Volume - 2
Issue - 3
March 2020
e-ISSN 2582-5755

2

Cybercrime: An Emerging Threat to Banks and NBFCs

– Jyoti
Research Scholar, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0002-1945-3005 jyotiningania@gmail.com

– Shirish Mishra
Associate Professor, Mahatama Gandhi Central University Bihar
https://orcid.org/0000-0001-7915-8297 shirishmishra@mgcub.ac.in

– Subodh Kesharwani
Associate Professor, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0001-8565-1571 skesharwani@ignou.ac.in

ARTICLE HISTORY
Paper Nomenclature:
Argument Based Credentials (ABC)
Paper Code: CYBNMV2N3MAR2020ABC2
Submission Online: 06-Mar-2020
Manuscript Acknowledged: 07-Mar-2020
Originality Check: 09-Mar-2020
Originality Test Ratio: 04%
Peer Reviewers Comment: 14-Mar -2020
Blind Reviewers Remarks: 16-Mar -2020
Author Revert: 19-Mar-2020
Camera-Ready-Copy: 22-Mar-2020
Editorial Board Citation: 31-Mar-2020
Published Online First: 31-Mar-2020

Invasion of the digital world has changed the way day to day activities are carried out. India being a country of young digital population with estimated 370 million users making up to about 30 percent of world's population becomes highly prone to carry out cyberattacks. The article highlights the emerging threat of today's cyber world known as cybercrime to the financial sector in general and banking in particular.

Keywords
- Cybercrime
- Cyber Threats
- Cyber Security
- Financial Sector

Introduction:

The modern era we are living in is known by the technology on which our daily routine life is greatly dependent and we live with it. This technology enables our reach to everything we need at our door steps that makes us more and more dependent on it. Innovation in technology has made the world a small place in which people are coming closer. This technological advancement has many opportunities and efficiencies to every type of organisation be it banking, education, medical, etc. But these technologies have also brought unprecedented threats with them known as **CYBERCRIMES**. In layman, Cybercrimes are known as the crimes that involve a network or computer. These days cybercrimes are becoming one of the most crucial issues across the globe that require utmost attention. Usually cybercrimes include an unauthorized access and security breach of information belonging to any person or organisation with the help of the internet. There is no doubt about the fact that cybercrimes are all time high in present, not even a single day passes when a bank's customers have not been fraudulently stolen of money from their bank account or an organisation suffering

a security breach. For everyone be it any bank or organisation the stakes involved in cybercrime is so high, it is all encompassing and its collective impact can be very astounding. Apart from financial losses cybercrimes also negatively impact an organisation's overall goodwill, reliability, trust, business assets, and reputation build in past along with its employees and shareholders, loss of business assets and reputation.

Across the globe banks are the most prone and have been largely hit by cyber criminals and hackers in recent years. Reason to that is usually cybercrime takes place where a large amount of money is found and undoubtedly banks and other financial corporations have got more money than any other entity at present therefore these are considered as the most prime and lucrative target of cybercriminals.

Banks possess the data of millions of users, which in a way provides numerous avenues for profits though extortion, theft, fraud, discontinuation of business, loss of assets/ business information, third-party claims etc. Cybercrime has become a big hacking business.

In comparison to any other kind of organisation, the financial sector is almost 3 times more prone to cyberattacks, which almost operates in a constant threat of it. These threats are actually a great challenge for the IT and security teams to safeguards the interest of all the stakeholder by actively keeping an eye on by collecting, disseminating and interpreting malicious events. A survey conducted by the PWC in 2016 on Global Economic Crime found that cybercrimes are the 2nd most globally reported crimes by which around 54% of organisations had been hit in the last two years.

One of the major significant factors of imposing cyber-attacks is also IoT connected devices, with these sensors assimilate, analyse and act on the information that offers new prospects for business, technology and media to create and new opportunities and values for the information to be compromised which results in sharing of more sensitive data the risks of which are exponentially greater. To do cybercrimes these days cyber criminals are using cloud based botnets to take over the power processing, launching Distributed Denial of Service (DDOS) attacks via cloud, exploiting near field communication etc. **(Deloitte)**

Some Facts About INDIA:

Emerging cybercrimes is a global problem that is increasingly leading to a variety of other problems from micro to macro levels and India is no exception to that. Digital landscape of today offers more flexibility and convenience for cyber criminals. According to a Forbes report highlights on banks and cybercrimes in comparison to any other industry banks are being targeted more frequently than other firms, over the past five years the security breaches rates of the financial sector have increased by around 300 percent amounting to a cost of $1 trillion each year to them.

The prime concern of the emerging threat is to find out ways and techniques to prevent frauds and data breaches in the digitally evolving global sphere. One of the major reasons for it becomes the unawareness about the cause and its implications. As per a survey conducted by KPMG in 2016, 12% of bank CEOs, 47 % of banking executives, VPs and MDs and 72% of senior VPs and directors didn't even know if their banks had been hacked. Hackers with advancement of technology undoubtedly are becoming more and more sophisticated in their methods. Below presented are some facts about the cybercrimes conducted in India:

In January 2018, the Aadhar system got hacked which compromised the personal data of over 100 billion people that caused greater concerns for national security.
According to the RBI reports during the period of 2008-17, total estimated reported cases of cyber frauds came out to be 1,30,000 amounting rupees700 crore. This figure clearly states that a cyberattack enough though no money is lost directly can result in a bank failure.
As per the data revealed by the National Crime Record Bureau (NCRB) in 2017, the cybercrime cases almost doubled in number and a big spike was observed over the previous years. The total number of cybercrimes across India was approximately 3,474 in 2017, up from around 2,402 cases in 2016. In 2018. As per the reports generated by RBI the observed cases of cyber fraud in 2018 amounted to Rs. 109.6 crore.
In December 2019, data breach of Airtel's mobile app compromised and exposed the data of 300 million users. In the caused security flaw personal information of the users such as name, email address, DoB, residential address, subscription information, device capability information for 4G/3G & GPRS, activation date, user type, and IMEI numbers etc. were exposed.
In Feb 2020, the debit/credit cards details of around half millions of people were put up on sale on an underground dark website; a popular hub for conducting financial crimes/frauds. The data included sensitive details of users such as card numbers, user name, CVV/CVC codes, date of expiry, email address etc.

Volume - 2
Issue - 3
March
2020
e-ISSN
2582-5755

Cyber Security:

Emergence of cybercrimes calls for robust cybersecurity measures and especially in the financial sectors cybersecurity has been of great importance as the very foundation of it lies in fostering trust and credibility. A weak cybersecurity measure by any bank can amount to a huge data breach can cause its customers base to take their money to some other bank, cancelling cards etc. Stringent cyber security measures should always be in the bank's priority list. To improve the cyber security framework the Indian regulatory situation has also become most robust and stringent. Reserve Bank of India (RBI) in 2016, made it mandatory for all the banks to put in place a robust and stringent cyber risk management system approved by their respective boards. In 2013, in order to fight against and protect the country's cyber ecosystem GOI released the National Cybersecurity Policy. Then in 2014, National Critical Information Infrastructure Protection Centre (NCIIPC) was developed to protect the information infrastructure against emerging cybercrimes. In 2017, the National Cybersecurity Coordination Centre (NCCC) was developed to create a consciousness about cybercrimes to the people in the country. In 2017, Cyber Swachhta Kendra was developed for the internet users to clean out the virus and malwares present in computers and other devices. Most recently the government has established Indian Cyber Crime Coordination Centre (14C) to strengthen the present system to tackle the issues related to cybercrimes in a more comprehensive and coordinated manner.

Cyber Security considerations for Banking Sector:

Many experts believe that though banks are protected from external threats but the threats that arise from within, which can result from the carelessness of the employees, have the potential to cause a greater risk.

To guard against such vulnerabilities banks must continuously engage in conducting various awareness programs, mock drills and stimulation exercises etc. for their employees to educate them against threats and to keep the infrastructure secure.

Following considerations in various services can be adopted by banks. For example, in internet banking transactions security measures such adaptive or two factor authentication, strong passwords, image authentication etc. can enhance security controls. While in m banking users must continuously ensure updating and testing of the application installed.

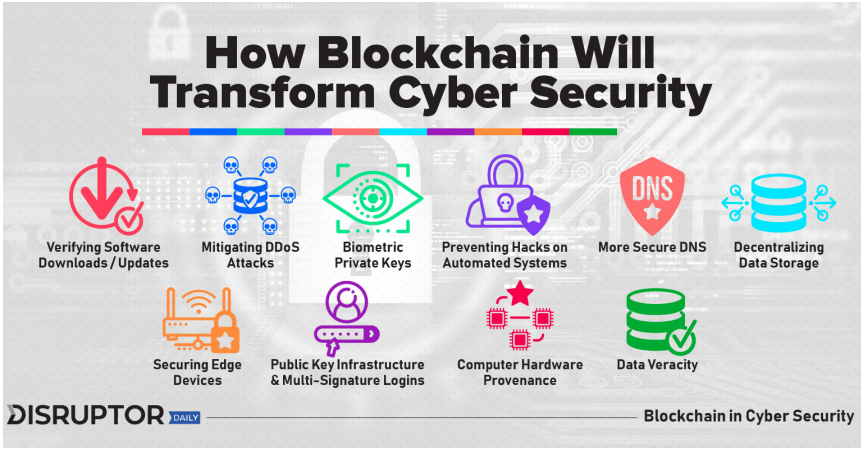
Mobile wallets or digital wallets should also be secured with strict passwords. In ATM's more stringent biometrics like voice scan, eye-retina, finger scan should be incorporated. Also banks and PSPs need to think through their security strategies, governance models and predictive controls to build a secure UPI environment that ensures a seamless user experience and at the same time balances security risks. (**BDO India)**

Implementing Blockchain Technology for Cyber Security:

Blockchain being one of the recent emerging technologies, though originally invented for bitcoins, holds the potential to become useful in strengthening cyber security framework. Owing to its distributed nature via eliminating the human interventions in the authentication process, blockchain leaves no scope for hacker or central failure and thus ensures a more tightened security framework. Blockchain will improve data integrity and digital identities via preventing the internet of things connected devices from Distributed Denial of Service (DDoS) attack and ensuring decentralized storage through encryption to guard against any unauthorised access or modification as it will demand consensus-based third-party validation for every transaction that will also improve the traceability of any and every transaction done.

Conclusion:

In recent years cybercrimes have emerged as a threat growing in leaps and bounds causing billions in financial sectors and its allied institutions. The imperative need of the hour for such financial institutions is to wake up and fight against their attitudinal mindset on a war footing. It is pertinent for all kinds of organisations to invest in multi-faceted, intelligent, smart and a cross-channel framework to tackle cybercrimes; that in a way besides helping save billions would also protect their credibility and reputation.



References:

- https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms?from=mdr
- https://www.techtimes.com/articles/245785/20191021/cybersecurity-in-banking.htm
- https://safeatlast.co/blog/cybercrime-statistics/#gref
- https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know
- https://www.information-age.com/cyber-crime-banking-sector-123464602/
- https://internationalbanker.com/banking/cybercrime-growing-threat-global-banking/
- https://www.hdfcbank.com/personal/resources/learning-centre/secure/5-reasons-why-cyber-security-is-important-in-banking
- https://www.stoodnt.com/blog/cybersecurity-in-banking-financial-services/
- https://financialit.net/sites/default/files/customerxps_white_paper_cybersecurity_vulnerability_in_indian_banks_1.pdf
- https://economictimes.indiatimes.com/industry/banking/finance/banking/watch-out-cyber-fraud-cases-in-banks-are-spiking/articleshow/67349755.cms
- https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms?from=mdr
- https://www.stoodnt.com/blog/cybersecurity-in-banking-financial-services/
- https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know
- https://sg.news.yahoo.com/bank-tomorrow-paperless-frictionless-without-physical-presence-105844743.html
- https://www.techtimes.com/articles/245785/20191021/cybersecurity-in-banking.html

Ms. Jyoti is currently pursuing her Doctoral Research study from SOMS (IGNOU), New Delhi. She has done her B.Com (H) from Shri Ram College of Commerce, University of Delhi and M.com from Hansraj College, University of Delhi and qualified UGC- NET JRF. She has been a part of various Seminars, Paper Presentations, Faculty Development Programme and National and International Conferences from time to time. She is an enthusiastic learner who believes in maintaining and maximizing the quality of life by implementing her skills and experience gained through education, hard work and dedication.

jyotiningania@gmail.com

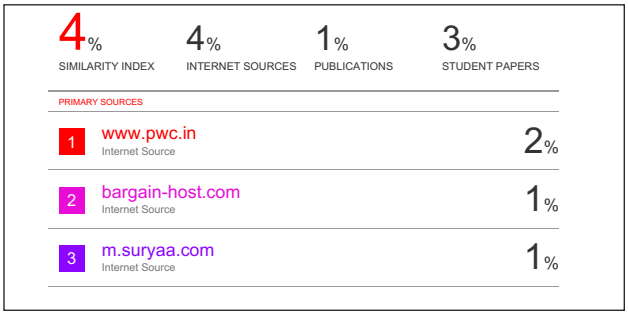
Dr. Shirish Mishra, Professor, Department of Commerce, Mahatma Gandhi Central University, Bihar.
shirishmishra@mgcub.ac.in

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

Annexure I

Submission Date	Submission Id	Word Count	Character Count
06-Mar-2020	1314616292	2039	9681



Note: The Cybernomics had used the turnitin plagiarism [https://www.turnitin.com/] tool to check the originality.

Reviewers Comment

Reviewer's Comment 1: The authors work had a magnified image over the work done on cybercrime. The content clearly pictured how various cybercrimes took place with increase in technological advancement. Various cases held in India showed its effect on banking and other sectors.

Reviewer's Comment 2: The article highlights the emerging threat of today's cyber world known as cybercrime to the financial sector in general and banking in particular.Even though the paper is short and crisp, then also it covered all the important and required aspects and also it is well structured.

Reviewer's Comment 3: The paper also had a liberal opinion on the positive effect of Blockchain technology helping to reduce cyber crimes that is the need of the hour.

Editorial Excerpt

The article has 4% of plagiarism which is accepted percentage for publication the finding related to this manuscript. This article talks about Cybercrime: An Emerging Threat to Banks and NBFCs. The prime concern of the emerging threat is to find out ways and techniques to prevent frauds and data breaches in the digitally evolving global sphere. It has been earmarked finalized for publication under the category of "**Argument Based Credentials** (ABC)".

Acknowledgement

Author is highly indebted to Scholastic Seed Inc &; editorial team of Cybernomics, for making the write-up in the shape of an article.

Disclaimer

All Views expressed in this paper are my own, which some of the content are taken from open source websites for the knowledge purpose. Those some of I have mentioned above in references section.

Citation

Jyoti, Shirish Mishra & Subodh Kesharwani "Cybercrime: An Emerging Threat to Banks and NBFCs" Volume-2, Issue-3, March 2020. (www.cybernomics.in)

Frequency: Monthly, Published: 2020
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in
https://orcid.org/0000-0002-7952-096X