Challenges of Co-Operative Financial Sector for Implementation of Cyber Security Controls

Bhagirath H. Chavda[1], Chandesh D. Parekh[2]
[1]*M. Tech, School of Information Technology & Cyber Security, Raksha Shakti University*
[2]*Dean, School of Information Technology and Cyber Security, Raksha Shakti University, Lavad, Gandhinagar, India*

***Abstract*- Co-operative financial sector is growing by time they are responsible for nation's economic growth. [1] It is mandatory to implement security controls to be followed guidelines by RBI. Co-operative financial sector somehow lacks to implement cyber security controls there are several challenges which financial sector faces. A proper cyber security infrastructure needed to prevent threats and control the level of risk which can cause damage to the Co-operative financial sector. Current scenario is not lacking completely when it comes to security. Observations obtained by conducting information security audit, VAPT, risk assessment, reviewing critical assets helps to give suggestion to the Co-operative financial sector. How they can improve the security parameters and what kind of challenges they face to implement that is crucial also how it affects to the customers as well as that particular financial sector. Current research basically focuses on Challenges of Co-Operative Financial Sector for Implementation of Cyber Security Controls.**

Researches states information obtained results from information security audit. There are few checkpoints having reference to guidelines from RBI which determines how security controls implemented to the Co-operative financial sector. Vulnerabilities also determined from VAPT which gives security measurement to system and logical controls. Also, infrastructure plays decisive role for the security controls in financial sector.

***Index terms*- Auditing, Information Security, Vulnerability Assessment, Penetration testing, Risk Assessment, Cyber security controls, Server Review, Network Diagram, Cyber security standards.**

I.INTRODUCTION

Co-operative financial sector is having large number of customers. Financial sector must implement security controls such physical security, logical security, system security and environment controls. Most of the Co-operative financial sectors maintain the security parameters then they somehow fail to implement cyber security controls as well as physical security controls. While conducting information security audit many findings took place as implantation of cyber security controls doesn't implied properly. There are several challenges that a Co-operative financial sector cannot controls large number of branches located at various remote location. The CIA (confidentiality, integrity, availability) concept must be followed by each individual Co-operative financial sector. There are many vulnerabilities found while conducting VAPT of critical system as well as each node responsible to banking operations. This study points out major challenges a Co-operative financial sector finds while implementing cyber security controls.

Information Security audit starts with understanding flow of network how it is established in that specific Co-operative financial sector. By understanding network diagram flaws can be determined and where Co-operative financial sector with respect to cyber security. Auditing all the branches of Co-operative financial sector and conducting VAPT to get findings in the domain of physical security, logical security, environment controls and system security. Review critical assets of Head office such as network diagram, Data centre and Disaster recovery review, Server review, Firewall review, Antivirus review, Mail and Messaging services review, Application review service wise, DVR review, Inventory management system review, ATM machine review, UAT environment review and many more assets are included.

[2] Banks are the custodians of economic transactions and their role is more important than ever in a very cashless economy. Within the past, an individual

could take live of the bank and spend it on any transaction they pleased. In today's digital marketplace, a transaction simply cannot be processed without the involvement of some reasonably online banking institution.

The banking sector is constructed upon trust. People that put their money within the bank don't check their accounts on a commonplace. This can be because they need faith within the banker's ability to stay their account secure and pay after they enkindle money. The bank's profits are a return for building this trust in its ability to stay account safe.

II. LITERATURE REVIEW

Challenges to the Co-operative financial sector for implementing centralized control over all the branch and monitor it constant basis. [4] The rapid propagation of technology and thereby resulted vulnerabilities gave thanks to malware attacks, cyber-attacks etc. by criminals, terrorists and hostile nations. The three main problems emerging from uncertainty in information security management are frequent changes within the security requirements, externalities caused by the safety system and obsolete assessment of security system. [5] Bhosale (2015) reviewed Indian banking sector and pointed that continuous technology advancements and innovations have influenced the bank's interaction with its customers, suppliers and equivalent.

[6] Ambhire and Teltumde (2011) conducted a study on information security in banking and financial industry by analysing the technological risk factors. The study identified four security issues namely, access to data system, secure communication, security management and development of secure management systems because the major risk factors. it's highly relevant to grasp the critical information security threats and risks among various security threats because the business impact from these security threats differ in terms of potential impact from operational and financial perspectives.

Consider an individual Co-operative financial sector having Data Centre and Disaster Recovery in their ownership. DC must have to be in HA (High-Availability) mode. Structure of network flow from a single node to DC as well as any individual asset must be defined properly. A major challenge for any Co-operative financial sector to implement regular patch updates for operating system such as windows. Almost every Co-operative bank is having windows 7 and some of the banks are having windows XP as their operating system. It is critical issue and vulnerable because using older versions of operating system cause number of vulnerabilities which leads to cause cyber-attack which disrupt banking operations as well as financial loss due to this mistake. Microsoft officially declared not to give official support to windows 7. Thus, it becomes more vulnerable so security parameters compromises. Any attack can take advantage of vulnerabilities in operating system and intrude to disrupt current operations of banking. It is not feasible to upgrade each and every node (computer system) which are used for banking operations because Co-operative banks are having more than 100 branches located in remote locations. So, to upgrade each system a Centralized Domain Control must be implemented. Active directory is useful to manages devices such as computer system over a network. Network admin can implement changes as well as upgradation and push that to the nodes connected on the AD. WSUS (windows server update services) is the best solution for maintaining windows updates and push it to the child nodes. Once latest patches upgraded to WSUS each Microsoft product will be upgraded and push it to the nodes connected to it. It is used for specific for windows services on server. To deploy other policies rather than Microsoft products to push AD DC (Domain Controller) mechanism is major concern. The changes are pushed to the branch server and that changes are applied to every computer connected to the branch server. Upgradation of operating system Co-operative bank faces issue regarding compatibility of CBS application with operating system. Co-operative banks should raise issue to the CBS vendor for the compatibility issue. In Co-operative bank Operating system upgrades are done still if it is not compatible then banking operations are compromised thus major challenge for every Co-operative bank is the OS upgradation and compatibility with all the banking applications running over it.

III. RESEARCH METHODOLOGY

Research starts with conducting IS audit of the Co-operative bank and by observations which security

factors are compromised and how the Co-operative bank should implement respective changes as per cyber security standards. Major challenges are OS upgradation and compatibility to run banking applications to the computer system. Conducting VAPT will give detailed vulnerability information at system level. [3] Vulnerability assessment refers to gain information about vulnerability which states what weakness are available in the system. Penetration testing exploits vulnerabilities and provide measurement of security by deploying an attack. So that prevention can be implemented from such attacks in network. Risk assessment defines evaluation of potential risk. Loopholes in critical assets and what level of risk determined through risk assessment.

A major challenge for Co-operative bank to install manageable switch at every branch to implement VLAN. Virtual Local Area Networks used to separate physical network into multiple logical networks. [7] Virtual Local Area Network (VLAN) creation allows you to create separate broadcast domains on a switch. the published domains can come with each other with the assistance of a Layer 3 device like a router. A VLAN is principally accustomed form groups among the hosts no matter where the hosts are physically located. Thus, a VLAN improves security with the assistance of group formation among the hosts. When a VLAN is formed, it's no effect until that VLAN is attached to a minimum of one port either manually or dynamically. one in all the foremost common reasons to line up a VLAN is to line up a separate VLAN for voice, and a separate VLAN for data. This directs the packets for both varieties of data despite using the identical network.

It is very costly to implement at every branch due to number of branches a Co-operative bank is having. It is not feasible to invest such amount because one standard manageable switch costs around 34000 INR. It is also challenge for Co-operative bank if VLAN is not implemented then cyber security standards are compromised.

Review of critical assets such as server ae also major factor of auditing. Server such as CBS server, CTS server, RTGS server, Database server, Antivirus server and many more. These critical assets must be placed at secure location where physical control is well established. These servers need to be configured and updated properly.

There are other challenges which are listed below:

- Infrastructure
- User Awareness
- Physical security controls
- Environment controls
- CBS Access Control
- Network Security
- Endpoint Vulnerabilities
- Logging and monitoring of assets
- Maintenance and Business continuity controls

Infrastructure is one the sensitive factor for any financial sector. Proper infrastructure should be followed with respect to cyber security as well as maintaining physical security to the unauthorized access. All the secure areas need to covered by CCTV so that any physical intrusion can be prevented. Having area where all the critical assets must be placed properly. Implement ATM machine in such a way that cables are concealed so that no attack can disrupt transactions. Implement fire alarms in critical areas are important factor for any financial institute are mandatory.

User awareness is also big challenge for Co-operative bank due to lack of awareness cyber fraud can take place. Most of the users such as employees responsible for critical responsibility to the bank are having limited awareness for the cyber security. They are having limited knowledge about how to prevent cyber-attack as they individually don’t follow security concerns such as they need to protect their system by giving strong system password as legitimate authentication must be followed to access such critical systems. Employees are using weak password in CBS application, Mail and messaging system, System password and many more applications. Also, employees saving password which stored in browser cookies can also be harmful. Sharing password with other employees, not logging out from the system whenever they are not using application move from their place. This basic security awareness needs to spread to each and every employee. Solution for that is Co-operative bank should conduct cyber security awareness seminars periodically. So that more awareness results less chances of any threats.

Physical security controls lack in Co-operative bank as any unauthorized person can have access to the critical areas. CCTV needs to work properly and keep records at least of 30 days. Night vision should be clear so that any suspicious activity can be monitored. Implementing environment controls is also challenge for Co-operative bank as it is costly to implement all the environment controls to each branch. In every branch there should be enough fire extinguisher and it needed to refill it periodically.

User of bank need to learn how to operate fire extinguisher. Smoke detector must be installed as disaster can happen anytime so it better to have control for prevention. Panic switch should be installed which needs to send notifications to Branch Manager, Assistant manager and Head office so that bank should take action if any consequences occurs. It is costly to implement every physical and environment security controls to each branch located separately but mandatory to implement for Co-operative financial sector.

In case of CBS access control most of the CBS application are provided by third party vendor so it doesn't come under bank's ownership. Any changes that may need to implement should take time to respond the third party. Multi factor authentication should be implemented for login. As challenge to implement it is providing each computer system a biometric device and integrate it to CBS application. It is expensive and take more time to implement to each branch. Proper validation should be implemented such as password like it should follow global password policy as having combination of alphanumeric and containing special characters and having at least one upper case alphabet. It needs to be implemented by default in CBS application. Session timeout neds to be implemented properly as most of Co-operative banks using CBS application are having 10-15 minutes of session timeout that can cause A long expiration time increases chances of an attacker by guessing a valid session ID. Co-operative bank must order CBS application vendor to implement such major findings to be overcome. Restriction of Internet while using CBS application must be followed if it is not followed then unwanted websites is allowed and virus can be injected in system as well as bank network. Multiple logins should not be enabled because it will increase risk of attack.

Network security states that networking devices needs to place in secure location having proper physical access control. It needs to located at such a place that anyone cannot have access near to networking devices and that is challenge to Co-operative bank as they already located networking devices which is visible to everyone. There must be cabinet facility provided and rack should be closed.

Endpoint vulnerabilities refers to each node used for banking operations. Giving administrator rights to every computer results user can install any unauthorized software or remove the installed software, and can modify the group policy, security configuration policy, and proxy can be set by user. It is mandatory to give standard rights as per user's role to work for banking operations. There must be authentication policy to access internet as well as while using internet CBS cannot be run so it needed to be auto switchable mode.

Maintenance and Business continuity controls refers to maintenance of complaint register and visitor register. Challenge for Co-operative banks is that maintaining such registers are important and each branch should follow it. But it is not feasible for bank to control whether branch is following such instructions or not it depends upon branch itself.

IV. RESULT & DISCUSSION

.

Research of challenges of Co-operative sector for implementation of cyber security controls determines how difficult for a financial sector to maintain the cyber security controls. It is mandatory to implement the control as possible to prevent cyber-attacks. Thus any critical sector needs to seriously take the challenges and overcome it regularly.

V. CONCLUSION

Co-Operative Financial Sector faces several challenges for Implementation of Cyber Security Controls. It is mandatory to overcome all the factors that compromise Cyber security standards. There are solutions available to implement cyber security controls however it is large domain implementation take time. Implementing it from smaller domain to the larger ones at a certain moment cyber security controls can be fulfilled in particular timescale.

Challenges can be overcome over a time period by implementing from smaller scale.

VI. ACKNOWLEDGMENT

I acknowledge my institute Raksha Shakti University to give opportunity to research and my guide Mr. Chandresh Parekh to give valuable guidance. Raksha Shakti University always focus on growth of students. I would like to apricate Mr. Niraj Goyal to provide me knowledge about all the auditing aspects. He helps me to choose domain for my research

REFERENCES

[1] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI129BB26DEA3F5C54198BF24774E1222E61A.PDF "Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs)", Latest Access Time for website is 19 April 2020.

[2] https://torii.io/security/security-implementation-banking-finance/"Cybersecurity Risks for Banks", Latest Access Time for website is 19 April 2020.

[3] https://www.veracode.com/security/vulnerability-assessment-and-penetration-testing "VULNERABILITY ASSESSMENT AND PENETRATION TESTING", Latest Access Time for website is 19 April 2020.

[4] Abbas H., Magnusson C., Yngstrom L., Hemani A., Addressing dynamic issues in information security management, Information Management & Computer Security 19(1) (2011), 5-24.

[5] Bhosale M.D., Indian banking sector at a glance, International Research Journal of Engineering and Technology (IRJET) 2(1) (2015), 212-221.

[6] Ambhire V.R., Teltumde P.S., Information security in banking and financial industry, International Journal of Computational Engineering & Management (IJCEM) 14 (2011), 101-105.

[7] https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-200-series-smart-switches/smb5097-configure-a-vlan-on-a-switch.html"Configure a VLAN on a Switch", Latest Access Time for website is 16 April 2020.