International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Analysis of the Information Security of Co-Operative Banks of India

Mr. Adarsh Desai [1], Dr. Priyanka Sharma [2]

[1] *Student of M. Tech. (Cyber Security), School of Information Technology and Cyber Security, Raksha Shakti University, Lavad-Dahegam, Gandhinagar - 382305, Gujarat, India. Email: ad8460367699@gmail.com*
[2] *Dean-Research and Publications, Professor-School of Information Technology and Cyber Security, Raksha Shakti University, Lavad-Dahegam, Gandhinagar - 382305, Gujarat, India. Email: dean-rp@rsu.ac.in, ps.it@rsu.ac.in*

Abstract - *Banking and financial services sector plays vital role in the development of a nation's economy. As two third of the population of India lives in the Rural areas, Co-operative banks play a crucial role in rural financing. They provide funding of areas under agriculture, livestock, milk, personal finance, self-employment, setting up of small-scale units. The past two decades witnessed dramatic transformations in the ways of doing business in financial sectors as more and more technological solutions were aggressively used in these financial institutions. The introduction of technological solutions has brought in convenience to the customers and cost effectiveness from the banking perspective, thus banks are highly obliged to maintain integrity of financial and non-financial transactions and protecting the privacy of customers while being accountable to the stakeholders. However, the adoption of these technologies has brought in a large number of information security threats that may cause financial liabilities to the banks. Such information breaches incidents may also result in tarnishing the goodwill and reputation of a bank and may lead to losing large number of existing customers. Therefore, Analysis of the Information Security, Understanding the Information Security Threats and preventing such incidents are highly required in a professional banking environment. Current research basically focuses on the implementation and audit of Information Security in the Co-operative Banks of India and technical and non-technical threats to them.*

Key Words: Information Security, Information Security Audit, Vulnerability Assessment and Penetration testing, Risk Assessment (as per ISO 27001:2013), Internal Control System, Cyber Security Policy, Core Banking System (CBS), etc.

1.INTRODUCTION

Banking is the blood to a country's economy. Indian banks have large volume of customer base as compare to the foreign banks. Latest research initiatives all around the world shows that the modern banking organizations face huge challenges in managing information security threats than yester years. This scenario is also visible in the Indian context. The concept of CIA (confidentiality, integrity, availability and accountability) has more relevance in today's banking context.

A co-operative bank is a financial organization which belongs to its members. So, they are at the same time the owners and the customers of their bank. Co-operative Banks are formed to promote the upliftment of financially weaker sections of the society and to protect them from the clutches of money lenders who provide loans at an unreasonably high-interest rate to the needy. The co-operative structure must follow the principles of cooperation, mutual help, democratic decision making and open membership. Cooperatives Banks are registered under the Cooperative Societies Act, 1912. Co-operative Banks of India are regulated by the Reserve Bank of India and National Bank for Agriculture and Rural Development (NABARD) under the Banking Regulation Act, 1949 and Banking Laws (Application to Cooperative Societies) Act, 1965.

The cooperative banking system started with the aim to promote saving and investment habits among people, especially in rural parts of the country. Co-operative financial sector is having large number of customers. The Information Technology revolution has had a great impact on the Indian banking system. It has undergone many a transformation and CORE Banking System (CBS) is the latest in the list of such transformations. CBS has brought a 360-degree change in the entire banking industry. There are many threats and less awareness of Information Security that prevent a person from using online banking. The threats are also being faced by banking channels of developed countries. Threats include Phishing, viruses, user identity theft and password cracking, etc. Bankers are fully dependent upon Information Technology for survival and the need to protect information and mitigate risk is more paramount than ever before. The various national surveys confirm a high number of attacks against organizations information resources. The incidents are frequent and also expensive; management must take security seriously to protect their critical organizational and customer information. The purpose of this study is to explore and assess information security system of Co-operative Banks. The overall purpose of this research study was to examine as well as extend the body of knowledge and understanding regarding information security system in Co-operative Banks of India.

2. REVIEW OF LITERATURE

The sphere of the research study is mainly linked with information security in CBS, security standards and Co-operative banks. Therefore, the researcher has reviewed the literature focusing on these domains of the study. The literatures available to the researcher on the application of information security in Indian banks are classified according to co-operative banking and Information Technology, Information Technology in banking a global perspective, Online banking security issues, Global Scenario, Information Security, Information Security Standards and Various articles published in newspapers on information security. Researcher conducted an extensive review of the literature to identify the key attributes of information security and related issues and the gaps identified from the literature review are listed below:

- Risk management in co-operative banks.
- Lack of knowledge and skills of the employees
- Lack of Prevailing standards and solutions
- Lack of awareness amongst end users about the information security
- Information Security Policy and procedure
- Physical Security and Environmental security
- Information Security Management
- Planning, management and monitoring of information security system
- Security testing is still in its infancy stage
- Network security is becoming more and more crucial.
- Business Continuity Planning
- Disaster Recovery Planning

The existing research in information security related to Co-operative Banks showed that there is still lack of studies in the present literature about the information security in co-operative banks. The researcher also found that there is still an increasing need for comprehensive but specific approaches to information security aspects that would assist management in implementation of effective information security program not only in CBS environment of co-operative banks but providing the technology-based solution. It was found from the literature review that there was not a single study carried out on Analysis of the Information Security of co-operative banks of India.

3. RESEARCH METHODOLOGY

3.1 RESEARCH OBJECTIVES

- To analyse the present status of overall information security systems of Co-operative banks (Co-Op. Banks).
- To find the gaps in the existing information security systems of Co-Op. Banks.
- To assess the applicability of security standard of information security system in Co-Op. Banks.
- To study the awareness of information security systems among end users of Co-Op. Banks.

3.2 SCOPE OF RESEARCH

The present study focuses on information security system in selected Co-operative banks in India. The present study is conducted for Co-Op. Banks who have implemented CORE banking solution (CBS).

3.3 METHODS OF DATA COLLECTION

The primary data is a data that is gathered for a specific research in response to a particular problem through interviews, questionnaires or observations. The primary data is collected from various co-operative bank's management members, Information Security Officer (IT heads), and employees by a structured questionnaire. Also, the Heads of the IT department of the respective co-operative banks are interviewed by researcher. However, the prime sources of data are the IS Audit and VAPT done by the researcher in the respective co-operative banks. This includes Information Security Policy, Measures included for controlling and monitoring information security system, Physical Access Control and Environmental Security, Asset Management, Human Resources Security, Logical Access Control System, Network Security, Operating System Access Control, Cryptographic Controls, Training and Awareness Program, Data Backup, Business Continuity Management, ATM Security, Internet Banking Security, Information System Security Technologies such as Anti-virus software, Firewall, Vulnerability/Patch Management, Static account logins/ passwords, Smart cards and other one-time tokens and Biometrics System, etc. and the experiences of the Co-Op. Banks with regard to Information Security related Problems, Training and Awareness, Roles and Responsibility.

The secondary data for this study was obtained from published documents and literature relevant to the study. The secondary data is obtained through various kinds of documents such as research papers, RBI annual reports, RBI and NABARD Guidelines to the Co-Op. Banks, books and articles, research papers from online journals and Government regulation for core banking and also from web information.

4. ANALYSIS

The six major activities involved in information security of Co-operative Banks are:

- Policy development.
- Specification of roles and responsibilities.
- Designing and developing a security control framework.
- Implementing a solution.
- Monitoring and awareness.
- Training and education.

All the Co-operative Banks agreed with that the implementation of CBS improve the operational efficiency,

better compliance and standardization of process. These help them to improve profitability of bank and offer various services to their customers. Most of the banks are using CBS from past 5-6 years. However, there is no provision made for upgradation of CBS and other IT infrastructure. The two-thirds of the banks do not have the proper Information Security Policy. Moreover, half of the banks still do not conduct the IS Audit Regularly.

Most of the banks have outsourced the CBS but they do not have the proper agreement of access, development and maintenance. Only few banks have deployed access controls (Swipe Cards) to restrict the access to sensitive area. Many banks don't have security guards. Most of all the banks have CCTV systems but some of them don't keep the history of a month. Server Rooms and Network Cabinet are not properly locked to restrict the access. However, All the banks keep visitor register. They have adequate procedure to take care of natural disaster like fire, earthquake, and flood. All the banks have secondary power supply. Majority of the banks don't have the Network Diagram and proper cable tagging in the devices. Moreover, only half of the banks have maintained detailed inventory of information assets as per ISO standards.

Almost all the banks have defined roles and responsibilities of personnel. They have appropriate HR policies and procedures in place e.g. disciplinary actions for staff and contractors that violate the IT security rules. All the Co-operative banks i.e. 100 percent stated that they have implemented successfully unique login ID and passwords on end user's computers for authorized access to information and information system. Password is changed on regular basis to avoid unauthorized access to information system. Similar percentage is supported for the passwords stored in encrypted form and password is not displayed on screen. Most of them i.e. 80 percent stated that they create user ID based on roles and responsibilities. 90 percent banks indicate that inactive terminals are shut down/log off automatically after a defined period of inactivity.

Most of the Co-operative banks uses their Private Network for the CBS. In this Network, even internet is strictly prohibited. They use internet services in other stand-alone system which is not connected to CBS Network. In Rest of the Banks, where CBS and internet are working simultaneously on a system, have implemented the Firewall. But the set of rules of firewall are not properly defined. 70 percent bank's network, Remote login is enabled with proper authorization.

50 percent Co-Op. banks stated that the Data Centre is owned by the banks themselves. All the co-operative banks have documented and tested data backup strategies and procedures. Moreover, the data backup is scheduled automatically. All the Co-Op. banks s have maintained physical and environmental security at Data Centre and disaster site. 50 percent co-operative banks review policies, procedures, standards and guidelines regularly for business continuity management. Rest half of the co-operative banks have no single rational framework for business continuity planning in their banks. Only, 35 percent co-operative banks members of the crisis/incident management and recovery teams and other relevant staff are aware of the plans and are clear on their personal roles and responsibilities.

50 percent co-operative banks implemented patch management. The same number of banks follow the best practice for configuration management. Only 20 percent co-operative banks have adopted computer forensics techniques to capture and maintain forensic evidence. It has been found that 65 percent banks do not conduct penetration testing on regular basis to identify the gap in information security architecture. Majority of banks i.e. 95 percent have policy procedure for virus protection. It has been also observed that they are using enterprise licensed Antivirus and update antivirus software regularly. It has been found that 80 percent co-operative banks have ensured end user computer's USB ports are locked.

85 percent co-operative banks stated that to operate ATM, dual control is set up. 95 percent co-operative bank's ATM is equipped with surveillance camera to record criminal activity at and around the ATM. 70 percent co-operative banks revealed that security guard is appointed at the ATM. The same number of ATMs are perfectly inbound with wall or floor or both and the cables are properly concealed. 50 percent co-operative banks provided internet banking facility to their customers. All the internet banking facilities support two-factor authentication for fund transfers through internet banking. 33.33 percent co-operative bank's software locks the user-id if it is used for X unsuccessful times to logon to the system. 80 percent urban cooperative bank's CBS system application software maintains password length minimum 8 characters and with combinations of alpha-numeric and special characters.

It has been found that 25 percent co-operative banks computer system was infected by malware, while 15 percent co-operative banks revealed that their systems were experienced phishing attacks. 20 percent co-operative bank's computer systems were experienced password sniffing and financial fraud. Denial of service, exploit of wireless network, system penetration, hardware theft or loss were experienced by their CBS solution environment confirmed by 12 percent banks. Few co-operative banks agreed upon insider abuse of internet access or e-mail, Exploit of DNS server. It is also observed that 20 percent co-operative banks stated that unauthorized access to the system by insider was taken place.

It has been found that 70 percent cooperative banks have carried out implementation audit for all the IT assets. 50 percent co-operative banks have carried out compliance audit for implementation audit. Only 30 percent co-operative banks have monitoring system/tools to provide logs,

warning, critical message and alerts. Very few co-operative banks i.e. 15 percent have followed ISO 27001: 2013 (code of practice for information security management) benchmark in IT infrastructure. It is also found that COBIT (IT Governance) standard is followed by only 10 percent co-operative banks.

5. CONCLUSIONS

It was revealed from the above analysis that:

1. The CBS environment of Co-Op. banks does not comply with information security standard applicable, security policy, procedure and guidelines.
2. Co-Op. banks' physical and environmental security controls in IT infrastructure are inadequate.
3. Co-Op. banks' data security control measures in IT infrastructure are inadequate.
4. End users of Co-Op. banks have positive attitude towards training and awareness program conducted by Co-Op. banks.
5. The password security awareness at all level of management is high in Co-Op. banks

The key challenging issues in information security in Co-Op. banks are:

- View security as of little importance
- Lack of Information Security Standard
- Budget constraints
- Lack of information security policies and procedures in place
- Inadequate physical and environmental security controls
- Inadequate access control procedure
- Weakness in Network Security
- Absence of adequate cryptography controls
- Poor implementation of security policies
- Poor implementation of information Security controls

Therefore, it is concluded that majority of the Co-operative banks are not serious about the information security. But they are trying their best to deal with the Information Security Threats. This may adversely effects on the functioning of Co-operative banks. Therefore, it is concluded that the information security in Co-operative banks' IT infrastructure is in adolescence stage.

REFERENCES

[1] Information systems audit policy for the banking and financial sector, Working group for information systems security for the banking and financial sector Department of Information Technology, Reserve Bank of India, Mumbai, October, 2001.
[2] Rupal R. Patel (2005), Operational Efficiency of District Central Cooperative Banks in Gujarat-A Comparative Study, Department of Business Management Saurashtra University, Rajkot, Gujarat (India).
[3] Report of Working Group on IT Support for Urban Cooperative Banks, Reserve Bank of India, December 19, 2007.
[4] Atul Bamrara, Gajendra Singh, Mamta Bhatt (2013), Cyber Attacks and Defence Strategies in India: An Empirical Assessment of Banking Sector, International Journal of Cyber Criminology, Vol 7, ISSUE 1, January - June 2013.
[5] Information security Framework (2012), An IDRBT Publication, Institute for Development and Research in Banking Technology (Established by Reserve Bank of India), Version 1, 2012
[6] Report on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, Reserve Bank of India, Mumbai, January 2011.
[7] Working Group report on Cloud computing option for Urban Cooperative Banks, Reserve Bank of India, October 2012
[8] https://www.rbi.org.in
[9] Ambhire V.R., Teltumde P.S., Information security in banking and financial industry, International Journal of Computational Engineering & Management (IJCEM) 14 (2011), 101-105.
[10] Bhosale M.D., Indian banking sector at a glance, International Research Journal of Engineering and Technology (IRJET) 2(1) (2015), 212-221.
[11] State of Data Security and Privacy in The Indian Banking Industry, Data Security Council of India-KPMG Survey, New Delhi, India, 2010
[12] NASSCOM and Data Security Council of India. https://www.dsci.in/resource/centre
[13] http://shodhganga.inflibnet.ac.in/
[14] http://en.wikipedia.org/
[15] http://www.nabard.org/