A SCENARIO OF CYBER CRIME FOR THE PRIVATE BANKS IN NAVI MUMBAI AND PANVEL ZONE

PUSHPENDU P. RAKSHIT[a1] AND ANURAG SHRIVASTAVA[b]

[ab]Global Institute of Management

ABSTRACT

This study is on a recent threat that is considered now far more dangerous than earlier days. Cybercrime is defined by police as the use of any computer network for crime. The Home Office and the SOCA-led Cyber Threat Reduction Board (TRB) use a three-fold categorization, dividing e-crime into: a) 'pure' online crimes, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to enable further crime); b) 'existing' crimes that have been transformed in scale or form by their use of the internet. The growth of the internet has allowed these crimes to be carried out on an industrial scale; and c) use of the internet to facilitate drug dealing, people smuggling and many other 'traditional' types of crime. This broad definition could cover crimes that are facilitated through using the internet as a means of communication. We are concerned that the TRB (Threat Reduction Board) and the ACPO (The Association of Chief Police Officers) definitions could be problematic for law enforcement agencies as they risk referring to all crimes whose perpetrators use the internet to organize themselves as 'e-crime'. As defined "Cybercrime is a clear, present, and permanent danger. While it's a permanent condition, however, the actors, threats, and techniques are very dynamic." — Tom Ridge, CEO of Ridge Global and first secretary of the US Department of Homeland Security.

Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating furthercrimes comes within the ambit of cyber-crime. Cyber-crimes are computer related as well as computer generated crimes which are increasing day by day. Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. This broad definition could cover crimes that are facilitated through using the internet as a means of communication. We are concerned that the TRB (Threat Reduction Board)and the ACPO (The Association of Chief Police Officers)definitions could be problematic for law enforcement agencies as they risk referring to all crimes whose perpetrators use the internet to organize themselves as 'e-crime'.

KEYWORDS: Cyber Crime, Frauds, Phishing, Vishing, Detection, Preventions, Navi Mumbai, Banks, Cyber Cell

In the current scenario, India has witnessed a huge increase in Cyber crimes whether they pertain to Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking the data or system to commit crime.

The offences which take place on or using the medium of Internet are known as cybercrimes. These include a plethora of illegal activities. The term 'cybercrime' is an umbrella term under which many illegal activities may be grouped together. Because of the anonymous nature of Internet, there are many disturbing activities occurring in the cyberspace which may enable the perpetrators to indulge in various types of criminal activities which are called as cyber crimes. Thus, cybercrime means any unlawful act wherein the computer is either a tool [Cybercrimes which involve computer as a tool are usually modification of conventional crimes such as drug-trafficking, on-line gambling, financial fraud or forgery, cyber defamation, pornography, intellectual property crimes, cyber-stalking, spoofing etc.], or a target or both.

OBJECTIVES FOR THE STUDY

The objectives of this research work are to touch all the important facets of the cyber crimes in a comprehensive way and to achieve new insights into it.

1. To explore how cyber crimes are committed (e.g. credit cards, internet)?
2. To study many of the trends in which crimes are committed and who commits them and why?
3. To explore how much money is at stake, lost and recovered?
4. To analyze how can such crime be reduced – by prevention or punishment?
5. To explore cyber risks to banks and customers.

[1]**Corresponding author**

6. To study how banks can better protect themselves from fraudsters?
7. To examine that how security aspects and company policies positively affect customers' attitude regarding their use?
8. To provide a probable solutions to improve the operational effectiveness of cyber security techniques and to maximize recovery opportunities in case of cyber crimes.

- How well protected are the banks today from these cyber risks?
- 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 are 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 technology andinfrastructure are concerned, I think banks are fairly secure. They have double authentication after theAugust2009 notification from the RBI and they are also initiating one time bank password and IVR-based passwords. You get one time password on your mobile phone, where you register, get an SMS and a password pin. As far as the banks are concerned, I think they are very well protected. The only thing is the human element which needs to be improved upon.

RESEARCH METHODS – APPROACH

- Deductive Approach (Qualitative) testing theory through observation and data (Primary & secondary).
- Exploratory Study Purposive, (deliberate) self-selection sampling and area sampling.
- Longitudinal projects must be around 1 year in length.
- Collection of data In- depth personal interview at beginning with banks and cyber cell. questionnaire method.
- Delphi method / expert advise for probable solutions
- Self-completion diaries to track issues and dynamism in cyber space.

This study is doctrinal in nature. An attempt has been made to make an analysis of cyber crimes occurring at various private banks in Navi Mumbai and Panvel Zone. The study will be completed using a survey instrument. The research involved two parts of the study. The first part of the study involves the development of the questionnaire for cyber crimes and practices for the banks in Navi Mumbai and Panvel zone along with customer perspective for the same and second part of the study is to show the further enhancements security solutions to banks and customers.

PROBLEM FORMULATION

There has been no comprehensive study in the areas of the impact of cyber security issues in the banks of Navi Mumbai and Panvel zone, at best there has been a reference made to attacks with mitigation and prevention, general customer satisfaction for services and intrusion detection.

This year, three in four (77%) respondents to the US State of Cybercrime Survey detected a security event in the past 12 months, and more than a third (34%) said the number of security incidents detected increased over the previous year. So it's no surprise that more than 59% of respondents said\ that they were more concerned about cyber security threats this year thanin the past.

As it is understood that not much studies are conducted on the banks of Navi Mumbai, the need to do so arises in my research work. Security policies should include:

- Security Policy for general users
- Security Policy for banks
- Security Policy for network
- Security Policy for software
- Backup Policy
- Technological advancements in the banking sector

PROBABLE SOLUTIONS

- The IT Act, 2000 provides that the appropriate Government may, by notification in the official Gazette, declare any computer resource as protected system because these directly or indirectly affect the facility of critical information infrastructure. The term "critical information infrastructure" means the computer resource which has impact on national security, economy, public health or safety. Any person who is authorized by the appropriate government to access protected systems are called authorized users.

- If any person accesses or attempts to secure access to a protected system, it will be treated as contravention of provisions and he shall be punished with imprisonment for a term which may extend to 10 years and shall also be liable to fine. It is the duty of the Central Government to prescribe the information security practices and procedures for such protected system.

- The Framework Core defines standardized cyber security activities, desired outcomes, and applicable references that constitute sound cyber security. It is organized by five continuous functions:
- **Identify:** An understanding of how to manage cyber security risks to systems, assets, data, and capabilities.
- **Protect:** The controls and safeguards necessary to protect assets or deter cyber security threats.
- **Detect:** Continuous monitoring to provide proactive and real-time alerts of cyber security-related events.
- **Respond:** The policies and activities necessary for prompt responses to cyber security incidents.
- **Recover:** Business continuity plans to maintain resilience and recover capabilities after a Cyber-breach.

CONCLUSION

I close by saying that "Thieves are not born, but made out of opportunities."This quote precisely reflects the present environment identified with innovation, where it ischanging quickly. When controller thinks of preventive measures to ensure clients frominnovative frauds, either the natures turf changes itself or new engineering rises. This helpsculprits to discover new regions to commit the extortion.Cyber crime can be protected by SMS Alert facility, User Awareness Programs, PasswordEncryption, Virtual Keyboard, Secure Socket Layer, Short message service alerts.Further the study is going on to evaluate and explore other techniques and possibilities to control and prevent cyber related issues of banks. Thus the study reveals many of the ways to detect and counter cybercrimes in city.

REFERENCES

Internet crime report January 1, 2005 - December 31, 2005.

(http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf:) Internet Crime Complaint Centre.accessed on 06/09/2007.

Internet crime report January 1, 2006 - December 31, 2006.

(http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf:) The Internet Crime Complaint Center. accessed on 06/09/2007.

Arora K. (2003), 'Indian Banking: Managing Transformation through IT', IBA Bulletin, Volume 25(3), March, pp 134-38

An Investigation of Financial Fraud in Online Banking and Card Payment Systems in the UK and China by Yan Sun, Loughboroug University May 2010.

Adv B Gordon Computer Crime – An Introduction (2002) February Servamus 35.

Ahmad, Tabrez, New Begining of Cyberlaw in India (July 29, 2009). Available at SSRN.

After Websites, Anonymous India to Hit Streets Against Cyber Laws,By Manoj Kumar. International Business Times, June 9, 2012. [37]

AshishPande, Deviation and Prevention, 2006, p. 126.

An Explorative Study of Satisfaction Level of Cyber-Crime Victims with Respect to E-Services of BanksJournal of Internet Banking and Commerce, Vol. 17, No. 3, 2012

Dr.AtulBamrara ,Gajendra Singh Chouhan ,Mamta Bhatt. Bharti, Dr. Dalbir, Police and People – Role and Responsibilities, APH Publishing Corporation, New Delhi, 2006.

Bayley, David H., "Community Policing", SardarVallabhbhai Patel Memorial Lectures (1984-2004), SVP National Police Academy, Hyderabad, 2005.

Brynjolfsson Erik (1993) "The Productivity Paradox of Information Technology", Communication of ACM, Vol. 36(12),p.67-77.

Brynjolfsson, Erik, Hitt, Lorin (1996) "Paradox lost? Firm-level Evidence on the Returns to Information Systems Spending", Management Science, April, Vol.42 No.4, p.541-558.

Business Standard, Mumbai Police fall prey tocyber crime, Salary accounts with AXI bankhacked, Sanjay Jog & Krishna Pophale | Mumbai June 14, 2013.

Chopra V. K. (2006), 'IT and Business Process Re-Engineering', Indian Bankers – Special Issue on e-payments and Commerce, Volume 1(3), March.

Chakravarthy, S.K., "Social Acceptability of the Police", The Indian Police Journal, Vol. XXVI, No. 1, July-September, 1979, p.3.

Business Standard, Mumbai Police fall prey to cyber crime, Salary accounts with AXIS bank hacked, Sanjay Jog & Krishna Pophale | Mumbai June 14, 2013.

Bitcoin will do nicely -- the state of Russian cyber crime, Ian Barke, 2014, Betanews. [86]

Britain threatens Internet 'trolls' with two years in jail,Business Standard, London, October 19, 2014. [92]

Chopra V. K. (2006), 'IT and Business Process Re-Engineering', Indian Bankers Special Issue on e-payments and Commerce, Volume 1(3), March.

Chakravarthy, S.K., "Social Acceptability of the Police", The Indian Police Journal,Vol. XXVI, No. 1, July-September, 1979, p.3.

Christopher D Chen Computer Crime and the Computer Fraud and Abuse Act of 1986 (1990) Computer Law Journal Vol. X No. 1 79.

Choudhary, J.N., "Indian Police Leadership – Can it meet the Challenges of 21st Century", SVP National Police Academy Journal, Vol. 52: No. 2, July-December 2000.

"China blames US and India for Cyber Attacks", The Hindu, August 11, 2011, p. 20

"Cyberabad Police to Roll out Host of New Measures", Staff Reporter, The Hindu, January 02, 2009.