



# Summer Internship Report

## A Study on Cyber Security Policy for Urban Cooperative Banks of Gujarat

Yogita Attal,  
Summer Trainee at RBI, Ahmedabad  
IMNU MBA FT (2020-2022)

## Title Page



<b>Author of the Report</b>	Yogita Attal
<b>Company Name</b>	Reserve Bank of India
<b>Company Address</b>	Ahmedabad Regional Office, Near Gandhi Bridge, Ahmedabad - 380014
<b>Project Title</b>	A Study on Cyber Security Framework for Urban Cooperative Banks of Gujarat
<b>Date of Report Submission</b>	12 <sup>th</sup> July 2021
<b>Purpose of the Report</b>	To understand the implementation of cyber security in urban cooperative banks.
<b>Prepared For</b>	Institute of Management, Nirma University
<b>Submitted To</b>	Prof. Sanjay Jain

## **Acknowledgements**

Summer Internship provides a platform to the post graduate students which helps them in learning, self-development and building up of necessary skills and competencies. It enables the students to work closely with the industry and to get real time learning exposure about the working of the corporate world. I express my gratitude to Institute of Management, Nirma University for providing me this opportunity to complete my summer internship with Reserve Bank of India.

I would like to express my special thanks of gratitude to Mr. Ashok Kumar, GM, RBI Ahmedabad who has given me his valuable insights and providing necessary information required for the completion of my summer internship research.

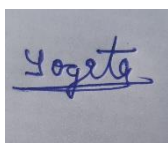
I would also like to thank Mr. Prince Bansal, Manager, RBI Ahmedabad for his constant help and support throughout the duration of two months by explaining me the basics of the topic and the list of probable topics that I can include in my research report.

I would like to express my thanks of gratitude to Prof. Sanjay Jain for his constant support, guidance and motivation. His motivation and guidance have played a major role in successful completion of this internship.

## Declaration

I, Yogita Attal hereby declare that the project titled- *A Study on Cyber Security Policy for Urban Cooperative Banks of Gujarat* is an original piece of research work carried out by me under the guidance of Mr. Ashok Kumar, GM, RBI Ahmedabad. All the information used in the research project are collected from authentic and genuine sources. I further declare that this project has not previously formed the basis of the award of any degree or diploma or similar title of recognition.

Signature:

A rectangular box containing a handwritten signature in blue ink that reads "Yogita".

Name: Yogita Attal

Roll No.: 201462

Section: D

Batch: MBA – FT (2020-2022)

Date: 12<sup>th</sup> July 2021

Place: Ahmedabad

## **Executive Summary**

Urban Co-operative Banks (UCBs) play an important role in the economy's financial sector. Till 1996, these banks were allowed to lend money only for non-agricultural purposes, however, this distinction does not hold today as the scope of their operations has widened considerably. UCBs have seen several changes in their operations and functioning throughout the years. They operate on a smaller scale compared with commercial banks; however, they endeavour to provide almost similar services like NEFT-RTGS, Internet Banking, Debit and Credit Cards, Locker Facility, E-Tax Payments, etc. to their customers. Banks' utilization of information technology has grown expeditiously, and now it has become a significant part of their everyday functioning. With the ongoing integration of digitization in their processes, Urban Co-operative Banks are also experiencing an increased frequency of cyber incidents/attacks. Thus, to fend UCBs from such cyber threats and malignant attacks, RBI has introduced comprehensive cyber security measures that prescribe several controls needed to be implemented by UCBs on the basis of their digital depth and interconnectedness to the various payments systems. For better functioning of UCBs, RBI has also released a Vision for Cyber Security for UCBs, which prescribes several actions to fortify the cyber security infrastructure of UCBs. As per RBI guidelines, UCBs have made several changes in their existing hierarchy and functioning. There are many challenges that the UCBs of Gujarat face in the implementation of the prescribed controls, as it requires sizable investment in building cyber security infrastructure and recruiting competent professionals who can manage it. Not only this, the Covid-19 Pandemic has also adversely impacted the assets and resources of the UCBs. Even in these difficult times, UCBs in Gujarat have implemented most of the cyber security controls as prescribed in the framework. They have made significant progress towards completing the actions that come under Cyber Security Vision. However, some smaller UCBs are finding it challenging to implement all the controls as they do not have ample resources to be invested. Going forward, the guidance and support of RBI and other associated institutions will be essential for such UCBs to manage their cyber security infrastructure more efficiently.

## Table of Contents

<b>Executive Summary</b> .....	<b>4</b>
<b>Part A: Profile of the Organization</b> .....	<b>7</b>
Company Brief .....	7
Major Functions/Services .....	8
Customers .....	10
<b>Part B: Project Work</b> .....	<b>11</b>
Introduction.....	11
Nature of Problem .....	11
Objectives of the study.....	11
Utility of the study.....	11
Methodology .....	12
Approach.....	12
Sources of Data .....	12
Method of Data Collection.....	12
Sample Size .....	12
Context of the Problem .....	13
Presentation of Data.....	13
Introduction to Urban Cooperative Banks of Gujarat.....	13
Major Changes in the Urban Cooperative Banking Sector .....	15
Introduction to Cyber Security .....	16
Most Common types of Cyber Security Incidents/Attacks .....	17
Cyber Security Incidents in various Banks of India .....	18
Cyber Security Trends and Challenges in Banking Industry .....	19
Role of Reserve Bank of India in Framing Cyber Security Framework for UCBs .....	20
Cyber Security Framework of RBI for Urban Cooperative Banks .....	20
Comprehensive Cyber Security Framework for Urban Cooperative Banks- A Graded Approach .....	21
Technology Vision for Cyber Security 2020-2023 for Urban Cooperative Banks.....	23
Factors affecting cyber security implementation in Urban Cooperative Banks of Gujarat.....	25
3 layers of Cyber Threat Mitigation and RBI’s Comprehensive Cyber Security Framework .....	26
Role of Top Management in Cyber Security Governance in UCBs .....	27
Awareness of Staff and Customers in minimizing Cyber Security Attacks.....	28
Steps taken by RBI and other regulatory institution for cyber security infrastructure .....	28
Importance of Cyber Security infrastructure in Urban Cooperative Banks after the Covid 19 scenario .....	29

Challenges faced by Urban Cooperative Banks due to Covid 19.....	30
Analysis and Discussion .....	31
Findings .....	32
Implementation of Technology Vision for Cyber Security in UCBs of Gujarat .....	32
Implementation of Comprehensive Cyber Security Framework in UCBs of Gujarat .....	32
Best Cyber Security Practices in UCBs of Gujarat.....	34
Suggestions and Recommendations .....	34
Part C: Learnings from the Project.....	37
<b>Annexure – A.....</b>	<b>39</b>
<b>Annexure – B.....</b>	<b>40</b>
<b>Annexure – C.....</b>	<b>41</b>
<b>Bibliography .....</b>	<b>42</b>

---

## *Part A: Profile of the Organization*

---

### **Company Brief**

Reserve Bank of India has come into existence on 1st April 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934. The head office of Reserve Bank of India (RBI) was initially established in Kolkata but was permanently shifted to Mumbai in the year 1937. It was originally set up as a private entity but after the independence, it became nationalised in the year 1949 and now it is wholly owned by the Government of India. It is also a member bank of the Asian Clearing Union. It issues information regarding the economy, banking and the financial system. The Banking Regulation Act of 1949 gave the Reserve Bank of India (RBI) the authority to "regulate, control, and inspect banks in India." The Banking Regulation Act further stipulated that no new bank or branch of an existing bank could be established without first obtaining a licence from the RBI, and that no two banks could have the same board of directors.

It is the apex bank that regulates the financial and banking system of the country and its primary function is to issue the currency notes and govern the monetary system of the country. It is also known as the Central Bank of the country. RBI is also responsible for the issuance of the monetary policy of the country. It manages the country's main payments system and also responsible for the economic development of the country.

Indian Banking Sector comprises both scheduled commercial and cooperative banks. Commercial banks can be further divided into 12 public sector banks, 22 private sector banks, 46 foreign banks and 43 regional rural banks.

Cooperative Banks comprises Urban Cooperative Banks and Rural Cooperative Banks. There are 1531 Urban Cooperative Banks out of which 53 are scheduled urban cooperatives and 1478 are non-scheduled urban cooperative banks. Out of 53 scheduled cooperative banks, 7 scheduled urban cooperative banks are in Gujarat.

All the affairs of RBI are governed by 21 Board of Directors which is appointed by the Government of India on the lines of the Reserve Bank of India Act.

#### **The preamble of RBI:**

“to regulate the issue of Banknotes and keeping of reserves with a view to securing monetary stability in India and generally to operate the currency and credit system of the country to its



advantage; to have a modern monetary policy framework to meet the challenge of an increasingly complex economy, to maintain price stability while keeping in mind the objective of growth.”

### Major Functions/Services

The services provided by the Reserve Bank of India can be broadly classified in form of various functions performed by it. The major functions of RBI are mentioned below:

- **Issuer of currency:** RBI issues and exchanges or destroys currency and coins not fit circulation. It is the only institution that has the authority to print currency notes. It administers that the general public has an adequate amount of currency notes in circulation.
- **Monetary Authority:** Formulates, implements and monitors the financial policy. The main objective is to maintain price stability, whereas keeping in mind the target of growth.
- **Regulator and supervisor of the money system:** RBI prescribes broad parameters of banking operations among that the country's banking and financial set-up functions. The main objective of this function is to maintain public confidence within the system, defend depositors' interests and supply cost-efficient banking services to the general public.
- **Banker to the Government:** It is the banker, agent and financial advisor to the government of India. It performs merchandiser banking functions for the central and state governments. As a banker, it manages the accounts of the government. As an agent, it buys and sells securities on behalf of the government. And as an advisor to the government, it helps them in framing the policies to regulate the money market.
- **Banker to banks:** RBI supervises the banking system of the country. As a banker's bank it has the same relations with other banks of the country as a commercial banks has with its customers. RBI accepts deposits from other banks and provides them loans when required. It maintains the banking accounts of all regular banks and monitors and issues guidelines regarding various liquidity requirements. It governs the entire banking system of the country which includes commercial banks, cooperative banks, foreign banks etc.

- **Credit Regulation:** It regulates the flow of credit in the country by keeping a check on inflation and taking corrective actions from time to time. RBI controls the supply of money in the economy by regulating the credit creation by commercial banks. During inflation, it restricted the supply of money and during deflation, it liberalizes the money supply.



- **Manager of the Foreign Exchange Reserves of the country:** It manages and regulates the Foreign Exchange Management Act, 1999. It not only manages the foreign exchange reserves but it also exercises the managed floating rate in order to maintain stability in the foreign exchange rate. The objective is to facilitate external trade and payment and promote orderly development and maintenance of the exchange market in India.
- **Developmental Role:** It performs a large variety of promotional functions to support national objectives.
- **Regulator and Supervisor of Payment and Settlement Systems:** RBI introduces and upgrades safe and economical modes of the payment systems within the country to satisfy the necessities of the general public at giant. The main aim is to maintain public confidence in payment and settlement system.

So in short, the various products and services offered by Reserve Bank of India are: Currency notes and money, loans to the government, credit settlement, foreign exchange reserves, etc.

## Customers

The main customers of the Reserve Bank of India are Government of India and the Banks. RBI does not deal directly with general public as customers, however, the various functions performed by RBI are directed towards the growth and development of the economy. It provides a number of services to the banks by taking care of their liquidity requirements. It serves commercial banks, cooperative banks and foreign banks as well. It issues regulatory guidelines to banks from time to time so that the banks can function efficiently. It provides loans to other banks of the country. RBI helps the Government in getting adequate amount of money whenever required.

**Note:** As RBI is not the profit earning entity but it is regulator of the financial and banking system, which is being established through an act and thus no other entity in the country has the authority to perform services which are being currently offered by RBI. It does not have any competitor and thus performing any kind of industrial analysis will not be a feasible option.

---

## ***Part B: Project Work***

---

### **Introduction**

#### **Nature of Problem**

Cyber security infrastructure involves huge capital outlay and a number of changes in the existing operations of the banks. RBI has issued certain circulars and guidelines mentioning Urban Cooperative Banks to upgrade their existing cyber security infrastructure. Urban cooperative banks operate at a small scale and cyber security practices are very new to them and thus this project tries to identify the challenges and barriers in implementation of the cyber security practices and finding out some solutions and best practices which can help smaller UCBs in building their cyber security infrastructure.

#### **Objectives of the study**

The main objectives of this research study are:

1. To understand the Co-operative banking scenario of Gujarat.
2. To understand the cyber security framework applicable to urban cooperative banks.
3. To know about the digital interconnectedness adopted by urban cooperative banks of Gujarat.
4. To identify the best cyber security practices implemented by urban cooperative banks of Gujarat.
5. To identify the challenges and barriers associated with the implementation of cyber security infrastructure in urban cooperative banks of Gujarat.

#### **Utility of the study**

The utility of the study is that it will help us to identify whether UCBs are able to comply with the cyber security infrastructure and guidelines issued to them by RBI. Cyber threats and crimes are increasing day by day and to minimize their impact RBI has introduced graded cyber security framework and technology vision for UCBs. The study will help us to find out the how UCBs of Gujarat has implemented the cyber security practices and what challenges has been faced by them during the process of upgrading their cyber security infrastructure. The project also aims to find out some best cyber security practices that can be adopted by other banks.

## Methodology

### Approach

The research design is based on qualitative research approach. This is because the research is predominantly based on the analysis and interpretation of data collected through the various interviews, reports, publications and circulars issued by Reserve Bank of India. Data is also collected by studying the annual reports of the sample that is Urban Cooperative Banks of Gujarat.

### Sources of Data

Both primary and secondary sources of data have been used for the collection of data regarding the cyber security policy for Urban Cooperative Banks of Gujarat. The sources like the employees of the banks, website of the organizations such as Reserve Bank of India, The National Federation of Urban Cooperative Banks and Credit Societies Ltd. (NAFCUB) etc. has been used. As mentioned above, official websites and annual reports of urban cooperative banks has also been used to know about their cyber security infrastructure.

### Method of Data Collection

The data was collected through both primary and secondary sources. For primary data collection, telephonic interview method has been used. Telephonic interviews of Chief Information Security Officer (CISO) of all scheduled urban cooperative banks has been taken to understand the cyber security infrastructure and best practices at their bank. Telephonic interviews have helped me to collect qualitative and subjective data for better analysis.

For secondary data collection the reports, circulars, press releases etc. has been used. These data were readily available in the public domain on the official website of Reserve Bank of India.

### Sample Size

In order to carry out the research, cyber security practices of 7 scheduled urban cooperative banks of Gujarat has been studied. Non-scheduled banks have not been taken for the study as the data on such banks were not readily available in the public domain and non-scheduled banks are very small in size providing limited services, so the cyber security framework issued by RBI may not be completely applicable to them. Thus, these 7 are the only scheduled urban

cooperative banks of Gujarat and this will truly represent the cooperative banking scenario of Gujarat and cyber security threats associated.

## Context of the Problem

Gone are the days when cyber security was only significant for IT companies. Nowadays, Cyber Security is equally important for other sectors as well. One such sector where cyber security has become paramount is banking. Cyber Security in banks involves all the measures taken to protect the bank's computer networks, data, and information from unauthorized access. Since the demonetization in November 2016, India has seen rapid growth in digital transactions and payments. Various banks have developed mobile applications for faster and secure transactions. Banks have also introduced different banking technologies like Wallets, 24\*7 money transfers, and many more. With such massive changes in banking transactions, the risk of cyber-attacks has increased manifold.

### **Importance of Cyber Security in Banking:**

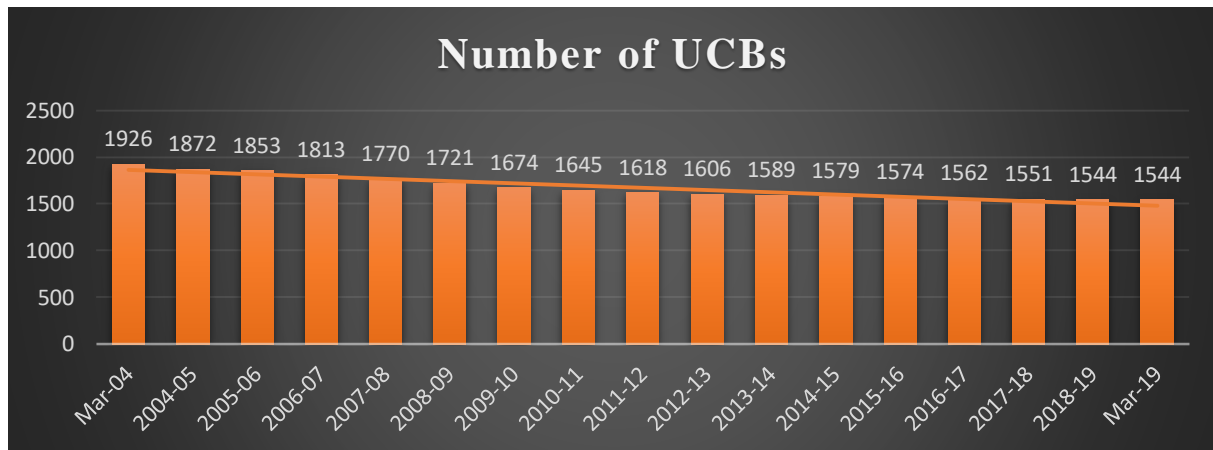
1. With the growing digitization and the increasing focus on cashless transactions, it becomes imperative for banks to update themselves with cyber security measures to reduce the chances of fraud.
2. A minor cyber security threat can cause much damage to the bank. It can lead to loss of public trust in banks and customer dissatisfaction.
3. A data breach impacts the reputation of banks and causes substantial financial loss to the customers. Therefore, banks must implement cyber security measures to protect the customers' data and their assets.
4. Customers put their trust in banks by revealing personal data for various documentation purposes. There have been many instances where the customers' private data has been accessed by criminal elements. Thus, cyber security is of utmost importance for banks to prevent their customers from such malicious attacks.

## Presentation of Data

### **Introduction to Urban Cooperative Banks of Gujarat**

As the name itself suggest, cooperative banks are financial entities, that work on the principle of co-operation and help. The term Urban Co-operative Banks (UCBs), though not

formally outlined, refers to primary cooperative banks settled in urban and semi-urban areas. These banks, till 1996, were allowed to lend cash just for non-agricultural functions. This distinction doesn't hold these days. These banks were historically centred around communities, localities work place teams. They basically season to little borrowers and businesses. Today, their scope of operations has widened significantly. Many Cooperative Banks are also providing services like ATM, Debit Cards, Online Payment etc. However, the services provided by cooperative banks are limited when compared with the commercial banks.



Source: RBI

Over the years, UCBs have shown a tremendous growth in the number of branches, size and the volume of business handled but it has seen a decline in the number of banks. In the year 1988, out of 1400 cooperative banks, Reserve Bank of India gave the status of scheduled bank to only 11 cooperative banks of the country and there were 3 cooperative banks who were granted this status in the state of Gujarat. Currently, Gujarat has a share of approximate 14.23% of Urban Cooperative Banks. There are 218 Urban Cooperative Banks in Gujarat, out of which 7 are scheduled cooperative banks and 211 are non-scheduled cooperative banks. The urban cooperative banks can be categorised into two groups Tier I banks and Tier II banks. This classification is based on the depositor base of UCBs. The following UCBs will be classified as Tier I:

- a) A deposit base of less than ₹1 billion operating in a single district, or
- b) b) A deposit base of less than ₹1 billion operating in more than one district, provided that the bank's branches are in contiguous districts and deposits and advances from branches in one district account for at least 95% of total deposits and advances.
- c) Deposit base of less than \$1 billion, with branches that started out in a single district but later became multi-district due to district reorganisation.

All other UCBs are defined as Tier-II UCBs.

All the scheduled UCBs of Gujarat are classified into Tier-II UCBs and can be categorised in Level 3 as per Comprehensive Cyber Security Framework for Urban Cooperative Banks – A Graded Approach. This categorization has been done on the basis of their digital depth and interconnectedness to the payment systems.

- Kalupur Commercial Cooperative Bank is the largest urban cooperative bank of Gujarat. It has total assets worth Rs. 1,09,36,11,62,359. It has total 60 branches and most of them are located in Gujarat. It has 2 branches in Mumbai and 1 in Jodhpur.
- Mehasana Urban Cooperative Bank Limited have total 58 branches out of which 53 branches are in Gujarat and 5 branches are in Maharashtra. The bank has total assets worth Rs. 66,64,56,53,977.
- Ahmedabad Mercantile Cooperative Bank Ltd. have 34 branches in total. It has assets worth Rs. 23,97,36,83,450
- Surat People's Co-Op. Bank Ltd. have 34 branches in total with most of them located in Surat. It has total assets that worth Rs. 58,77,59,70,964.
- Nutan Nagarik Sahakari Bank Ltd. have total 23 branches out of which 21 are in Ahmedabad, 1 is in Surat and 1 in Mumbai (Andheri). It has total assets worth Rs. 19,34,78,87,154.
- Rajkot Nagarik Sahakari Bank Ltd. has total 34 branches out of which 3 are in Mumbai and rest all are in Gujarat. It has total assets worth Rs. 55,42,08,88,156.
- SBPP Co-operative Bank Ltd. has total 11 branches.

### **Major Changes in the Urban Cooperative Banking Sector**

Urban Cooperative Banking Sector has witnessed some major changes in the recent years which will help in strengthening the functioning of the Urban Cooperative Banks. Some of the major changes include:

#### **1. Constitution of Board of Management:**

All the Primary (Urban) Cooperative Banks having deposits size of Rs.100 crores or more are required to constitute a Board of Management (BoM) as this will be the mandatory requirement for the banks who want to open new branches to expand their



area of operations. Urban Cooperative Banks have deposit size less than 100 crores and Salary Earners Banks are exempted from this requirement.

**2. Central Repository of Information on Large Credits (CRILC):**

As per the rules Primary (Urban) Co-operative Banks (UCBs) having total assets of ₹500 crore or more as on 31<sup>st</sup> March of the previous fiscal year needs to report credit information as well as classification of associate account as Special Mention Account (SMA), on all borrowers having aggregate exposures of ₹5 crore or more with them to Central Repository of Information on Large Credits (CRILC) maintained by the central bank of the country.

**3. Modification in Single/Group Borrower Exposure Norms:**

In order to reduce the concentration risk within the exposure of UCBs and additional strengthen the role in promoting monetary inclusion Prudential Exposure Limits for Single and Group Borrower has been revised from existing 15% and 40% of Capital Fund to 15% and 25% of Tier I Capital that is to be achieved by 31<sup>st</sup> March 2023.

**4. Modification in Priority Sector Lending Target:**

Priority Sector Lending Target enhanced from existing 40% of ANBC to 75% of ANBC or CEOBSE (Credit Equivalent of off-balance sheet exposure) which is to be complied by 31<sup>st</sup> March 2024. At least 50% of the loans and advances given by UCB's ought to be loans of not more than Rs.25 Lakh, subject to a maximum Rs.1 crore, per borrower/party.

All the above mentioned changes has been made in order to strengthen the operations of the UCBs or reduce the risk of any frauds or defaulters.

**Introduction to Cyber Security**

Cyber Security refers to the practice and process of protecting computers, networks, servers, system, devices and data from malicious attack, damage or unauthorised access. Nowadays, with the increasing use of technology for smooth business operation, more and more organizations are prone to the risk of cyber-attacks. Organizations transmit data from one device to another, from one network to another in its day to day business operations and in such cases, organization faces the risk of cyber-attacks like the leak of sensitive information to

outsiders, misuse of data by third party etc. Cyber Security helps in protecting these data from such unwanted attacks.

### **Most Common types of Cyber Security Incidents/Attacks**

1. **Phishing**: In phishing attacks, the attacker tries to send some email that appears to be from a known source. The email may seem legitimate and authentic. The email may contain some attachments to open or a link to click. Opening the attachment may install the malware in the computer, thereby having access to personal information.
2. **Malware**: Malware includes some malicious programs that may be inactive scripts or codes, other software, etc. Such objects interrupt system operations, capture sensitive information, and sometimes corrupt critical system files.
3. **Spoofing**: Spoofing is the act of dissimulating a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, websites, or more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server. Spoofing may be accustomed to gain access to a target's personal information, unfold malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack.
4. **Trojan**: It is a type of malware that is often disguised as legitimate software. Cyber-attackers use Trojan to gain access to users' systems. The user might see a pop-up for a fake antivirus program that claims that the computer is infected with some virus and invites the user to run a program to clean it. In reality, the users are downloading a Trojan into their device. Through this, attackers can use the victims' sensitive data and gain backdoor access to their system.
5. **Man-in-the-middle Attack**: Man-in-the-middle (MitM) attacks, additionally referred to as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and purloin the information. There are two common points of ingress for MitM attacks: A) On unsecured public Wi-Fi, attackers can insert themselves between a visitor's device and

the network. The visitor passes all information through the attacker unknowingly. B) Once the malware has breached a device, an attacker can install software to process all of the victim's information.

6. Denial-of-Service (DoS): This type of cyber-attack tries to shut down a machine or server, therefore making it inaccessible to its intended legitimate users. DoS attacks are generally carried either by flooding the service or by crashing the service. Though such attacks do not typically result in the theft or loss of meaningful information or other assets, they can cost the victim a great deal of time and money to handle.

### **Cyber Security Incidents in various Banks of India**

Cosmos Bank Cyber Attack in Pune: On August 11<sup>th</sup> and 13<sup>th</sup> of 2018, Cosmos Bank has faced a malware attack in its servers in Pune, which has led to the cloning of thousands of bank debit cards. In just two days, the hackers managed to withdraw Rs.78 crores from various ATMs across 28 countries and Rs.2.5 crores from multiple ATMS's of India. All these transactions were placed through only Visa Debit Cards outside India and through Rupay Debit Cards in India within a period of just seven hours on August 11<sup>th</sup>, 2018. Not only this, on August 13<sup>th</sup>, 2018, Rs.13.92 crore was transferred to a Hong Kong based entity.

Canara Bank ATM system hacked: In mid-2018, a cyberattack occurred using Canara Bank ATM and Debit Cards. The hackers had wiped off Rs.20 lakhs from 50 different banks accounts. The hackers were having ATM details of around 300 bank accounts.

Yes Bank ATM Security Breach: A significant data breach took place in May and July of 2016 but was discovered in the month of September. Hitachi Payment Services operate most of the ATMs of Yes Bank. This data breach can be attributed to malware found in Hitachi Payment Services' central Switch processors. Due to this data breach, 19 commercial banks were forced to block or recall an estimated 32 lakh debit cards of customers as a precautionary measure.

Union Bank of India Cyber Attack: In July of 2016, Union Bank of India had faced a cyber-attack when an employee of the bank opened an email attachment releasing malware that has helped the hackers steal the bank's data. The hackers had stolen the Union Bank's access codes for the SWIFT transactions. The codes had been used to send transfer requests for about \$171

million to a Union Bank account at Citigroup Inc. in New York. Union Bank of India had traced the money trail and blocked the movement of funds.

### **Cyber Security Trends and Challenges in Banking Industry**

The Information and Communication Technology revolution over the last two decades has changed the way banking services are being availed by the customers. Recently, the Covid-19 pandemic has caused a significant disruption in the traditional way of banking and has quickened the pace of these reforms further. With the shift away from brick and mortar model of banking towards digital platforms, the banks are increasingly investing in new and emerging technologies to better serve their customers and enhance the resilience of their systems and services. Against this backdrop, the various cyber security trends and challenges that have been emerging in banking are discussed below:

- **Use of Artificial Intelligence for Detecting Cyber Security Frauds:**  
Banks are adopting AI for detecting payment frauds, transactions frauds, etc. Banks are working on implementing advanced machine models to detect frauds and minimizing cyber security threats.
- **Blockchain technology can revolutionize the traditional banking:** More and more number of banks are adopting blockchain technology as blockchain can underpin an evolution in RTGS, enhancing the security of digital transactions and minimizing the potential for any errors or frauds. Not only this, distributed ledger technology could allow transactions to be settled directly and keep record of transactions better than existing SWIFT Technology.
- **Identifying and preventing risks in third-party collaboration:**  
Third-party vendors play a vital role in the banking industry. These third-party vendors provide innovative banking technologies and solutions, and banks are adopting such solutions on a large scale. Thus, it becomes imperative for banks to monitor third-party cyber security infrastructure, measures, and policies before any collaboration.
- **Mobile apps will create more security risks:**  
As more and more banks are offering mobile banking services to their customers through apps and payment wallets, the risk of cyber frauds has also increased as mobile phones can be more easily hacked.

- **Heavy Investments in Systems and People:**

To fight against cyber security threats, banks are investing heavily in building infrastructure and creating dedicated teams to look after cyber security risks.

### **Role of Reserve Bank of India in Framing Cyber Security Framework for UCBs**

Reserve Bank of India (RBI) is the regulatory authority that supervise the entire banking sector of the country. In the last five years, Urban Cooperative Banks has seen an increase in the number of frauds. In view of the growing digitization and technology adoption by banks, the banking sector has seen several incidents of cyber-attacks. Nearly 1000 cases of fraud have been recorded that worth Rs.220 crores. In order to minimize such cases, Cyber Security is most important for the banks. By keeping all these in mind, RBI has issued several guidelines for cyber security policy that needs to implemented by banks either by modifying or by restructuring their existing cyber security infrastructure. The move was taken by RBI in order to protect the funds and data (information) of both banks and consumers from any malicious attacks. The banks are responsible for securing consumer information as per guidelines for cyber security policy issued by RBI. The Central Bank aims at strengthening the cyber security infrastructure of banks, so that the banks can adopt the proactive cyber security measures rather than the reactive ones.

### **Cyber Security Framework of RBI for Urban Cooperative Banks**

RBI has issued several guidelines through the Cyber Security Policy for Urban Cooperative Banks (UCB). The cyber security policy mentions that the Information Technology and Information Security should be different from the cyber security policy of UCB by highlighting the risks from cyber threats and the measures to address/reduce these risks. The basic cyber security framework by RBI is mandatory for all the UCB's to implement<sup>1</sup>. Not all UCB operates at same level in terms of size, region, services etc. and that is why RBI has issued some additional guidelines to those UCB's that provide a number of digital services and has high IT penetration. The UCB's has been divided into four levels according to their digital depth and interconnectedness with payments systems<sup>2</sup>. And the UCB's falling under the level 2, 3 & 4 are required to implement some extra measures for cyber security. These additional guidelines aim at strengthening the cyber security of those UCB that may have high risk

---

<sup>1</sup> [Circular DCBS.CO.PCB.Cir.No.1/18.01.000/2018-19 dated October 19, 2018](#)

<sup>2</sup> <https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11772&Mode=0>

exposure due to extensive digitization. In order to minimize the cyber threat on UCB's, RBI has come forward with a new vision for Cyber Security for UCB's. The mission comprises of various action plans like Governance Oversight, Utile Technology Investment, Appropriate Regulation and Supervision, Robust Collaboration and Developing necessary IT, Cyber Security skills set. Timeline for various action plans has also been mentioned<sup>3</sup>.

Salient features of the cyber security policy for urban cooperative banks:

- The cyber security policy of banks should be approved by the Board of the bank and should be different from the Information Technology and Information Security Policy of the bank.
- A minimum baseline cyber security and resilience framework introduced by RBI for urban cooperative banks should be implemented by all the banks regardless of the level under which they fall.
- A special tier wise guidelines have been made in which four different levels of cyber security control has been introduced and UCB's are required to adapt cyber security practices on the basis of their digital interconnectedness.
- UCB's are required to have proper framework for any cyber incident response and management. The banks should share information with RBI if any such incident occurs.
- All UCB's are require to set up Security Operations Center (SOC) and to make arrangements for continuous surveillance to monitor and manage the cyber threats.

### **Comprehensive Cyber Security Framework for Urban Cooperative Banks- A Graded Approach**

- **Baseline Cyber Security and Resilience Requirements:** Banks are required to submit a quarterly report to RBI mentioning any cyber security incident that happened. In case of no such incidents, banks are required to submit report by mentioning nil. This control requires a strong password management policy in all the UCBs. Banks are also required to go for two factor authentication for assessing their Core Banking Solution (CBS) and the devices connected to their CBS.
- **Vendor/Outsourcing Risk Management:** This control requires carefully analysing the third party processes and functions before the selection of the vendor.

---

<sup>3</sup> <https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1159>

- **Network Management and Security:** UCBs are required to maintain a centralised inventory of the authorized devices connected to their network. The network should be able to detect any unusual activity in the server.
- **Application Security Life cycle:** Besides business functionalities, security needs regarding system access management, authentication, dealings authorization, information integrity, system activity work, audit path, session management etc. needed to be clearly specified at the initial and in progress stages of system development/acquisition/implementation. It also requires to make sure that adoption of recent technologies is sufficiently evaluated for existing/evolving security threats which the IT/security team of the UCB come through cheap level of comfort and maturity with such technologies before introducing them for crucial systems of the UCB.
- **Secure Configuration:** This control requires disabling the remote connections from outside machines to the network hosting vital payment infrastructure (Ex: RTGS/NEFT, ATM Switch, SWIFT Interface). Disable Remote Desktop Protocol (RDP) on all vital systems and modifying IP table to limit access to the clients and servers in SWIFT and ATM Switch atmosphere solely to authorised system.
- **Advanced Real-Time Threat Defence and Management:** Build a strong defence against the installation, spread, and execution of malicious code at multiple points within the enterprise by implementing whitelisting of web websites/systems.
- **Maintenance, Monitoring and Systematic Analysis of Audit Logs:** All the stakeholders should be involved before finalising the audit log storage collection. The audit log should be capable of analysing, detecting, responding and recovering from any attack.
- **Incident Response and Management:** UCBs shall have necessary arrangements, together with a documented procedure, with such third party vendor's/service suppliers in case of any incident. This requires having information about any cyber security incident occurring in respect of the bank on timely basis to early mitigate the danger associated.
- **Anti-Phishing:** UCBs are required to buy Anti-phishing/anti-rogue application services from external service providers for distinguishing and taking down phishing websites/rogue applications to protect their data.

- **Data Leak Prevention Strategy:** This control requires UCBs to develop and implement a comprehensive information loss/leakage bar strategy to safeguard sensitive (including confidential) business and client data/information.
- **User/Employee/Management Awareness:** UCBs should build cyber security awareness programs obligatory for brand new recruits and web based quiz and training programs for lower, middle and higher management every year.
- **Risk Based Transaction Monitoring:** This control is applicable to those UCBs who are having their own ATM Switch Interface or Swift Interface. Such banks are required to have continuous monitoring and surveillance process across all their delivery channels.

### **Technology Vision for Cyber Security 2020-2023 for Urban Cooperative Banks**

Reserve Bank of India has released the technology vision for cyber security 2020-2023 in order to strengthen the cyber security practices of UCB's against the upcoming IT and cyber threats. This technology vision has been developed after taking inputs from various stakeholders. To accomplish the technology vision, the mission is established through a five pillared approach named as GUARD., viz., Governance Oversight, Utile Technology Investment, Appropriate Regulation and Supervision, Robust Collaboration and Developing necessary IT, Cyber security skills set.

This technology vision also provides the timeline comprising of details like who needs to take the action and what is the maximum timeframe available to the party.

- **Governance Oversight:**

This action point mentions that the Board is responsible for the cyber security and information security of the Urban Cooperative Banks and thus the regular discussions on cyber security should be part of board meetings. This action is required to be completed by 2020.

Governance Oversight also include the action regarding development of technology vision by UCBs on their own comprising of their plans to inculcate the IT solutions in a safe manner. This action is to be completed by all the UCBs falling in the level 2 – 4 by 2021 and the UCBs falling in level 1 by 2022.



- **Utile Technology Investment:**

As the implementation of cyber security controls involves huge cost, thus UCBs are advised to create a reserve fund out of its net profits for its cyber security measures and practices. This will be completed in two phases and the phase 1 guidelines will be issued by NAFCUB before 2022.

UCBs are required to periodically monitor the lifecycle of its IT Assets so that the risk associated with obsolete hardware and software could be minimized and UCBs can upgrade their IT infrastructure on time. For UCBs falling in level 2 – 4, the action should be taken by 2021 and for level 1 UCBs by 2022.

Due to the Covid-19 pandemic, UCBs have seen major disruptions in their normal functioning and in order to avoid such future disruptions, UCBs are required to come up with Business Continuity Plan (BCP) in order to establish a digitally secured workplace on need basis. This action is to be completed by all the UCBs falling in the level 2 – 4 by 2021 and the UCBs falling in level 1 by 2022.

- **Appropriate Regulation and Supervision:**

In case of any unusual cyber security incident, UCBs are required to report it immediately to RBI apart from the other concerned authorities. And by the year 2021, an offsite supervision for all the UCBs would be conducted in order to monitor their cyber security posture.

A document named as ‘Cyber Security Hygiene’ will be issued to all the UCBs by 2021 by RBI. This document will contain the examples of UCBs with best cyber security practices in different areas. This document could be use by other UCBs as a reference document for implementing their cyber security controls.

- **Robust Collaboration:**

A forum can be set up at State/regional level in which key people from management and other stakeholders may come and discuss some best practices for cyber security controls and any issues or challenges in implementation of such controls. The action will be taken by all federations of UCB by 2021.

CISO Forums could also be set up for UCBs falling in the level 3 and 4 by IBRBT by 2021.

As huge cost is involved in implementation of cyber security controls and thus to make it cost effective, cloud based services can be used for its implementation across all the UCBs.

- **Developing necessary IT, cyber security skills set:**

Various skill oriented certification and training programs regarding cyber security will be designed for staff of the UCBs. Certification programs will also be introduced for board of directors and senior management customised as per their functions and responsibilities.

### **Factors affecting cyber security implementation in Urban Cooperative Banks of Gujarat**

Various factors affecting cyber security implementation can be categorised into three different segments:

- 1. Human Factors:**

Human factors can cause significant threat to cyber security in any organization and the most common threat can arise due to lack of proper communication. Human errors can pose a serious threat to the bank's cyber security. These errors could be accidental or intentional and may arise due to improper risk management, miscommunication or differential thought process. Thus, all UCB's require efficient communication and understanding of risk among all its stakeholders.

- 2. Organizational Factors:**

Organization factors here would be the size of the business of the banks, its structure and the support from the top management to effectively implement and manage the cyber security measures. The transactions are much critical in banks and thus require more resources to be invested for the cyber security measures. And thus, without the support of the top management it would be difficult for the banks to implement the cyber security practices. Not only this, it requires the top management of the UCB's to be qualified enough to handle uncertainties and take strategic actions whenever the need arises. Therefore, this factor plays a major role in deciding upto what level the bank will be able to enforce cyber security practices.

### 3. Technological Factors:

Technological factors play a very major challenge in the cyber security implementation. The complexity of the technology and the prices concerned makes it troublesome for the strategist to take decisions as comparing the cost involved with the risk is quite complicated. Not only this, sometimes complicated networks and systems make it troublesome for security practitioner to adopt security protocols and applications. Moreover, this complexness is simply not a results of innovation in technology however additionally depends on varied alternative environmental factors like size of the bank, business and services offered, open setting, vulnerabilities and IT management distribution. Also, the support from security tools isn't sometimes comfortable to fulfil the protection standards and henceforward have an effect on the implementation of cyber security in the bank.

### 3 layers of Cyber Threat Mitigation and RBI's Comprehensive Cyber Security Framework

Classification of the some of the guidelines issued by RBI in its comprehensive cyber security framework with respect to the three layers of cyber threat mitigation:

- **Threat Prevention**

The comprehensive cyber security framework for primary (urban) cooperative banks – a graded approach dated 31<sup>st</sup> Dec 2019 includes various measures for cyber threat prevention in UCB's. Some of these measures are:

- *Vendor/Outsourcing Risk Management* which includes carefully evaluating the need for outsourcing the critical business processes and selection of vendor/third after thoroughly evaluating the credentials of the parties involved.
- *Real time Network Management and Security* by maintaining an up to date inventory of IT devices connected to the UCB's system.
- *Authentication framework for customers* to secure their transactions.
- *User Access and Control Management* for securing the confidential information regarding UCB's assets and services within/outside the network.

- **Threat Identification**

For identification of threat various measures has been introduced in the comprehensive cyber security framework. Some of these are:

- *Setting up of Cyber Security Operation Centre (C-SOC)* for detecting any threats aligned with the banking technology. C-SOC will also help in detecting, analysing and escalating cyber security incidents.
- Subscribing to *Anti-Phishing* application services for identifying rouge applications.
- *Periodic Testing* for assessing the vulnerability of the web/mobile applications, servers, networks etc.

- **Threat Remedy**

It includes the measures related to minimize the impact the threat.

- Putting effective *Incident Response and Management* practices in order to take corrective actions if any cyber incident happened.
- *Advance Real Time Threat Defence and Management* against the spread and execution of malicious threats.

### **Role of Top Management in Cyber Security Governance in UCBs**

Cyber security is not just a technical issue but it is a management issue as well. Cyber Security in urban cooperative banks depends on the three cornerstones: Infrastructure, Technology and the Bank itself. With the digital banking, customers are more vulnerable to the cyber security scams and leaving cyber security only to the IT function will strengthen only the one cornerstone that is the infrastructure. Cyber security incidents can also arise due to the management failure. Measures to be taken after any such incidents are solely depended on how the top management reacts. And thus, top management of Urban Cooperative Bank plays a very critical role in the designing and implementation of the cyber security measures as per the level in which they fall. The main reason for involving the top management in the cyber security measures is to ensure that the bank's governance is aligned with the cyber security policy issued by the Reserve Bank of India. Not only this, top management will also take care of the efficient use of the resources required for effective implementation. When top management is involved, then the regular maintenance will also be taken care by other employees of the bank. And taking care of the cyber security is ultimately the responsibility of all the employees of the bank, however, when the direction arises from the top management, then it indicates effective leadership.

### **Awareness of Staff and Customers in minimizing Cyber Security Attacks**

Cyber security cannot be fought by CIO's and CISO's alone. It requires active involvement of all the stakeholders including staff and customers. UCB's should educate all his employees and staff to strictly avoid clicking on any links received via email in order to prevent phishing attacks. In order to educate and train the staff, UCB's can create simulation of cyber-attacks so that the staff can understand the threats and losses they are likely to face if any such incident occur. Banks can aware customers regarding the fraud messages and calls claiming for passwords and OTP's.

### **Steps taken by RBI and other regulatory institution for cyber security infrastructure**

- **Issue of regular advisories and alerts:**

RBI has issued various circulars to strengthen the cyber security infrastructure of UCB's. Not only this, various improvements have been made in the existing cyber security framework for urban cooperative banks. The updated framework will help in implementation of progressively stronger security measures based on the nature, variety and scale of digital product offerings of banks.

- **Umbrella organization for UCB's:**

RBI has been working for the formation of umbrella organization that will look after the capital requirements and IT infrastructure of UCB's. It will also help the UCB's in improving their liquidity and transparency.

- **Setting Up of Working group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds:**

A working group on information security, electronic banking, technology risk management, and cyber frauds was set up in April 2010 under the chairmanship of then Executive Director G. Gopalakrishna. The group had examined various issues arising out of the use of Information Technology in banks and made its recommendations in nine broad areas. These areas are IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programs, and Legal aspects way back in April 2011. This working group was also responsible for undertaking a comprehensive assessment of IT and E-banking-related guidelines, providing recommendations concerning information

security, business continuity, and information systems audit and also help in the evaluation of the impact of legal risk arising out of cyber laws.

- **Setting Up of Cyber Security and Information Technology Examination (CSITE)**

**Cell:**

RBI has set up a CSITE Cell in the Department of Supervision in the year 2015. This cell carries out thematic studies on various cyber security issues. CSITE Cell has been continuously interacting with ReBIT, CERT-In and various government entities and industry experts to evolve coordinated approach in strengthening cyber ecosystem in banks. All the banks are required to report all the unusual cyber security incidents within 2-6 hours of detection to CSITE Cell through an online platform devised for the purpose.

- **CERT – In:**

The Indian Computer Emergency Response Team (CERT – In) has taken several measures to strengthen the cyber security practices and cyber resilience among the UCB's. Various measures include cyber security exercises/drills, sharing tailored advisories with the CISO community, establishment of Financial Sector Computer Security Incident Response Team (CSIRT – Fin) etc.

- **National Level Advertisement Campaign like RBI Kehta Hai:**

RBI has introduced national level advertisement campaign like RBI Kehta Hai to educate its customers regarding the setting up limit in their cards in order to safeguard customers against any frauds etc.

### **Importance of Cyber Security infrastructure in Urban Cooperative Banks after the Covid 19 scenario**

A robust cyber security infrastructure will help the UCB's in the following ways:

- 1. Better Customer on boarding process:**

With sufficient cyber security infrastructure, the chances of cyber-attacks will be less and this will help the UCB's in better customer on boarding for various digital banking

services. With this, customers can avail some of the banking services from the comfort of their home.

## **2. Reduction in customers' footfalls at banks:**

Due to the Covid 19 pandemic, people are moving towards cashless transactions. And when the customers will know that UCB's are having better online services which are not prone to any attacks, the customers' footfalls at bank will be reduced as now they can avail services without actually going to the bank for example online money transfers, payments, withdrawals through ATM's etc.

## **3. Reduction in other costs to banks:**

The resources required in cyber security infrastructure should be considered as an investment as it will help the banks in reduction of other costs that may arise due to the frauds or scams.

### **Challenges faced by Urban Cooperative Banks due to Covid 19**

The Covid-19 pandemic and the lockdown due to it has already shown adverse effect on the economy and it can also be seen in the current situation of the loans given by Urban cooperative Banks. Micro, Small and Medium Enterprises (MSME) got most of their loans from Urban Cooperative Banks and due to the Covid 19 most of the loans were under moratorium. Even though the MSME Companies are considered as being with less risk however the share of missed payments of loans has jumped from approximately 9% in March 2020 to 25% in June 2020. If we considered the companies with the highest risk, then the share of missed payments of loans has been more than tripled from 11% to 36% between the same period.

UCBs are facing stiff competition from Small Finance Banks, NBFC etc. as they provide high interest on deposits as compared to UCBs and this has been the reason why they have survived the Covid-19 comparatively better than UCBs. Many UCBs has also face the problem of small capital base. Not only this, due to the Covid-19 disruption, financial position of urban cooperative banks is very weak and many of them had reported loss. Some of the UCBs are unable to meet the minimum regulatory capital requirements.

And in such a scenario, investing in cyber security infrastructure by Urban Cooperative Banks seems challenging.

## Analysis and Discussion

Through telephonic interviews with CISO officers, I have identified the following challenges that has been faced by urban cooperative banks of Gujarat in implementing or upgrading their cyber security infrastructure:

**1. Inadequate Budgets due to their small size:**

Urban Cooperative banks are smaller in size having very limited branches in specific locations. Their services are also limited to those areas and that is why it becomes difficult for such banks to implement robust cyber security infrastructure as such banks suffers from lack of funds and installing cyber security measures may seem costly to banks.

**2. High cost of cyber security compliance:**

Cyber Security infrastructure is not only costly to install but its regular maintenance and supervision is also costly. Due to this reason, many urban cooperative banks are not able to implement the measures as they are not having enough resources for the cyber security compliance.

**3. Unavailability of tech savvy clientele in small towns:**

Urban Cooperative banks are located more in semi-urban areas and small towns. Availability of tech savvy customers in such towns are rare. And sometimes this become another barrier in the implementation and upgradation of cyber security infrastructure of such banks and this left the customers in a situation which is more vulnerable to frauds and scams.

**4. Lack of skilled manpower for operations:**

Cyber security infrastructure requires skilled manpower for regular supervision, so that they can identify threats if any and take corrective actions. However, the availability of skilled manpower who are familiar with robust information and technology software are very less.

**5. Low awareness among employees:**

The awareness regarding the cyber security measures remains very low in urban cooperative banks. Employees are not aware about the risks and the cyber threats. And not only this, sometimes the top management also do not want to invest in the training of their employees. And due to this reason they are not upgrading their existing cyber security infrastructure.



## Findings

The progress on cyber security practices in UCBs of Gujarat was known through the telephonic interviews with CISO. The findings were as follows:

### **Implementation of Technology Vision for Cyber Security in UCBs of Gujarat**

As all the scheduled UCBs of Gujarat falls in level 3 on the basis of their digital depth, so the actions mentioned in Technology Vision document needs to completed by UCBs by the year 2021. The following points shows the progress of the actions:

- **IT Vision Document:**

All the scheduled cooperative banks of Gujarat have prepared their own IT vision document that highlights their plans to incorporate IT solutions into businesses. UCBs have also got it approved from their Board. Timeline has also been mentioned for the actions and the banks also have a mechanism of periodically reviewing their vision document and reflect changes when required. Until now, for most of the UCBs two reviews has already been completed.

- **Management of Business IT Assets:**

Management of IT Assets have been a regular thing for all scheduled urban cooperative banks. They also reviewing their IT assets periodically and upgrading them from time to time so that the bank's infrastructure is not exposed to risk due to hardware or software obsolescence. And this action has been completed by all the UCBs of Gujarat.

- **Banking Services Availability:**

Many UCBs have their Business Continuity Plan way before this technology vision document was introduced. UCBs also conduct their business continuity check periodically.

All the actions from the part of the UCBs are completed. Rest other actions are to be done by RBI or the Federation of UCBs.

### **Implementation of Comprehensive Cyber Security Framework in UCBs of Gujarat**

The UCBs of Gujarat has already put various cyber security controls into its routine operations. The UCBs of Gujarat fall under Level III, however many of the UCBs have also tried to implement some Level IV controls like setting up of security operation centre for better management of the banks' and customers' security. The progress on these cyber security controls are:

- **Baseline Cyber Security and Resilience Requirements:** Under this control banks are required to go for two factor authentication of their CBS. Bigger scheduled urban cooperative banks are able to implement this two factor authentication but smaller banks are unable to implement this as such banks are not much cyber security acquainted and in Gujarat there is scarcity of professionals on cyber security and this is also the reason why many banks are outsourcing most of their cyber security services and outsourcing professionals from agencies who will take care of these requirements.
- **Anti-Phishing:** It includes two parts, one is the protection from phishing mails and the other one is protection from phishing websites and applications. Most of the UCBs of Gujarat have completed the first part that is protection of phishing mails however, the second part is still in process by all the UCBs as this require capital outlay of around 1 crore to 1.5 crore every year and being a small bank it becomes difficult for them to invest this huge amount every year. Most of the UCBs are working together on this control.
- **Risk Based Transaction Monitoring:** Only a few UCBs are having their own ATM Switch Interface or Swift Interface as it is very expensive and now this demands continuous monitoring and surveillance which is very difficult for the banks to implement and thus till now only one UCB is able to implement this control.
- **User/Employee/Management Awareness:** All the UCBs of Gujarat are trying hard to educate their employees and management. Many of the UCBs have put a number of efforts like conducting online sessions, periodically mail to vendors and customers, educating them via calendars, posters and banners inside banks' branches and ATMs etc.
- **Application Security Life Cycle:** There is very few in house developments of applications by UCBs as most of them have procured applications through third party. And in such case the third party is taking care of life cycle of application security and there is minimal involvement of bank in this respect.
- **Real-Time Threat Defence and Management:** The real-time threat defence and management requires continuous monitoring and surveillance of any threat of malicious code at multiple points. Most of the UCBs are conducting periodic surveillance as real time surveillance is not economically feasible option for them.

Rest all the cyber security controls have been implemented by all the UCBs of Gujarat.

## Best Cyber Security Practices in UCBs of Gujarat

Some of the best cyber security practices that have been identified are:

- **Periodic Testing:** Periodic Testing of web/mobile applications, networks, servers etc. will help in identification of malicious threat if any. If any vulnerabilities are detected, then these can be rectified at the earliest by keeping in mind the risk management and treatment framework of UCBs. Not only this, periodic testing should also be conducted at the time when any changes or updates have been introduced in the web/applications.
- **User/Employee and Management Awareness:** Management awareness regarding cyber security is the first step for better implementation of the cyber security infrastructure. When employees are educated and aware about the damages that may incur due to cyber-attacks, they will try to focus on the protection of IT assets of bank and consumers' information.
- **Data Leak Prevention Strategy:** All the UCBs should have a comprehensive data leak and prevention strategy in order to secure consumer's sensitive information. If most of the services provided by UCBs are through third party, then the vendor should also take care of the consumers' data and should have a robust data leak and prevention strategy.
- **Board Approved Cyber Security Policy:** The cyber security policy of UCBs should be approved by the Board/Administration. The board is responsible to check whether the controls put in plan are able to secure the complex data and should be align with the banks' business risks.

## Suggestions and Recommendations

The following suggestions will help the UCBs in better implementation of the cyber security practices:

- **Consolidation of Small and Weak UCB's:**  
Despite being the large number of UCBs, there are many UCBs which are single branch entities having limited ways to raise capital and some of the UCBs are also having negative net worth. In such scenario, a better way forward will be the merger of small and weak UCBs with some strong UCB having sufficient number of branches so that the stressed out assets of such small UCBs can be reduced and their functioning can be improved. No doubt that Reserve Bank of India Vision Document 2005, talks about the

mergers of weak UCB with the strong ones but still there is need for more such mergers as Covid-19 pandemic has shaken the normal functioning of many UCBs.

- **Awareness Programmes for UCB's by RBI and other associated bodies:**

The National Federation of Urban Cooperative Banks and Credit Societies Ltd. (NAFCUB) can organise some activities and training programmes for UCBs regarding the need and importance for cyber security practices. The awareness programmes could include the examples of other UCBs who has successfully implemented the required cyber security measures. RBI can design other awareness programmes or campaigns just like RBI Kehta Hai.

- **Awareness Programmes by UCB's for their staff and customers:**

Reserve Bank of India has its own training institutes which can be used for imparting training to the employees specific to their domain and functionality. Not only this, various awareness programmes can also be introduced for making the customers aware about the cyber-crimes and educating them to not disclose any confidential banking information to the unknowns. The cyber security awareness among customers and staff will help in reducing the impact of cyber-attacks and will improve the cyber security preparedness of UCBs.

- **Strict Implementation of Cyber Security Controls:**

With the introduction of various cyber security measures for UCBs by Reserve Bank of India, a way for better functioning of UCB will be possible when the cyber security practices will be in stricter implementation. Regulator should introduce new bodies who will help UCBs to implement these cyber security control in a better way. And this will require penalising the banks in future if it fails to upgrade their cyber security infrastructure with the minimum practices as mentioned.

- **Assessment of cyber security infrastructure and controls by empanelled IS auditors along the lines of statutory auditors:**

Just like statutory auditor is legally required to assess the financial statements of the bank, similarly RBI can have made it mandatory for UCB's to appoint Information Security Auditor who will be responsible for analysing and assessing the cyber security infrastructure of the bank. This will also ensure stricter implementation of cyber security practices by banks and thus helping RBI to ensure better implementation of its technology vision for cyber security.

- **Financial help to UCBs for implementation of some important cyber security controls:**

RBI with the help of other agencies like CERT-IN or NAFCUB should help smaller banks with their cyber security infrastructure. Some of the cyber security controls like Anti-Phishing, Baseline Cyber Security and Resilience Requirements etc. require huge capital outlay and which is sometimes more than the banks' actual revenue and thus smaller banks can't comply with such controls. RBI should guide them in this respect either by providing some services at free of cost.

- **Direct Involvement of Board Members in Cyber Security:**

UCBs are facing the problem of convincing Board Members for fund allocation in various cyber security controls. Board Members hesitate to allocate funds to IT department as they feel that this department incurs only cost and there is no revenue generation from the department. In such instances, if RBI is directly involved with the Board Members then the cyber security controls might have been easily approved by the Board Members.

---

## *Part C: Learnings from the Project*

---

My summer internship with the Reserve Bank of India provided me with both tangible and intangible takeaways that I would carry with me in the corporate world. It has given me real time experience of the corporate world and taught me how to deal professionally.

With this research project, I was able to put my learnings from the Business Research Methodology subject into real world. During the course I learnt about the problem formulation, methods of data collection, methods of sampling etc. and through this summer internship I learnt how these can be used in the corporate world.

In this research project, I learned how to build the topic that was assigned to me and how to conduct rigorous and in depth study about the topic. While starting with the research I was having a lot of data pool available to me and thus it becomes imperative to segregate the important data from the trivial ones. In order to make the report authentic, the sources of data play an important role and thus it helped me in narrowing down the sources of data to only the credible ones which I will be referring for the research.

The topic assigned to me was *A Study on Cyber Security Policy for Urban Cooperative Banks of Gujarat*. I have learnt about cyber security in the subject Management Information System and its importance in different sectors. With this research I was able to explore and gain understanding regarding the cyber security with respect to urban cooperative banks. While referring to various articles and documents, I have come across a number of business and management related terminologies in various context.

During the telephonic interviews with CISO officers, I gain insights about working of urban cooperative banks, learnt about their cyber security infrastructure and how they changed their existing infrastructure in order to comply with the RBI guidelines.

During my internship, I have learnt about the working of Urban Cooperative Banks and role of various regulatory authorities in the functioning of such banks. While working with department of supervision, I learned about various models of banking performance evaluation and one such is CAMELS model. The CAMELS acronym stands for Capital Adequacy, Asset quality, Management, Earnings, Liquidity and sensitivity. I have also gain insights about the impact of Covid-19 on deposits, loans and NPAs of Urban Cooperative Banks. I have also learnt about the need for cyber security infrastructure and some best practices in the sector.

Apart from these, the summer internship has also helped me to develop and enhance my interpersonal skills. Through conference and video calls with mentors and supervisors, it has helped me to develop the corporate communication skills.

At last, this summer internship opportunity has given me a sense of accomplishment and has boost my confidence. This experience will remain life-long as it has prepared me for a job.

## Annexure – A

### RBI's guidelines to the Urban Cooperative Banks with respect to Cyber Security

Sr. No.	Date	Type	Title
1.	Sept 24, 2020	Reports	'Technology Vision For Cyber Security' For Urban Cooperative Banks- 2020-2023
2.	Dec 31, 2019	Notifications	Comprehensive Cyber Security Framework For Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach
3.	Dec 31, 2019	Notifications	Cyber Security Controls for Third Party ATM Switch Application Service Providers
4.	Oct 19, 2018	Notifications	Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs)



## **Annexure – B**

### **List of Scheduled Urban Cooperative Banks of Gujarat whose Annual Reports has been referred<sup>4</sup>**

<b>Sr. No.</b>	<b>Name of Bank</b>
1.	Ahmedabad Mercantile Co-Op Bank Ltd.
2.	Kalupur Commercial Coop. Bank Ltd.
3.	Mehsana Urban Co-Op Bank Ltd.
4.	Nutan Nagarik Sahakari Bank Ltd., Ahmedabad
5.	Rajkot Nagrik Sahakari Bank Ltd.
6.	SBPP Co-operative Bank Ltd., Killa Pardi, Dist Valsad (Gujarat)
7.	Surat Peoples Coop Bank Ltd.

---

<sup>4</sup> Annual Reports for the financial year 2019-20 has been referred to study about the major developments that has been made in the Co-operative Banking Sector. The annual reports have been retrieved from the official website of the above mentioned banks.

## Annexure – C

### Questionnaire used for the Telephonic Interview

1. Do you know about the cyber security framework for urban cooperative banks? Your bank falls under which level of controls as per the comprehensive cyber security framework?
2. Is your bank has implemented the same? Please give brief description about the controls that has been implemented by your bank.
3. Do you know about the technology vision for cyber security for urban cooperative bank that has been issued by Reserve Bank of India? How has your bank taken this vision statement forward?
4. Did your bank's staff possessed enough skills to implement the about the cyber security practices or were they given training before any controls could be implemented?
5. What is your bank's average annual expenditure on cyber security infrastructure? Do you find this expenditure reasonable?
6. Do you find any relationship between implementation of cyber security practices and smooth functioning of the bank?
7. Do you find any negative impact of cyber security infrastructure on banks?
8. What are your views on mergers of small UCBs with the larger UCBs?

## Bibliography

*Challenges in Cyber Security in Banking.* (2020, November). Retrieved from Deloitte:

<https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-cybersecurity-in-the-indian-banking-industry-noexp.pdf>

*Cyber Security.* (2020, November 17). Retrieved from Edureka:

<https://www.edureka.co/blog/what-is-cybersecurity/>

*Cyber Security in Bnking and Financial Services Sector.* (2018, March 26). Retrieved from Stoodnt:

<https://www.stoodnt.com/blog/cybersecurity-in-banking-financial-services/>

*Developments in Co-operative Banking.* (2019, December 24). Retrieved from Reserve Bank of India:

Developments in Co-operative Banking

D'Souza, R. (2019, October 10). *Observer Research Foundation.* Retrieved from

<https://www.orfonline.org/expert-speak/demise-urban-cooperative-banks-around-corner-56421/>

Lele, A. R. (2019, Dec 31). Retrieved from Business Today: [https://www.business-](https://www.business-standard.com/article/economy-policy/rbi-wants-urban-cooperative-banks-to-focus-mainly-on-priority-sector-119123001276_1.html)

[standard.com/article/economy-policy/rbi-wants-urban-cooperative-banks-to-focus-mainly-on-priority-sector-119123001276\\_1.html](https://www.business-standard.com/article/economy-policy/rbi-wants-urban-cooperative-banks-to-focus-mainly-on-priority-sector-119123001276_1.html)

Mohanty, P. (2019, Nov 21). Retrieved from Business Today:

<https://www.businesstoday.in/industry/banks/story/urban-cooperative-banks-poor-governance-makes-ucbs-vulnerable-to-npas-non-performing-assets-pmc-bank-fraud-240065-2019-11-21>

*Reserve Bank of India - Annual Reports.* (2021, May 27). Retrieved from Reserve Bank of India:

<https://rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1319>

*Reserve Bank of India - Functional .* (n.d.). Retrieved from Reserve Bank of India:

[https://www.rbi.org.in/scripts/fun\\_urban.aspx](https://www.rbi.org.in/scripts/fun_urban.aspx)

*Reserve Bank of India - Notifications.* (2009, Jan 30). Retrieved from Reserve Bank of India:

<https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=4806&Mode=0>

*Reserve Bank of India - Notifications.* (2018, October 19). Retrieved from Reserve Bank of India:

<https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11397>

*Reserve Bank of India - Notifications.* (2019, December 31). Retrieved from Reserve Bank of India:

<https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11772>

*Reserve Bank of India - Press Releases.* (2019, December 31). Retrieved from Reserve Bank of India:

[https://rbi.org.in/scripts/BS\\_PressReleaseDisplay.aspx?prid=49017](https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=49017)

*Reserve Bank of India - Publications.* (2019, December 24). Retrieved from Reserve Bank of India:

<https://rbi.org.in/scripts/PublicationsView.aspx?Id=19366>

*Reserve Bank of India - Reports.* (2020, September 24). Retrieved from Reserve Bank of India:

<https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1159>

*Reserve Bank of India.* (2021, January 11). Retrieved from Reserve Bank of India Website:

<https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1169>

Sharma, S. (2019, Dec 19). Retrieved from Mumbai Mirror:

<https://mumbaimirror.indiatimes.com/mumbai/other/breach-of-data-led-to-loss-of-rs-29-cr-says-top-co-op-bank/articleshow/72800070.cms>

Srivastava, A. (2021, Jan 27). Retrieved from Outlook:

<https://www.outlookindia.com/newscroll/urban-cooperative-banks-report-nearly-1000-frauds-worth-over-rs-220-cr-in-past-five-fiscals-rbi/1718645>