't allow any user without their identity card/ driving license /etc. for their address proof (original – not Xerox copy) and they keep the scanned copy for future use.

f) Most of the centers on general holidays, Saturday's, Sunday's and vacation holidays mostly adolescent children browsing and playing video games without any sort of control on them. They are sitting in congested cubicles, not monitored by the supervisors of centers may get into addiction to these games and driven away from their studies. There is always a chance that they may put their eyes into to objectionable and psychologically unhealthy sites are a very heartening fact observed by the researcher.

g) Adolescent children also seen using social sites and there is chance of they share the information not conducive for their age and healthy social upbringing. They give wrong date of births and register themselves into these sites and social networks.

- **Conclusion:**

The study conclude that though there is a partial awareness about the cyber crimes, there is a need of "plan of action" from government to educate the public completely about it and the onus rests on the government and enforcement agency to protect the public from such specialized crimes. The study conclude with an appreciation of the preventive measures and systems adopted by cyber centres but they need to continuously monitor that system adopted is unscrupulously followed round the clock in their centre to protect the society and his customers. The study concludes that children – the future of our country should be protected becoming victim to any type cyber addiction. They need to be monitored and guided so that their energy and precious age of learning is spent on education and career development rather than wasting time on games, social network and objectionable sites. They have to be guided to take the advantage of internet for their mental, intellectual and psychological growth and how to be away from the rest of the Cyber Ocean filled with crimes, terrorism, wild games and useless information and to learn to know the difference between good and bad.

Suggestion:

The researcher is confident after the preliminary survey and will be heading towards a longer research journey and would sincerely try to find the present level of the implementation of cyber laws in India and also try to find suitable

models for enforcement of cyber laws, prevention of cyber crimes and training requirement of enforcement authorities - through years of research which would be of help for government and all

other stake holders in the process and especially to the benefit of the society in creating fearless environment where they will have happy surfing, e-banking, e-shopping and e-mailing internet experiences for their lifetime

General Awareness Points:

- **What is the meaning of strong password**
- **What is the meaning of SMS alerts**
- **Don't access net banking account from cyber café or public computer.**

Use a single computer as far as possible.

- **Login net banking site by directly typing site name.**

- **Don't click any link, if that link takes you to login page, close the page, and start over. Bank or its representative never asks for password and username over telephone. Change the password after 6 months.**

- **Remember the id and password, don't write it anywhere. Don't give any of the personal information to any web site that does not use encryption or other secure methods to protect it. Don't share any information to any one regarding to account Install good antivirus programme on the system and regularly update the programme.**

➢ Reference Persons :

1. Prof. Dr Ashok Ranade Mentor And Guide, Bharati Vidyapeeth IMED, Pune
2. Prof. Santosh Bothe Guide, Bharati Vidyapeeth IMED, Pune
3. Prof. Sachin Ayarekar Guide, Bharati Vidyapeeth IMED,Pune
4. Susheel Chandra Bhatt Research Scholar, Computer Science department Kumaun University, Nainital, Uttarakhand, India
5. Durgesh Pant Prof. & Director, School of Computer Science & IT Uttarakhand Open University Dehradun Campus, Dehradun, Uttarakhand, India