International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 03(I), July - September, 2021, pp 17-20

CYBER SECURITY IN BANKS

Apeksha Lalitprasad Dave*

ABSTRACT

Since the pandemic has set foot worldwide in 2020, cyber attacks in banks have hogged headlines across the world. Moody warned banks globally of "increased risks of cyber attacks during the continued COVID-19 pandemic". Consistent with a VMware report, cyber attacks against banks and financial institutions globally increased 238 percent amidst the COVID-19 crisis between February 2020 and April 2020. Ransomware attacks increased during the same period. In India, the RBI red-flagged cyber security issues in its financial stability report in July 2020. In a very recent statement, the national security advisor affirmed that "financial frauds increased exponentially because of greater dependence on digital payment platforms following the COVID-19 pandemic". In other news, global hackers made headlines as they attempted over 40,000 cyber attacks on India's banking system, amongst others, over a period of 5 days in the last week of Jan. However, cyber security incidents don't seem to be unaccustomed the banking world. The history of the primary cyber threat goes back to 1970. For many years, banks across the world are fighting countless borderless battles with faceless criminals in cyberspace. With the rapid digitisation of the industry (and other industries), cyber threats and attacks became more pervasive and complex. This has led to an increasing evolution of cyber security. Indian banks have seen a gradual rise in cyber threats as they need been exploring or embracing complex technologies (such as mobile and internet banking), improving employee intranet, and more recently, adopting hybrid cloud technology. As a result, they need been selective in adopting digitisation in the past. Before the COVID-19 crisis, a majority of the Indian banks focused on strategic digitisation of their customer services and experiences one among the four pillars of the banking ecosystem. The rapidly changing behaviour and preferences amongst rising urban customers, millennial, and therefore the middle-income population (demanding faster solutions and better customised products) drove digitisation in services to customers. On the opposite hand, usages of digital technologies amongst three stake holders employees, business alliances, and vendors were measured and gradual. This is often partly due to the complexity of operations and also the associated degree of cyber risks. In the future, this trend of selective digitisation will change due to the evolving trends within the post COVID-19 era.

Keywords: *Cyber Crime, Banking Business, Pandemic, Threats, Transactions, Opportunities.*

Introduction

Banking system is one of the oldest businesses systems in the world and retained its existence from past in India. The banking system has its source in the earlier centuries. Awareness of banking was there among the prehistoric society because they felt the necessity of banking and makes use of money transaction to induce proper benefits. The importance of industry was recognized by the people because they'd realized the price of money in their life. Application of information Technology was successfully administered in the industry. Therefore it's concluded that information technology is the trouble shooter of the industry and also most helpful for the consumers for his or her day to day banking transactions. Phone Banking, automated teller machine machine Machines (ATM), Credit Cards,

* Assistant Professor, Sanskruti College of Management & IT, Surendranagar, Gujarat, India.

Debit Cards, ATM Cards, Smart Cards, Electronic Funds Transfer (EFT), Shared Payment Network System (SPNS), Electronic Clearing Services (ECS), Point of sale [POS] terminal, D-Mat Accounts, Electronic Data Interchange (EDI), E-Cheques, Computerized Accounting, E-Mail and RBI Net are variety of the samples of administration of information Technology in the Indian industry. However the implementation of recent technology in industry and advancement of E-banking not only offered opportunities for the consumers to avail comfortable banking services and for the banks to expand banking business but has also gave an equal opportunities and opened the doors for brand bright criminal activities. The present Article is the assessment of the impact of cyber crimes on the E-banking in India. This study may be a trial to look out up to what extent legal provisions are effective and efficient enough for controlling the cyber crimes against e-banking in India. The results of this study may encourage be helpful in assessing the effectiveness of the legislation, their weaknesses and may suggest ways to amend and plan for the long term.

Importance of Internet in Cybercrime

In today's environment almost every bank provides the service of payment of Bills or money transfer and retrieval of information from the information system of the Banks software through use of the internet banking. At any time of the day or night, makes everything you are doing along with your finances a bit easy

- **Pay Your Bills Online:** From internet banking, you'll be able to pay all bills like house rent, credit card bills, and electric bills, etc through online banking. There are some options for automatic payments also it'll be helpful for all people in their busy work some people forgot to pay their bill they'll use this automatic bill payment in online banking.
- **View Transactions:** Online banking allows you to access your recent and every transaction are done through your account. It also enables you to seek out out any unauthorized transition quickly it's easy to resolve your problem immediately with the assistance of online banking.
- **Transfer Money between Accounts:** this can be one amongst the most effective features in online banking we are able to transfer money to our family, friends so easily and, we will transfer money everywhere the world.
- **Online Banking in Mobile Application:** Most of the bank offers a mobile app to access their online banking from this you'll be able to transfer money and might use for shopping. Now some merchants are giving discounts while paying by banking applications.

Types of Cyber Attacks

- **Denial-of-service (DoS):** This attack is performed over the network user's computer to create it inaccessible to the user by flooding them with messages to trigger the crash.
- **Phishing:** Phishing is the process of acquiring the username and password of the user without his knowledge. These user login details will be anything sort of a checking account or social media login credentials.
- **Malware:** Malware could be a sort of software that spreads viruses through devices to other computers to crash the system. This will also crash remotely connected network computers.
- **Spam emails:** Spam emails are emails that are pushed inside the user's mail account without prior permission. It will be junk advertisement postings or anything inappropriate to the user.
- **Man-in-the-middle attack**: During this attack, a malevolent actor acts as a middleman between the transactions between two parties and gathers the data, and uses it against the users to realize access.
- **Spamming:** Spamming may be a method of messaging system to send a spam message to several recipients for advertising.
- **Spyware:** Its malicious software installed during a user's computer without their knowledge hacker can access all the files and their stored move into the system.

Proposed Ways for Internet Banking Security

The major responsibility of maintaining a secure Internet banking experience lies on the customer; customer to update browser, choose appropriate browser, update antivirus, choose appropriate antivirus, remember of phishing attacks, keeping of Malware, remember to update password every six months, choose a fancy password, etc. During this paper, we propose a unique model that shifts a number of these responsibilities to the banks. Banks have state-of-the-Art Information

Technology Operations and Centers. By investing a touch more, the banks can take a number of the responsibilities off from the customer and reduce the danger of security threats, thereby offering a reasonably secure environment for its customers. Below given proposed suggestions bridges the gap between the users and the Bank. The model states that the banks can enforce their security policies to confirm safer banking experience for users. On the opposite hand, users should follow the instructions provided by the bank to confirm a secure Internet banking experience.

Internet banking users should change password every three months, however, the bank is responsible to confirm that this happens by expiring the users' password every three months and forcing the user to settle on a new password. The users should detain mind while choosing a password that it mustn't be easy to guess, however, it's the banks responsibility to permit passwords that have capital and small letters, numbers and a special character. Any password that doesn't have these features won't be accepted. The bank should enforce that the user shouldn't use the previous 2 passwords additionally. Using virtual keyboard for safe guarding sensitive information like password or debit credit may be a responsibility added to the bank side. The Bank can enforce users to use virtual keyboard by disabling the sensitive field by using virtual keyboard provided on the webpage. As there's an opportunity for the user device to be infected by a malware or a key logger program that detects the key stroke and may compromise the password security.

Banks should use the concept of trusted device to make sure the identity of the users while the user is logging on. If the user has logged in from an untrusted device the bank system should send an SMS attentive to confirm if it had been the intended user. Education of the users could be a key component to make sure safe Internet banking experience. The bank can provide security warning on their sites after the user has successfully logged in to familiarize users on the threats that are risk for Internet banking. Banks should use computer software or machine based learning software that may make judgments on the user behaviour example transferring large amount of money to a destination not within the monthly pattern of the user. This software is wont to detect all electronic transactions including credit card transaction and can be able to detect if the user has made a purchase not within the customer's pattern and can alert and sometimes disable the credit card or E-banking account in extreme cases until the customer's identity is verified. The machine based learning or computing should predict this anomaly and take appropriate action. Information security could be a critical a part of the net banking process. Therefore, banks can improve the safety features from their side by securing their servers and therefore the communication between the user and Internet banking server.

Legal Remedy Available for Cyber Terrorism Under I.T.Act, 2000

The threat created by the malware for cyber terrorism is successfully controlled as long as provisions of the I.P.C with the strict provisions of the information Technology Act, 2000 jointly implemented. Courts can use their discretion by combining provisions of various statutes to undertake and do the whole justice goodbye the provisions can operate in the presence of each other. Accordingly, the Indian codification, 1860 and also the provisions of IT Act is add-on with the provisions of I.P.C to manage the cyber terrorism. The protection of IT Act is claimed for:

- **Violations of Privacy:** Right to privacy is a part of the Right to life and personal liberty enshrined under Article 21 of the Constitution of India. The numerous provisions of the IT Act 2000 pertinently protect the online privacy rights of the netizens. The legal remedy available against the culprit using the malware. Section 1(2) read with Section 75 of the IT Act 2000 provides for an extra-territorial application of the provisions of the Act. Thus, if someone (including a remote national) contravenes the privacy of an individual by means of computer, system or network located in India, he would be liable under the provisions of the IT Act 2000.
- **Prevention of knowledge and data theft:** Provisions of IT Act 2000 handling the data theft under section 43, section 65, Section 66, Section 70 and Section72 is also successfully invoked. Likewise Provisions of ITA Act 2008 under section 43A and section 72A jointly supplemented with section 22 of I.P.C.,1860 and 378 of I.P.C.,1860 are going to be invoked.
- **Prevention of distributed denial of services attack:** A malware may use the strategy of distributed denial of services (DDOS) to overburden the electronic bases of individuals. Thus, distribute denial of services by use of malware are visiting be tackled by invoking the provisions of sections 43,section 65 and section 66 of IT Act 2000 collectively.

- **Prevention of network damage and destruction:** In India there is not any law, which is specifically dealing with prevention of malware through aggressive defense. Thus, the analogous provisions must be applied in an exceedingly purposive manner.

Conclusion

The Internet banking service is obtainable by banks to supply convenience for their customers, however, there are great benefits to banks still. The foremost important benefit to banks is the reduction in operational cost be incorporating many services on their online portal. Therefore, the banks should take more responsibility in ensuring a safer Internet banking environment for their customers. In this article, we proposed a model that comes with more responsibility on banks to confirm that the data Technology policies are adhered by customers. As an example, instead of informing customers that it's good practice to alter password every 3-6 months, the banks should force customers to alter their passwords every three months through expiring their passwords so customers are forced to alter their password. The Banks should also integrate the newest Information Security Technologies to make sure that the communication is secure between bank and customers. The proposed model would supply a safer Internet banking environment which might be of mutual interest to both banks and customers. Also the technologies proposed during this model are existing technologies and wish not be invented nor developed from scratch. For instance, the trusted device concept is an available technology and already in use by non-banking industries. Google already uses trusted devices in their Gmail application. Also there are many existing algorithms for Artificial Intelligence (AI) supervised and unsupervised learning that would be integrated to learn customer's behaviours and detect anomalies.

References

1. Haq S and Khan B.L." E-Banking Challenges and opportunities in The Indian Banking Sector" published in Innovative Journal of Business and Management 2 : 4 July – August (2013) available at www.innovativejournal
2. Sharma V., Part B- An Overview of cyber law, paper I, Introduction to the cyber world and cyber Law published on http://www.elearningilidelhi.org/eSikshak/other/Courses/Course101/
3. Module9/OVER VIEW OF CYBER LAW
4. Reserve Bank of India "Anti-Money Laundering (AML) Measures/Combating of Financing of Terrorism (CFT)/Obligations of banks under PMLA, 2002" – 30th June 2010
5. Manikyam K.Sita Mrs. "Cyber Crimes Law & policy perspectives" published by Hind Law House Pune. 2009.
6. Jagadeesh, S. (2005) "Credit Card Fraud: Causes and cures from professional's perspective. C.A Journal of the Institute of CAI, Vol. 53 No. 7, January
7. Gharaibeh, N., 2013. The impact of customer knowledge on the security of E-banking. *International Journal of Computer Science and Security (IJCSS)*, *7*(2), p.81.
8. Kesharwani, A. and Singh Bisht, S., 2012. The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. *International Journal of Bank Marketing*, *30*(4), pp.303-322.
9. Al-Ajam, A.S. and Md Nor, K., 2015. Challenges of adoption of internet banking service in Yemen. *International journal of bank marketing*, *33*(2), pp.178-194.
10. Hanafizadeh, P., Keating, B.W. and Khedmatgozar, H.R., 2014. A systematic review of Internet banking adoption. *Telematics and informatics*, *31*(3), pp.492-510.
11. Kierkegaard, S., 2007. Swallowing the Bait, Hook, Line, and Sinker: Phishing, Pharming, and Now Rat-ing!. In *Managing Information Assurance in Financial Services* (pp. 241-260). IGI Global.
12. Council, F.F.I.E., 2005. Authentication in an internet banking environment. *Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp.(FDIC). Retrieved March*, *18*, p.2005.