EXCELLENT PUBLISHERS

International Journal of Current Research and Academic Review

ISSN: 2347-3215 Volume-2 Number 2 (February-2014) pp.173-178

www.ijcrar.com

The effect of cybercrime on a Bank's finances

A.R. Raghavan[1] and Latha Parthiban[2*]

[1]Flat no 20, Door no 9, Prashanth Manor, Bajanai Koil Street,Vadapalani, Chennai – 600026
[2]Department of Computer Science, Pondicherry University community college, Lawspet, Pondicherry – 605008, India

***Corresponding author**

KEYWORDS

Cybercrime;
Banking Sector;
Financial Loss.

A B S T R A C T

The Information Communication Technology (ICT) has revolutionalized different aspects of human life and has made our lives simpler. It has been applied in different industries and has made business processes simpler by sorting, summarizing, coding, and customizing the processes. However, ICT has brought unintended consequences in form of different cybercrimes. Cybercrimes have affected different industries and banking sector is one of them which has witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, Denial of Service. The paper discusses the problem of cybercrime in the banking sector and its impact on the bank's finances. It assesses the cybercrime scenario and identifies the actors involved in the scenario. It also examines the different types of cybercrimes which plague the banking sector and the motives of the cyber criminals behind such acts. The financial loss in the banking sector is huge across the globe both in terms of combating the cyber-attacks and on development of systems, so that such attacks need to be prevented in the future.

Introduction to Cybercrime in Banking Sector

Until mid-1990s, banking sector in most parts of the world was simple and reliable; however since the advent of technology, the banking sector saw a paradigm shift in the phenomenon (Jaleshgari, 1999). Banks in order to enhance their customer base introduced many platforms through which transactions could be done without much effort (Vrancianu and Popa, 2010). These technologies enabled the customer to access their bank finances 24*7 and year around through, ATMs and Online banking procedures.

However, with the enhancement in technology, banking frauds have also increased likewise (Alaganandam et al, 2007). Cybercriminals are using different means to steal one's bank information and ultimately their money as well (Choo, 2011). The results of empirical study conducted by Anderson et al (2012) revealed that globally, the banks have incurred billions of dollars in losses; and provides details of cybercrimes conducted across the globe in banking sector due to direct and indirect losses, criminal revenue and indirect costs.

It is therefore, a collective consensus of banks and regulators to make policies and adopt measures in order to protect banking platforms from cyber threats (Anderson et al, 2012). A number of technical defence and control measures like increased real-time supervision on transactions have been undertaken by the banks, however, even today the problem persists (Premchaiswadi, Williams, and Premchaiswadi, 2009). The reason behind this is that the defence measures currently available with banks are often reactive, time consuming and available in public domain which can be accessed even by the cybercriminal who in turn adopts measures to combat from these defences. The attackers allocate their time in developing new means for cybercrime and also simultaneously work on finding the solutions to bridge these defence measures (Böhme and Moore, 2009).

One of the ways to mitigate the problem of cybercrimes in banking sector is to identify the factors related to banks that are generally targets of such cyber-attacks, and why some banks have never faced such a situation. According to the empirical study conducted by Moore and Clayton (2007), some banks are targeted more frequently than others, generally by a financial malware. Banks which are generally targets of cybercrimes suffer from various malware attacks in form of online phishing, keystroke-loggings malwares, identity theft, etc. Some of key factors which were identified in the study which reflects the pattern why some banks are targeted more than other include their size (market share), the number of clients, their authentication system is weak, their money transfer policies are not safe and the country in which these banks are located is also an important pre-requisite for the cyber criminals. Studies conducted recently concluded that some of the malware used to attack these banks are becoming more specific (Sherstobitoff, 2013; TrendMicro, 2013). However, more such researches will have to be conducted to conclude if indeed cyber criminals are selecting their target specific tools or not.

Problem Statement

Cybercrime is a growing threat in the virtual world because individuals and organizations are relying more on internet at an increasing rate. The use of internet and other technologies have enhanced the risk of attack from cyber criminals across the globe. With the number of incidents of theft, phishing, computer viruses, hacking, on the rise, there is a need to explore the cybercrime scenario.

Although, with the advent of technologies, the banking sector has been able to reach more customers however, it has also enhanced the risk for customers who often feel reluctant and insecure in opting for such services. There is a need for the banks to evaluate their current operating practices. In this paper, the researcher makes and attempt to study the cybercrime scenario and its impact on banking sector.

Literature Review

Cybercrime in Banking Sector

Cybercrime according to Douglas and Loader (2000) can be defined "computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties". In the banking sector, the cybercrimes which are committed using online technologies to illegally remove or transfer money to different account are tagged as banking frauds (Wall, 2001). The cybercrimes according to Wall (2001) can be categorized into four major categories i.e. cyber-deceptions, cyber-pornography, cyber-violence and cyber-trespass. The banking frauds are sub-categorized in cyber-deception which can be defines as an immoral activities including "stealing, credit card fraud, and intellectual property violations" (Anderson et al., 2012).

There are number of frauds or cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the frauds are executed with the ultimate goal of gaining access to user's bank account, steal funds and transfer it to some other bank account. In some cases the cyber criminals uses the banking credentials like PIN, password, certificates, etc. to access accounts and steal meager amount of money; whereas in other cases they may want to steal all the money and transfer the funds into mule accounts. Sometimes, the intention of cybercriminals is to just harm the image of the bank and therefore, they block the bank servers so that the clients are unable to access their accounts (Claessens et al., 2002; Hutchinson & Warren, 2003).

As a lot of vulnerabilities exist in the defense system of banking sector, thus there is a need to investigate the ways to increase awareness about the measures that can be undertaken to combat cybercrimes in the banking sector. However, not many studies in the past have been conducted in this area which would suggest ways to mitigate the risks and combat such crimes (Florêncio & Herley, 2011; McCullagh & Caelli, 2005).

In order to understand the fraud system in banking sector we will have to understand and describe the attackers and defenders in this environment. The next section therefore describes the different actors which are involved in cybercrimes.

Actors of Banking Fraud

The actors of banking fraud can be categorized into four main categories; malicious exploiters, money mules, victims, and security guardians. Each of these actors and their characteristics have been defined below individually.

Cyber Criminals

As per the OECD report (2007), these malicious exploiters can be categorized into five sub categories. ***Innovators*** (who seek to find security holes in the system to overcome protection measures adopted by the banks). ***Amateur*** (who are beginners in this area and their expertise is limited to computer skills, which is exploited by the cyber criminal). ***Insiders*** (who are working within the bank to leak out important information in order to take some kind of revenge). ***Copy cats*** (they are interested in recreating simple tasks). ***Criminals*** (highly organized and very knowledgeable who may use all the above mentioned stakeholders for their own profit).

Money Mules

As per the definition given by OECD report (2007), money mules are "*individuals recruited wittingly and often unwittingly by criminals, to facilitate illegal funds transfers from bank accounts*". According to the FBI (Federal Bureau of Investigation), these individuals engage in the money transfer activity in exchange of some percentage of that money. According to Florêncio and Herley (2010) there role is to "*convert reversible traceable transactions into irreversible untraceable ones*".

Victims

Victims, according to OECD (2007), in the banking sector can be categorized into two categories; banks and users of these banks. The users or customers can be individuals, SMEs, or large multinational organizations. The most negative externality among the legitimate actors is created by individual users and SMEs who do so by not employing risky online behavior or by not employing security measures during transactions (Asghari, 2010; Mannan & van Oorschot, 2008).

Security Guardians

They are the most important actor of this system as they improve the existing banking system and help in removing the vulnerabilities and development of systems so that banking frauds can be mitigated. The security guardians in case of banking sector could be the bank itself or the some third party hired by the bank in order to ensure security from such threats.

Impact of Cybercrime on Bank's Finances

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions. The banking sector is forced to evaluate its current practices in order to analyze and manage their risks effectively. Technology-driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in everyday life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services affordable and accessible (KPMG, 2011).

However, this has also increased the risk of becoming targets of cyber attacks. Cybercriminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the bank's finances. Globally, USD 114 Billion is lost nearly every year due to cybercrimes, and the cost spend to combat cybercrimes is double is amount i.e. USD 274 billion (Symantec Cyber Crime Report, 2012). On an average, banking facilities take 10 days to fully recover from a cyberact which further adds to the cost of operation. Comparing the financial losses faced by the Indian Banking Sector, it is nearly 3.5% of the loss in cash in comparison to global loss. USD 4 billion is lost in recovering from the crime and USD 3.6 billion is spent to combat such crimes from happening in future. The average time taken to resolve the crime in Indian banking sector is also higher in comparison to global scenario i.e. 15 days (Muthukumaran B., 2008).

In order to fight these cybercrimes, the banking sector needs to collaborate with global authorities and watchdog organisations so that a model can be developed which can help in controlling

and dealing with such threats. The main issue of concern here is that there is absence of effective compilation service in the banking sector which can identify the trends in cyber-crime and compile a model according to it. However, in the last few months, banks all across the globe have perceived cybercrime as among their top five risks (Stafford, 2013). High profile banks in the UK like Barclays and Santander were targeted by hackers who stole personal information of nearly 2.9 million credit card customers by hacking the software maker system of these banks, which led them to incur huge losses. However, the scenario is not restricted to UK, in US as well such attacks have surfaced in the past years and in order to curb the affect, they launched the program Quantum Dawn 2 which test the efficacy of system installed in banks in response to cyber-attacks (Stafford, 2013).

However, the sad truth is that most the systems are one-step behind the tools adopted by cyber criminals which has resulted in demand of development of system which is flexible is meeting and destroying the incoming assaults. A solid defense system to resolve attack is the need of the hour before, during and after the attack.

Conclusion

The paper gives a brief overview of cybercrime scenario in the banking sector and impact of cybercrimes on bank finances. The major cybercrimes which plague the banking sector are ATM frauds, Denial of Service, Credit Card frauds, phishing, etc. The rapid growth to global electronic crime and the complexity of its investigation requires a global presence. Presently, the measures undertaken the banks are not sufficient and therefore it is imperative to increase cooperation among the banks across the world for the development of tools and models which can be applied to counter global banking cybercrimes.

References

Alaganandam, H., Mittal, P., Singh, A., & Fleizach, C. 2007. Cybercriminal Activity.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. 2012. Measuring the cost of cybercrime.

Asghari, H. 2010. Botnet mitigation and the role of ISPs: A quantitative study into the role and incentives of Internet Service Providers in combating botnet propagation and activity. Delft University of Technology.

Böhme, R., & Moore, T. 2009. The Iterated Weakest Link--A Model of Adaptive Security Investment.

Choo, K.-K. R. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 308: 719-731.

Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. 2002. On the security of today's online electronic banking systems. *Computers & Security*, 213: 253-265.

Douglas, T., & Loader, B. D. 2000. *Cybercrime: Security and surveillance in the information age*: Routledge.

Florêncio, D., & Herley, C. 2010. *Phishing and money mules*. In Information Forensics and Security WIFS, IEEE International Workshop on pp. 1-5. IEEE.

Florêncio, D., & Herley, C. 2011. Where Do All The Attacks Go? *Economics of Information Security and Privacy III* pp. 13-33. Springer New York.

Hutchinson, D., & Warren, M. 2003. Security for internet banking: a framework. *Logistics Information Management*, 161: 64-73.

Jaleshgari, R. 1999. Document trading online. Information Week, 755: 136.

KPMG 2012 [Online] Cybercrimes: A Financial Sector Review. Government and Public Sector. Available at: https://www.kpmg.com/in/en/industry/publications/fs_cybercrime_booklet.pdf

Mannan, M., & van Oorschot, P. C. 2008. Security and usability: the gap in real-world online banking. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms.

McCullagh, A., & Caelli, W. 2005. Who goes there? Internet banking: A matter of risk and reward. Paper presented at the Information Security and Privacy.

Muthukumaran. B 2008. Cyber Crime Scenario in India, Criminal Investigation Department Review, pp.17-23

OECD. 2007. Malicious Software Malware: A Security Threat to the Internet Economy.

Premchaiswadi, N., Williams, J. G., & Premchaiswadi, W. 2009. A Study of an On-Line Credit Card Payment Processing and Fraud Prevention for e-Business. In T. Bastiaens, J. Dron, & C. Xin Eds., World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2009: 2199-2206. Vancouver, Canada: AACE.

Sherstobitoff, R. 2013. Inside the World of the Citadel Trojan McAfee Labs.

Stafford P. 2013 [Online] Cyber crime threatens global financial system. Available at: http://www.ft.com/cms/s/0/9804988c-3722-11e3-9603-00144feab7de.html#axzz2tMwSTsmF.

Symantec Cyber Crime Report, 2012 [Online] Cybercrime Report. Available at: http://now-static.norton.com /now/en /pu/images /Promotions /2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

TrendMicro. 2013. Security Threats to Business, the Digital Lifestyle, and the Cloud.

Vrancianu, M., & Popa, L. A. 2010. Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests. The Amfiteatru Economic Journal, 1228: 388-403.

Wall, D. 2001. 1 Cybercrimes and the Internet. Crime and the Internet: 1.