International Journal of Innovations & Research Analysis (IJIRA)
ISSN : 2583-0295, Volume 01, No. 03, October - December, 2021, pp 57-59

CYBER SECURITY IN BANKING SECTOR

Mrs. Shalu Pareek*

ABSTRACT

One of the most significant tools in the field of banking technology is cyber security. It aids in the security of information and is the world's greatest challenge today. Cyber security is nothing more than the protection of transactional data. As cyber thieves become more sophisticated, hacking not only online transactions but also the profiles of specific businesses and organizations, it is critical to scrutinize criminals solely through security measures. Governments and businesses are putting in place measures to combat cybercrime. Aside from numerous measures, the banking industry continues to be a major source of concern. ATM security, online database transactions, and other threats are key concerns in banking. As a result, the study focuses on the use of cyber security through ranking analysis, cyber incidents in the banking industry by percentage analysis, and the ways to address those concerns in the banking industry. As a result of the study's findings, banks must be vigilant of internet usage and email because cyber crimes continue to diverge along multiple roads as new technologies and applications are introduced, shedding light on cyber security challenges. There is no ideal answer for cybercrime because it is increasing every day, but banks should do all possible to reduce it in order to have a safe and secure future in cyber space.

Keywords: *Cyber, Crime, Technology, Security, Andriod App.*

Introduction

Today humans are able to send and receive data in any form just by clicking single button, but they ever think how those data has been transmitted or sent to the other person safely without any leakage of information. The answer depends on cyber security. Cyber security is the application of protecting systems, networks and programs from digital attacks. These cyber attacks are aimed at accessing, changing or destroying sensitive information; extorting money from users and interrupting the normal business processes.

One of the most significant tools in the field of banking technology is cyber security. It aids in the security of information and is the world's greatest challenge today. Cyber security is nothing more than the protection of transactional data. As cyber thieves become more sophisticated, hacking not only online transactions but also the profiles of specific businesses and organizations, it is critical to scrutinize criminals solely through security measures. Governments and businesses are putting in place measures to combat cybercrime. Aside from numerous measures, the banking industry continues to be a major source of concern. ATM security, online database transactions, and other threats are key concerns in banking. As a result, the study focuses on the use of cyber security through ranking analysis, cyber

* Assistant Professor, Department of Computer Science, S.S.G Pareek PG Girls College, Jaipur, Rajasthan, India.

incidents in the banking industry by percentage analysis, and the ways to address those concerns in the banking industry. As a result of the study's findings, banks must be vigilant of internet usage and email because cyber crimes continue to diverge along multiple roads as new technologies and applications are introduced, shedding light on cyber security challenges. There is no ideal answer for cybercrime because it is increasing every day, but banks should do all possible to reduce it in order to have a safe and secure future in cyber space.

It wasn't too long ago that sophisticated executives could have long, thoughtful discussions on technology strategy without even mentioning security. Today, companies have substantial assets and value manifested in digital form, and they are deeply connected to global technology networks – even as cyber attackers become ever more sophisticated and adaptable to defenses. At most companies, boards and senior executives acknowledge the serious threats that cyber attacks pose to their business. What they are not sure of is how to create a strategy that helps them understand and address the threats, in all their forms, today and in the years ahead. And they're asking for such a strategy every day. Our experience working to protect some of the world's largest and most sophisticated companies, and our proprietary research, have revealed three broad mandates that can help organizations transform their cyber security efforts. In this compendium, we offer a comprehensive series of articles that describe how companies can make these mandates a reality, and help their leaders sleep more soundly.

In this study a novel model is proposed which puts more responsibility on banks to avoid security breaches which are caused due to negligence or lack of awareness by the users. The responses from the conducted survey highlighted two aspects regarding users: 1) User behavior while conducting Internet banking and 2) User awareness on threats relates to Internet banking. Some of the negative response is related to lack of awareness of users on threats related to Internet banking. It would be difficult for users to cope with the changing technologies and threats. So the logical solution could be that banks could control the process by imposing information technology policies that can help bridge the gap that lead to a safer E-banking environment and reduce the possibility of security breaches. They can use behavioral study or model that are based on Artificial Intelligence or Machine based Learning that could provide early-detection of negligence of users or target those domains which could lead to a security breach on Internet banking.

Digital Wrongdoing can be just expressed as violations that include the utilization of PC and a network1 as a medium, source, instrument, target, or place of a wrongdoing. With the developing part of web based business and e-exchanges, the financial wrongdoing has floated towards the advanced world. Digital wrongdoings are expanding all around and India also has been seeing a sharp increment in digital violations related cases in the ongoing years. Digital Violations can be comprehensively arranged into classifications, for example, digital fear based oppression, Digital harassing, PC Vandalism, Programming Robbery, Wholesale fraud, Online Robberies and Fakes, Email Spam and Phishing and some more.

Nonetheless, from the part of money related digital wrongdoings submitted electronically, the accompanying classifications are transcendent:

The Internet banking service is offered by banks to provide convenience for their customers, however, there is great benefits to banks as well. The most 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 more secure Internet banking environment for their customers. In this paper, we proposed a model that incorporates more responsibility on banks to ensure that the Information Technology policies are adhered by customers. For example, rather than informing customers that it is good practice to change password every 3-6 months, the banks should force customers to change their passwords every three months through expiring their passwords so that customers are forced to change their password. The Banks should also integrate the latest Information Security Technologies to ensure that the communication is secure between bank and customers. The proposed model would provide a more secure Internet banking environment which would be of mutual interest to both banks and customers. Also the technologies proposed in this model are existing technologies and need not be invented nor developed from scratch. For example, 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 could be integrated to learn customer's behaviors and detect anomalies.

Conclusion

The investigation has given an outline to the idea of E-saving money by talking about profoundly different digital wrongdoings, distinguished explicitly in the managing an account division. The Saving money framework is the soul and spine of the economy. Data Innovation has turned into the foundation of the saving money framework. It gives an enormous help to the regularly expanding difficulties and managing an account necessities. By and by, banks can't consider presenting money related item without the nearness of Data Innovation. Anyway Data Innovation has an unfavorable effect too on our managing an account division where wrongdoings like, phishing, hacking, falsification, bamboozling and so on are submitted. There is a need to avert digital wrongdoing by guaranteeing validation, recognizable proof and check procedures when an individual goes into any sort of saving money exchange in electronic medium. The development in digital wrongdoing and intricacy of its examination strategy requires proper measures to be embraced. It is basic to expand the collaboration between the partners to handle digital wrongdoing. As indicated by National Wrongdoing Records Agency it was discovered that there has been a tremendous increment in the quantity of digital violations in India in recent years. Electronic wrongdoing is a difficult issue. In instances of digital wrongdoing, there isn't just money related misfortune to the banks yet the confidence of the client upon banks is additionally undermined. Indian managing an account division can't abstain from keeping money exercises helped out through electronic medium as the investigation recommend that there has been an expansion in the quantity of installments in e-saving money. Nonetheless, the adjustment in the saving money industry must be such which suits the Indian market. In conclusion, it very well may be presumed that to dispense with and kill cybercrime from the internet is certifiably not an apparently conceivable assignment however it is conceivable to have an ordinary keep an eye on managing an account exercises and exchanges. The main auspicious advance is to make mindfulness among individuals about their rights and obligations and to additionally making the usage of the laws all the more firm and stringent to check wrongdoing.

References

1. Amoroso, E. (2006). *Cyber Security*, Summit, Silicon Press, New Jersey
2. Bayuk Jennifer L. Healey J and others (20120*, Cyber Security Policy Guidebook*, Wiley and Sons, Hoboken, New Jersey
3. Chaubey,R.K. (2015). *An Introduction to Cyber Crime and Cyber Law*, Kamal Law House, Kolkata
4. Chopra, Deepti and Merrill. Keith, (2002) *Cyber Cops. Cyber Criminals and internet, I. K. International*, New Delhi.
5. Duggal. Pawan (2018) *Cyber Law 3.0*, Universal Law Publishing, Lexis Nexis, Gurgaon.
6. Dongre, Shilpa S. (2015). *Cyber Law and its Applications*, Current Publications, Mumbai.
7. Kataria, R.P. and Sriniwas, S.K.P. (2017*). Cyber Crimes,*Orient Publishing Company, New Delhi.
8. Mani,K.(2012*), A Practical Approach to Cyber Laws*, Kamal Publishers, New Delhi
9. Mishra,J.P. (2014*), An Introduction to Cyber Law* , Central Law Publications, Allahabad
10. Rastogy, Anirudh(2014), *Cyber Law, Law of Information Technology and Internet,* Lexis Nexis,Gurgaon.
11. Rattan J. and Rattan V. (2017) *Cyber Laws and Information Technology*, Bharat law House Pvt. Ltd. New Delhi.
12. Rao S. V. Joga (2004*). Law of Cyber Crimes, Information Technology Law*, Wadhwa and Co. Nagpur.
13. Sharma, Nishesh (2017). *Cyber Forensics in India, A Legal Perspective,* Universal Law Publishing, Lexis Nexis, Gurgaon.
14. Shrivastav, V. P. (2003). *An Introduction to Cyber Crimes Investigation*, Indian Publishers Distribution, Delhi
15. Singh, Yatindra Justice(2015). *Cyber Laws,* Universal Law Publishing Co., New Delhi.

❑❍❑