Growing Threat of Cyber Crime in Indian Banking Sector

– **Subodh K Kesharwani,** Associate Professor, SOMS, IGNOU
https://orcid.org/0000-0001-8565-1571 skesharwani@ignou.ac.in
– **Madhulika P. Sarkar,** Reader, SOMS, IGNOU
https://orcid.org/0000-0002-0506-7090 madhulikalal@gmail.com
– **Shelly Oberoi,** Research Scholar, SOMS, IGNOU
https://orcid.org/0000-0002-7806-6742 shellyoberoi83@gmail.com

Article History
Paper Nomenclature: Case Study (CS)
Paper Code: CYBNMV1N4SEP2019CS2
Submission Online: 09-Sep-2019
Manuscript Acknowledged: 11-Sep-2019
Originality Check: 16-Sep-2019
Originality Test Ratio: 3%
Peer Reviewers Comment: 24-Sep-2019
Blind Reviewers Remarks 28-Sep-2019
Author Revert: 29-Sep-2019
Camera-Ready-Copy: 30-Sep-2019
Editorial Board Citation: 30-Sep-2019
Published Online First: 09-Dec-2019

In the dictionary of criminal terminology, cybercrime is a relative a new term; it has emerged mainly after the introduction of technology in financial sector in late 90's. The present article focuses on the current scenario and technical aspects of cybercrimes concerning the banking sector and their related challenges and impcats.it also highlights the measures to combat the resulting cyber-attacks for better enhanced security.

Keywords: Banking System | Cloud Cyber Threads | Cloud Security Standard

Introduction

With the expansion of internet technologies, cyber-crimes have evolved worldwide and its nature and pattern have become more complex. More than half of the population is connected to web these days and every individual has easy access of internet for their daily routine purposes like banking, entertainment, education etc. The availability and use of smart phones have really added weightage to the remarkable growth in the internet. The demand of online services has made a challenge for providing security to the customers, mainly due to increase in cybercrimes, which is serious threat to the financial institutions and banks. Cybercrimes can take many forms like E-laundry, ATM fraud, credit card fraud, etc. There have been significant changes in banking industry due to emerging technologies and IT revolution. Banks have implemented IT solutions and is providing E-services to their customers like Mobile banking, National electronic fund transfer (NEFT), Real time gross settlement systems (RTGS), Electronic clearing systems (ECS) etc.

The present manuscript mainly discusses about cyber threats in banking systems and challenges to cater cybercrimes in banking industry.

Cyber threats in Indian banks

Banks are susceptible to many types of online frauds and cybercrimes. Cyber criminals are continuously carrying frequent attacks and Distributed denial of service (DDOS) and Internet of thing (IOT) is used as a platform for such attacks. According to India's computer emergency response team (CERT-in), there have been approx. more than one lakh cyber security incidents from 2014-2016, which included website intrusions, defacement, phishing etc. There has been multifarious increase in debit and credit card on account of skimming. Skimming, malware attacks, compromise of credentials by insiders etc has also become very common. Mobile banking and various applications provided by banks are also utilized by criminals and software vulnerabilities in banks apps and Adhar based account frauds by some business correspondents are also surfaced. Bank's SWIFT systems credentials for transfer of funds have also been misused through unlawful access. Recently, it has been advised by Reserve bank of India to stop issuing LOU's and LOC's. Nowadays, E-mail has become a tool for pilfering confidential credentials and their user has become prey to phishing attacks. Cyber criminals take advantage of poor security controls and end point

vulnerabilities. They also change their attack patterns to escape detection.

Symantec report has reported that cyber criminals has disrupted the IT services with IT tools and cloud services which has become vulnerable in cloud infrastructure.

Hence, for security purposes, banks have now strengthened their perimeter infrastructure by managing their security operation Centres and through following tools:

a. Security information and event management (SIEM)
b. Network behaviour anomaly detection (NBAD)
c. Privilege identity management (PIM)
d. File integrity management (FIM)
e. Anti-advanced persistent threat (Anti-APT)
f. Anti-phishing malware monitoring
g. Distributed denial of service (DDOS)
h. Web application filtering (WAF)
i. Vulnerability management

Challenges of cyber security

Cybercrimes are more prevalent in those organizations who have not implemented baseline cyber security defence. Cyber criminals scans all the connected devices for easy targets who slackers in cyber security implementation. It's very critical to identify critical assets and valuable information as many times it has been observed that there are shadows IT systems which do not come under cyber security purview. In banks, there can be leakage of personal data, stolen card data and unauthorized data sharing due to customer privacy violation. With the growth of the technology, cyber-attacks have taken a new shape in form of web attacks and Ransomware. Cyber-attacks in banks, generally, take in form of extortion of funds from individuals to organizations. The confidential credential is being stolen by phishing mails and syphoning of funds through whaling. It is a challenge for banks and financial institutions, to manage threats from multiple cyber-attacks, as consumers want the assurance from bank for protection of data. The major challenge is the lack of awareness of cyber threats and their serious implications by bank's staff and customers.It is also difficult for banks to manage and adhere to the regulatory compliance in India, as the volume of regulations has increased over the past few years.

Conclusion

It can be concluded that there is a gradual increase in the preference for online services by customers due to advantage in terms of cost saving, ease of use and convenience.

Even the banking systems are offering many online services to upturn volume of cashless transactions, but the threat of cyber security and cyber-attacks, is the main concern for the customer to avail those services. Now days, traditional way of banking transactions have been switched by E-banking. It has also been observed that financial institutions have overlooked some essential aspects relating to technology, which demands huge attention. The lack of awareness and inadequate knowledge to customers and banking officials has also simplified the work for cyber criminals. It has become easy for them to deceive customers due to lack of latest attack methodologies and protective measures. Moreover, the traditional polices laws and standards are also not adequate to cater the cybercrimes. The ministry of home affairs has constituted a committee, constituting officials from central bureau of investigation, national investigation agency, intelligence bureau and Delhi police, in 2015 to form a new legal framework, to cater to cyber-crime in our country. It has also been observed that the local law enforcement agencies do not possess the required skills to cater cybercrimes.For quicker and better cybercrime, it is required to engage the specialized cyber security professionals, as per NASSCOM's cyber security task force, it has been estimated that India needs almost one million trained professionals by 2025.

At present time, financial organizations need well laid cyber security with digital professionals, specialized security teams consisting of competent professionals should be engaged to cater cybercrimes proactively. It has become obligatory to continuously asses the cybercrime risk to improve security posture. It is a need of an hour to introduce cyber awareness campaigns to train customers about the latest attack methodologies. A well-organized and comprehensive Threat intelligence technology is also essential which will reduce the cyber threat vulnerabilities. A critical infrastructure is also required to be built to avoid cybercrimes in financial institutions and banks. The cooperation of Indian Goveremnt and industrial groups is also required to strengthen the legal framework for cyber security. The central bank of India i.e. Reserve bank of India has setup a cyber-security framework for guiding and monitoring cyber-attacks. RBI has also provided the guidelines on electronic banking, information security and cyber frauds, which instructs banks and financial institutions, to modify their policies, procedures and technologies based on emerging concerns. RBI has instructed banks to constitute a board on cyber security policy and also to establish cyber risks in real time through security operations center and to make necessary arrangements

for continuous surveillance on cyber threats. It has also warned all Indian banks weather private or commercials, to share all information on cyber security incidents with RBI. It also mentioned to evolve immediately cyber crisis management plan and to create awareness among stakeholders bout cyber security.

References

- ChangsokYoo, Byung-Tak Kang and Huy Kang Kim, (2015) Case study of the vulnerability of OTP implemented in internetbanking systems of South Korea, Multimed Tools Appl ,vol. 74, pp. 3289–3303.
- Claessens, J., Dem, V., De Cock, D., Preneel, B., and Vandewalle, J. (2002). On the security of today s online electronic bankingsystems. Computers & Security, 213: 253-265.
- Ellen Messmer (2008). First case of drive-by pharming identified in the wild [Online] Available:http://www.networkworld.com/article/2282527/lan-wan/first-case-of--drive-by pharming--identified-in-the-wild.html
- Florêncio, D., and Herley, C. 2011) Where Do All The Attacks Go? Economics of Information Security and Privacy III pp. 13-33, Springer New York.
- Gopalakrishana, G. (2011) Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds, RBI, Mumbai, Maharashtra, January
- Jason Milletary, Technical Trends in Phishing Attacks, US-CERT
- John, La. (2014) Vishing campaign steals card data from customers of dozens of banks [Online] Available:http://blog.phishlabs.com/vishing-campaign-steals-card-data-from-customers-of-dozens-of-banks
- MohdKhairul Ahmad, Rayvieana Vera Rosalim, Leau YU Beng and Tan Soo Fun, (2010) Security issues on Banking Systems,International Journal of Computer Science and Information Technologies, vol. 1, no.4, pp. 268-272.
- Moore. T, Clayton. R and Anderson.R (2009). "The Economics of Online Crime" , Journal of Economic Perspectives, Volume 23,Issue no.3, Summer 2009, pp.3-20.
- Pharming, Wikipedia Available: https://en.wikipedia.org / wiki/Pharming#cite_note-3
- Kaur, R. (2013) Statistics Of Cyber Crime In India: An Overview, International Journal of Engineering and Computer Science,vol.2, no. 8, pp. 2555-2559,
- Special Advisory –Data Breach in Indian Banks, 2016 www.mitkatadvisory.com
- Top Ten Cyber Squatter Cases Available: http://www.computerweekly.com/photostory/2240107807/Photos-Top-tencybersquatter-cases/1/Cybersquatting-cases-Number-10Dell

Dr. Subodh Kesharwani is an academician with a bronze medal in his post graduate and Doctorate in ERP System in 2002 from Allahabad University. He is one of the researchers who had concentrated his research on Total Cost of Ownership [TCO] & Critically evaluate ERP vendors including SAP. Dr. Kesharwani is presently an Associate Professor, School of Management Studies with a total 20 years of hardcore teaching and research in Information System and its linkages with various domains of management at Indira Gandhi National Open University, New Delhi.

skesharwani@ignou.ac.in

Dr. Madhulika P. Sarkar is currently Reader at SOMS, IGNOU (PhD LLB). She has a 15 year teaching experience with IGNOU. Her Area of interest is Taxation, Economics and Law. She has been part of various Seminars, Paper Presentations, and numerous Research Papers published in various National and International Journals. She is also a lifetime member of Indian Commerce Association.

madhulikalal@gmail.com

Ms. Shelly Oberoi Research Scholar,SOMS, IGNOU (BCom, University of Delhi, MCom, PGDBM, MPhil, and UGC Net) has worked with University of Delhi, IP University and Bhartiye Vidhyapeeth as Assistant Professor. She hasbeen part of various Seminars, Paper Presentations, and numerous Research papers published in various National and International Journals. She is also a lifetime member of Indian Commerce Association (Gold Medalist, Manubhai Shah Memorial Award, 2018). She has displayed vast success in continuously acquiring new knowledge and applying innovative pedagogies and has always aimed to be an Effective Educator and have a global outlook which is the need of today.

shellyoberoi83@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
16-Sep-2019	1208347032 (turnitin)	1519	9119

ORIGINALITY REPORT

3%	2%	1%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Dr Subodh K Kesharwani, Dr Madhulika p Sarkar, Shelly Oberoi. "PROSUMER&#65533;S UNDERSTANDING TOWARDS SOCIAL MEDIA MARKETING: AN EMPIRICAL STUDY", Industrial Engineering Journal, 2019 Publication	1%
2	techziffy.com Internet Source	1%
3	www.myfloridaindian.com Internet Source	1%

Note: www.Cybernomics.in Uses a "Turnitin" https://www.turnitin.com which is an American commercial, Internet-based plagiarism detection service, a subsidiary of Advance and also offers plagiarism-detection service for newspaper editors and book and magazine publishers called iThenticate..

Reviewers Comment

Review 1: Cybersecurity has been of great importance in the financial sector. It becomes all the more necessary since the very foundation of banking lies in nurturing trust and credibility.

Review 2: Everyone seems to be going cashless, using digital money, e. debit cards and credit cards. In this context, it becomes very important to ensure that all measures of cybersecurity are in place, to protect your data and your privacy.

Review 3: Banks need to be on their guard more than most businesses. That's the cost of holding onto the kind of valuable personal data that banks do. Your data with the bank can be breached if not protected from cybercrime threats.

Editorial Excerpt

The article has 3% of plagiarism which is accepted percentage for publication. The finding related to this manuscript noteworthy related to "**Growing Threat of Cyber Crime in Indian Banking Sector**". The Bank is one of the example of institute that using Information Technology (IT) in its daily task to fulfill the needs of organization's and customers. Technology nowadays gives an opportunity to satisfy the need of faster and efficient banking transaction but it is a double sword in Information system. The article has been earmarked and decided under "**Case Study**"

Scholastic Seed Inc.
www.scholasticseed.in

Citation
Subodh K Kesharwani, Madhulika P. Sarkar and Shelly Oberoi "Growing Threat of Cyber Crime in Indian Banking Sector" Volume-1, Issue-4, Sep 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.