CYBERCRIME IN BANKING SECTOR

SUJA.P*

NIRMALA RAGHAVAN**

Abstract

Cyber crimes are committed using computer as a storage device, or as a target of the crime. As a storage device, computers can either store information that will assist in the execution of the crime and as a target, if the information that they contain is altered or retrieved in an unlawful way. The Perpetrators against banks can use several kinds of cyber-crimes namely, phishing, spoofing, identity theft, worms and trojan horses, spyware, search engines, blackmail etc., Cybercrimes can range from hacking to cyber terrorism. Cyber-related crimes, pose high risk to all vulnerable businesses which includes banks, insurance, communications/media, defense contractors, health care, technology, high-profile businesses, financial institutions and governments. The risks are probably higher in the banking sector as compared to the risks in other sectors. This paper is an attempt to provide an insight into the different types of cybercrime, challenges faced by the banking industry against cybercrime and measures undertaken by the various countries to combat cybercrime in the banking sector.

Keywords: cybercrime, cyberspace, cyber security, core banking, phishing, hacking, spoofing,

* Assistant Professor, S.D.N.B.Vaishnav College for Women, Chromepet, Chennai, Tamil Nadu

** Assistant Professor, Crescent Business School, B.S.Abdur Rahman University, Vandalur, Chennai, Tamil Nadu

Introduction

Cybercrime denotes intentional use of information technology by cyber terrorists for producing destructive and harmful effects to tangible and intangible property of others. Cyber crime is an international problem with no national boundaries (Jajjodia, 2008**).** There are several kinds of cyber-crimes committed against the banking sector namely, phishing, spoofing, identity theft, worms and trojan horses, spyware, search engines, Blackmail etc., cybercrimes can range from amateur hacking to terrorism (Madan Bhaisin 2007).

Bhasin, D. 2009, had studied the 3 basic categories of cybercrime a) cybercrime against person b) cybercrime against property c) cybercrime against the government According to a e-crime watch survey, conducted by the U.S. secret Service and the U.S. computer emergency, cyber-related crimes, pose high risk to all vulnerable businesses which includes banks, insurance, communications, defense contractors, health care, technology, high-profile businesses and financial institutions and governments. The risks are very much higher for the banking industry. Information technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, offering speedy, efficient, and time saving method of transactions (Madan Bhaisin 2007). Internet has emerged as a blessing for the present pace of life but at the same time also poses various threats to both customers and the financial institutions (Jajjodia, H.V. 2008).

There are several kinds of cyber-crimes namely, phishing, spoofing, identity theft, worms and trojan horses, spyware, search engines, blackmail etc., Many banks, financial institutions, investment houses, brokering firms etc. are being victimized and threatened by the cyber terrorists to pay extortion money to keep their sensitive information intact to avoid huge damages. And it had been reported that many institutions in US, Britain and Europe have secretly paid them to prevent huge meltdown (Jajjodia, H.V. 2008).

Level of Awareness in cybercrime among the Users and Public

It is imperative, that banks sector have to play key role in spreading awareness on cybercrime among public (Bhatt Durgesh Pant.S.C. 2011). Arpana and Chauhan, M. (2012) had investigated the awareness level among different respondents on the issue of cyber crime. The target respondent is comprised of 100 working I.T professionals. The results of chi-square analysis proved that there was no association between the respondents occupation and level of awareness. The study suggested an information security awareness training program to be organized to create an awareness among the public in order to maintain the equilibrium between usability, productivity and security.

Another study also emphasizing awareness of cybercrime in schools, universities, governments, and private organizations in the Middle East was conducted by Fadi Aloul (2010). The study had examined the security awareness among users in the Middle East. It was found that there was a high internet penetration growth rate in the Middle East and the limited security awareness among users which had provided an attractive target for cyber criminals. Similar study on public awareness of cybercrime was conducted by Dowland. S. et al.,(1999) which focused on the influence the media over individual views and perceptions of cybercrime. A survey was

conducted among 1175 respondents ranging from individuals and organization, to collect diverse opinions. It was found that the respondents do not perceive computer abuse as a problem which indicates that they either have an extremely lenient view of the activities or do not recognize the significance of IT in modern society. A study conducted by Singh. N. et al., (2010) had analyzed the adverse impact of cyber crime on the national interest of India. It was found that the most effective way of controlling cyber crimes, was to make people aware of different types of cyber crimes through several modes of mass media, as still it plays 43% part on awareness among masses.

Fafinski, S., et al., (2009) had focused on raising awareness on the issues that might help users to combat cybercrime. A survey commissioned by 'Get Safe Online' had found that 15% of people think that it was their own responsibility to protect themselves, 49% think it should be the responsibility of 'big business' and 11% think that it should be a government responsibility. It was suggested that anti-spyware and anti-malware software is the only remedy against the cyber threats identified. Another study, conducted by Bhatt Durgesh Pant.S.C. (2011), had suggested awareness programs through cyber security awareness initiatives among the citizens of South Africa. Similar study was conducted by Veerasamy.N. and Taute. (2009) which discussed the various security threats posed by cybercriminals and found that the users need to be sensitized on the techniques of combating cybercrime.

Alou, F.A., (2011) had examined the security awareness among users in the Middle East among the students and professionals in UAE. A study by Bhatt Durgesh Pant, S.C. (2011) had created a four dimensional cybercrime prevention model comprising of education, training and awareness (ETA) among the users. All banking customers do not use online facilities due to lack of awareness. Similar cybercrime prevention model was created by Imran.A. et al., (2010) which was based on the crime prevention theories and techniques.

CHALLENGES FACED BY BANKING SECTOR AGAINST CYBERCRIME

Through cyberspace, nation-states can perpetrate espionage; industrial spies can steal trade secrets; criminals can steal money; and militaries can disrupt command-and-control communications. Today all business activities including production, manufacturing, transportation, telecommunications is heavily dependent on the Internet. There is a drive in South Africa to integrate all its government services systems, such as home affairs, SARS (South African Revenue Service) and commercial banks. Since the users of cyberspace span across all the layers of the society, so does the cyber attacks and therefore a comprehensive and integrated approach is required for the security of the citizens of any country. (Wada,F. & Odulaja,G.O. 2012)

The growth of online banking has provide enhanced opportunities for perpetrators of cyber crime. Absence of specific law dealing with card-related crimes in Nigeria increased the cases of cybercrime. (Wada,F. & Odulaja,G.O. 2012). Similar study was conducted on the increase of cybercrime by Aboud.S.J (2011), who had investigated the increasing number of cybercrimes in Iraq . The results show that 45.5% of cybercrimes were committed by high school students; and 23.7% were committed by registered scholars. The higher percentage revealed that the law enforcement agencies must be established to safeguard organizations

and individuals. It was found that there was an urgent need for data ethics and ethical education programs among youth for all age groups.

CYBERCRIME SAFETY MECHANISM

Cyber Security Awareness Initiatives in South Africa (2011), had recognised the need for a cyber policy to prevent cybercrime. It was evident that though there are many techniques evolved to curb the criminal activities by cyber terrorists, still the problem persists in legal structure to curb cybercriminals (Wada,F. & Odulaja,G.O. (2012). This finding is supported by another study conducted by Lovet.G. (2009) who had brought to light the technical, juridical issues in combating cybercrime. He had concluded that there is no permanent solution that could eradicate cybercrime.

Another study by Bhatt Durgesh Pant.S.C. (2011) had focused on the cybercrime safety mechanism against cybercrime namely password encryption, virtual keyboard, secured socket layer (SSL), sms alerts, firewalls, digital signatures etc., Similar study had been done by Jajjodia.H.V. 2008 in his study, who had also examined the safety mechanism against cybercrime. A different study conducted by Mehta.S., & Singh.V., (2011), had compared the opinions of both genders and students in the field of Information technology . It was found that that all were equally interested in combating cyber crime.

Wada.F & Odulaja, G.O. (2012) had examined the impact of the information communication technology (ICT) revolution on business, industry and government in the light of the consequences of cybercrime. There is presently no law that is specific to cyber crime in Nigeria. whereas in India, the Information Technology Act, 2000 was enacted taking into consideration UNICITRAL model of Law on e- commerce 1996 (Jajjodia.H.V. 2008). Another study conducted by Nappinai, N.S. (2010) in her study had also focused on the ITA, 2008. Absence of effective provisions to combat cybercrime are avoidable loopholes, which can be rectified. Lack of user awareness and monitoring capability had encouraged the cybercriminals. International prosecution is time consuming, expensive and non-standardized process and varies for each country (Alaganandam.H. et al.,2005).

CONCLUSION

Public awareness of computer crime and abuse is a double-edged sword. On one side, adequate awareness about cybercrime is essential but on the other side, the same awareness may deter public from using the e-banking services. It is clear from the results that awareness of computer crime amongst the public is high and it can be suggested that the media has a significant role to play. The more the users of cyberspace are spread across the layers of the society, the increase would be the cyber attacks and therefore a comprehensive and effective cyber laws are imperative to combat cybercrime against the banking customers.

References

Arpana and Meenal Chauha, M. (2012), 'Awareness of cybercrime in Tricity', International Journal of Enterprise Computing and Business Systems, ISSN (Online) : 2230-8849 Http://www.ijecbs.com , vol . 2 issue 1 January 2012.

Alaganandam,H., Mittal,P., Singh,A., Fleizach.C., (2010), "Legal Policies and the future of cybercrime", Journal of International Commercial Law and Technology vol. 5, issue 1 (2010)

Aboud,S.J.(2011) " Combating the cybercrime: Practices in Indian Society", The Research Bulletin of Jordan ACM, Volume II (II).

Aloul.F.A., (2010) , "The need for effective information security awareness ", International Journal of intelligent computing research (IJICR), vol1, issue 3, june 2010.

Aloul.F.A., (2011), "Information Security Awareness in UAE: A Survey Paper ", Department of Computer Science & Engineering American University of Sharjah, United Arab Emirates, Special Issue of the International Journal of the Computer, the Internet and Management, vol. 19 no. 1, june, 2011

Bhaisin.M (2007), "Mitigating cyber threats to banking industry", Information Technology, the chartered accountant, pp 1618-1624

Bhasin,D. (2009) , 'The Bad Guys are a Step Ahead of the Good Guys', (SME WORLD-Technology), march.

Bhatt Durgesh Pant,S.C. (2011), "Study of Indian Banks Websites for Cyber Crime Safety Mechanism ", International Journal of Advanced Computer Science and Applications, Vol. 2, No.10, 2011 www.ijacsa.thesai.org

Cyber Security Awareness Initiatives in South Africa: A Synergy Approach, Special Issue of the International Journal of the Computer, the Internet and Management, Vol. 19 No. SP1, June, 2011

Dowland, S., Furnell,S.M., Illingworthl, H.M., and Reynolds,P.L., "Computer Crime and Abuse: A Survey of Public Attitudes and Awareness,''Computers & Security Vol.18, No.6, pp.715-726, 1999

Fafinski,S., Garlik, Minassian,N., Invenio, Research powerful stuff ,'UK Cybercrime report 2009'-,September 2009

Lovet,G. (2009), "Fighting cybercrime: Technical, Juridical and ethical challenges",Virus Bulletin Conference, Sept 2009

Imran,A., Jahankhani,H., Al-Nemrat,A.., Education in IT Security - Trends and Questions, "Proceedings of the 4th National Conference; INDIACom-2010, Computing For Nation Development, February 25 – 26, 2010, Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

Jajjodia,H.V. ' Cybercrime – overview and the measures', Articlesbase- Free articles directory, Aug 27, 2008.

Mehta.S., & Singh.V., , "An Overview of Cybercrime in Iraq" Special Issue of the International Journal of the Computer, the Internet and Management, Vol. 19 No. SP1, June, 2011

Mehta.S., & Singh.V (2012), "Combating the cybercrime: Practices in Indian society", International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 volume 3 issue 3 september 2012.

Nappinai, N.S., "Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends?

Singh,N., Jamwal,D., Sambyal, G.S., (2010), " Dark side of Cyber Crime in India: A Case Study, Proceedings of the 4th National Conference; INDIACom-2010 Computing For Nation

Development, February 25 – 26, 2010 Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

Veerasamy.N., & Taute,B. (2009) "An introduction to emerging threats and vulnerabilities to create user awareness", Council for Scientific and Industrial Research (CSIR)

Wada,F. & Odulaja,G.O. (2012) "Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories", African Journal of Computing & ICT Reference Format: vol 5. no. 1. pp 69-82. january, 2012 - ISSN 2006-1781

****