International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

Transformative Waves: Impact of Information Technology on Operations of Commercial Banks in India

Rizwana Begum[1], Dr. Asiya Jabeen[2], Tabassum Begum[3], Taiyaba Khanam[4], Tampa Sowmya Guna[5], Tankari Deepika[6]

[1]Lecturer, IPGDCW (A), Nampally, Hyderabad, Telangana, India.

[2]Assistant Professor, IPGDCW (A), Nampally, Hyderabad, Telangana, India.

[3, 4, 4, 5] Student, IPGDCW (A), Nampally, Hyderabad, Telangana, India.

Abstract

This research abstract provides a glimpse into a study focused on investigating the profound impact of Information Technology (IT) on the operations of commercial banks in India. Employing a mixed-methods approach, incorporating qualitative insights and quantitative analyses, this study aims to explore the multifaceted dimensions of IT integration, its challenges, and the resultant transformation in the operational landscape of Indian commercial banks. The qualitative aspect of the study involves interviews, case studies, and expert opinions to capture nuanced perspectives on how IT adoption has reshaped banking operations in India. Simultaneously, quantitative data will be analyzed to identify trends, correlations, and statistical patterns associated with the impact of IT on key operational metrics. Various dimensions of the impact of IT on banking operations will be investigated, including enhanced efficiency through automation, the evolution of digital banking channels, cybersecurity challenges, and the overall influence on customer experience. The study aims to provide insights into the strategic implications of IT integration for commercial banks in India. The findings from this research are anticipated to offer valuable insights for banking professionals, IT experts, policymakers, and decision-makers. By understanding the multifaceted impact of IT on operations, stakeholders can formulate strategies to harness technological advancements, address challenges, and contribute to the ongoing digital transformation of the banking sector in India. This study serves as a foundation for informed decision-making and future research within the realm of its impact on the operations of commercial banks.

Keywords: *Information Technology, Commercial Banks, Operational Transformation, Digital Banking, Financial Technology, IT Integration, Cybersecurity, Efficiency, Customer Experience.*

1. Introduction

1.1 Role of Information Technology in Banking Sector

The term “Information technology” refers to the use of sophisticated information and communication technologies together with computer science to enable banks to offer better services to its customers in a secure, reliable, and affordable manner, and sustain competitive advantage over other banks. Banking technology also subsumes the activity of using advanced computer algorithms in unraveling the patterns of customer behavior by sifting through Customer details such as demographic, Psychographic, and transactional data. The banks in India are using Information Technology (IT) not only to improve their own internal processes but also to increase facilities and services to their customers. Banks today have become synonymous with technology and have leveraged IT in all areas of governance, operations and control. Effectively use of Technology has facilitated accurate and timely management of the increased volume of banks that comes with a larger customer base.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

The banking sector is the most dominant sector of the financial system in India. Significant progress has been made with respect to the banking sector in the post liberalization period [1]. The financial health of the commercial banks has improved manifolds with respect to capital adequacy, profitability, and asset quality and risk management. Further, deregulation has opened new opportunities for banks to increase revenue by diversifying into investment banking, insurance, credit cards, depository services, mortgage, securitization, etc. Liberalization has created a more competitive environment in the banking sector. During the recent years, the pace and quality of banking was changed by the technological advancements made in this area. Computerization as well as the adoption of core banking solution was one of the major steps in improving the efficiency of banking services. The process of computerization of the banking sector continued [2].

1.2 Evolution of Banking

Despite the enormous changes the banking industry has undergone through during the past20 years let alone since 1943one factor has remained the same: the fundamental nature of the need customers has for banking services. However, the framework and paradigm within which these services are delivered has changed out of recognition. It is clear that people's needs have not changed, and neither has the basic nature of banking services people require. But the way banks meet those needs is completely different today. They are simply striving to provide a service at a profit. Banking had to adjust to the changing needs of societies, where people not only regard bank account as a right rather than a privilege, but also are aware that their business is valuable to the bank, and if the bank does not look after them, they can take their business elsewhere (Engler & Eslinger, 2000). Indeed, technological and regulatory changes have influenced the banking industry during the past 20 years so much so that they are the most important changes to have occurred in the banking industry, apart from the ones directly caused by the changing nature of the society itself. In this book, technology is used interchangeably with information and communication technologies together with computer science [3]. The relationship between banking and technology is such that nowadays it is almost impossible to think of the former without the latter. Technology is as much part of the banking industry today as a ship's engine is part of the ship. Thus, like an engine, technology drives the whole thing forward (Engler &Eslinger, 2000). Technology in banking ceased being simply a convenient tool for automating processes. Today banks use technology as a revolutionary means of delivering services to customers by designing new delivery channels and payment systems. For example, in the case of ATMs, people realized that it was a wrong approach to provide the service as an additional convenience for privileged and wealthy customers [4]. It should be offered to the people who find it difficult to visit the bank branch. Further, the cost of delivering the services through these channels is also less. Banks then went on to create collaborative ATM networks to cut the capital costs of establishing ATM networks, to offer services to customers at convenient locations under a unified banner (Engler &Eslinger, 2000). People interact with banks to obtain access to money and payment systems they need. Banks, in fact, offer only what might be termed as a secondary level of utility to customers, meaning that customers use the money access that banks provide as a means of buying the things they really want from retailers who offer them a primary level of utility. Customers, therefore, naturally want to get the interaction with their bank over as quickly as possible and then get on with doing something they really want to do or with buying something they really want to buy. That explains why new types of delivery channels that allow rapid, convenient, accurate delivery of banking services to customers are so popular. Nowadays, customers enjoy the fact that their banking chores are done quickly and easily (Engler &Eslinger, 2000). The kind of enormous and far-reaching developments discussed above have taken place along with the blurring of demarcations between different types of banking and financial

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

industry Activities [5]. Banking Evolution are shown in Figure 1.

1. Governments have implemented philosophies and policies based on an increase in competition in order to maximize efficiency. This has resulted in the creation of large new financial institutions that operate simultaneously in several financial sectors such as retail, wholesale, insurance, and asset management.
2. New technology creates an infrastructure allowing a player to carry out a wide range of banking and financial services, again simultaneously.
3. Banks had to respond to the increased prosperity of their customers and to customers 'desire to get the best deal possible. This has encouraged banks to extend their activities into other areas.
4. Banks had to develop products and extend their services to accommodate the fact that their customers are now far more mobile. Therefore, demarcations are breaking down.
5. Banks have every motivation to move intonew sectors of activity in order to try to deal with the problem that, if they only offer banking services, they are condemned banks realized the convenience of ATMs, new services started to be added.

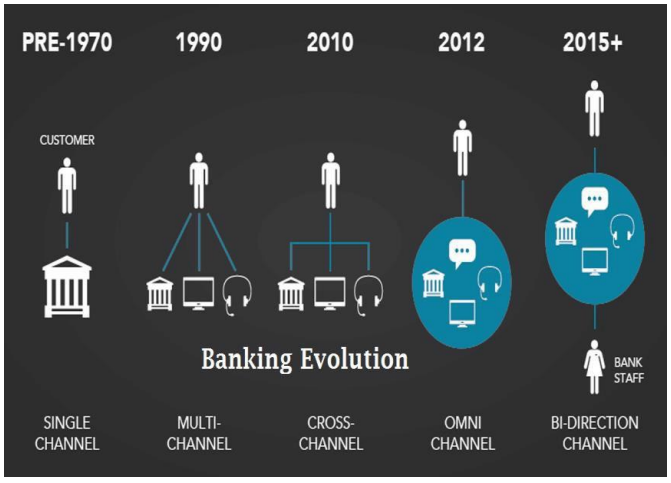

Figure 1 Banking Evolution

2. Online Banking

Online banking, also known as internet banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website [6]. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services. Some banks operate as a "direct bank" (or "virtual bank"), where they rely completely on internet banking [7]. Internet banking software provides personal and corporate banking services offering features such as viewing account balances, obtaining statements, checking recent transaction and making payments. Access is usually through a secure web site using a username and password, but security is a key consideration in internet banking and many banks also offer two factor authentications using a (security token). Online Banking are shown in Figure 2.

2.1 Operations

To access a financial institution's online banking facility, a customer with internet access will need to register with the institution for the service, and set up a password and other credentials for customer verification. The credentials for online banking is normally not the same as for telephone or mobile banking. Financial institutions now routinely allocate customers numbers, whether or not customers have indicated an intention to access their online banking facility. Customer numbers are normally not the same as account numbers, because a number of customer accounts can be linked to the one customer number [8]. Technically, the customer number can be linked to any account with the financial institution that the customer controls, though the financial institution may limit the range of accounts that may be accessed to, say, cheque, savings, loan, credit card and similar accounts. The customer visits the financial institution's secure website, and enters the online banking facility using the customer number and credentials previously set up. Each financial institution can determine the types of financial transactions which a customer may transact through online banking, but usually includes obtaining account balances, a list of recent

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

transactions, electronic bill payments, financing loans and funds transfers between a customer's or another's accounts. Most banks set limits on the amounts that may be transacted, and other restrictions. Most banks also enable customers to download copies of bank statements, which can be printed at the customer's premises (some banks charge a fee for mailing hard copies of bank statements). Some banks also enable customers to download transactions directly into the customer's accounting software. The facility may also enable the customer to order a cheque book, statements, report loss of credit cards, stop payment on a cheque, advice change of address and other routine actions [9].

2.2 Features

Online banking facilities typically have many features and capabilities in common, but also have some that are application specific. The common features fall broadly into several categories:

1. A bank customer can perform non-transactional tasks through online banking, including:
   - Viewing account balances
   - Viewing recent transactions
   - Downloading bank statements, for example in PDF format
   - Viewing images of paid cheques
   - Ordering cheque books
   - Download periodic account statements
   - Downloading applications for M-banking, E-banking etc.
2. Bank customers can transact banking tasks through online banking, including:
   - Funds transfers between the customer's linked accounts
   - Paying third parties, including bill payments (see, e.g., BPAY) and third party fund transfers (see, e.g., FAST)
   - Investment purchase or sale
   - Loan applications and transactions, such as repayments of enrollments
   - Credit card applications
   - Register utility billers and make bill payments
3. Financial institution administration
4. Management of multiple users having varying levels of authority
5. Transaction approval process

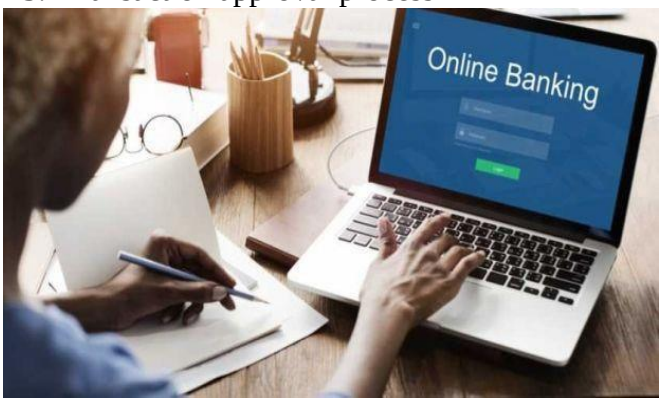

Figure 2 Online Banking

2.3 Security

Security of a customer's financial information is very important, without which online banking could not operate. Similarly, the reputational risks to banks themselves are important. Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is no consistency to the various approaches adopted [10]. The use of a secure website has been almost universally embraced. Though single password authentication is still in use, it by itself is not considered secure enough for online banking in some countries. Basically, there are two different security methods in use for online banking: Security image shown in Figure 3.

- The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions. TANs can be distributed in different ways; the most popular one is to send a list of TANs to the online banking user by postal letter. Another way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token (two-factor authentication or 2FA).
- More advanced TAN generators (chip TAN) also include the transaction data into the TAN generation process after displaying it on their

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

own screen to allow the user to discover man-in-the-middle attacks carried out by Trojans trying to secretly manipulate the transaction data in the background of the PC.

- Another way to provide TANs to an online banking user is to send the TAN of the current bank transaction to the user's (GSM) mobile phone via SMS. The SMS text usually quotes the transaction amount and details; the TAN is only valid for a short period of time. Especially in Germany, Austria and the Netherlands many banks have adopted this "SMS TAN" service.
- Usually online banking with PIN/TAN is done via a web browser using SSL secured connections, so that there is no additional encryption needed.
- Signature based online banking where all transactions are signed and encrypted digitally. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium.

Figure 3 Security

2.4 Attacks

Attacks on online banking used today are based on deceiving the user to steal login data and valid TANs. Two well-known examples for those attacks are phishing and pharming. Cross-site scripting and key logger/Trojan horses can also be used to steal login information. A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background. A 2008 U.S. Federal Deposit Insurance Corporation Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of $30,000. That adds up to a nearly $16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second. In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states. Another kind of attack is the so-called man-in-the-browser attack, a variation of the man-in- the-middle attack where a Trojan horse permits a remote attacker to secretly modify the destination account number and also the amount in the web browser. As a reaction to advanced security processes allowing the user to cross-check the transaction data on a secure device there are also combined attacks using malware and social engineering to persuade the user himself to transfer money to the fraudsters on the ground of false claims (like the claim the bank would require a "test transfer" or the claim a company had falsely transferred money to the user's account and he should "send it back").Users should therefore never perform bank transfers they have not initiated themselves [11].

2.5 Countermeasure

There exist several countermeasures which try to avoid attacks. Digital certificates are used against phishing and pharming, in signature based online banking variants (HBCI/FinTS) the use of "Decoder" card readers is a measurement to uncover software side manipulations of the transaction data. In 2001, the U.S. Federal Financial Institutions Examination Council issued guidance for multifactor authentication (MFA) and then required to be in place by the end of 2006. In 2012, the European Union Agency for Network and Information Security advised all banks to consider the PC systems of their users being infected by malware by default and therefore use security processes where the user can cross-check the transaction data against manipulations like for example (provided the security of the mobile phone holds up) SMS TAN where the transaction data is sent along with the TAN number or standalone smartcard readers with an own screen including the transaction data into the TAN generation process while displaying it beforehand to the user (see chip TAN) to counter man-in-the-middle attacks [12].

3. Mobile Banking

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. Unlike the related internet banking it uses software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted. Mobile banking is dependent on the availability of an internet or data connection to the mobile device. Transactions through mobile banking depend on the features of the mobile banking app provided and typically includes obtaining account balances and lists of latest transactions, electronic bill payments, remote check deposits, P2P payments, and funds transfers between a customer's or another's accounts Some apps also enable copies of statements to be downloaded and sometimes printed at the customer's premises. From the bank's point of view, mobile banking reduces the cost of handling transactions by reducing the need for customers to visit a bank branch for non-cash withdrawal and deposit transactions. Mobile banking does not handle transactions involving cash, and a customer needs to visit an ATM or bank branch for cash withdrawals or deposits [13]. Many apps now have a remote deposit option; using the device's camera to digitally transmit cheques to their financial institution. Mobile banking differs from mobile payments, which involves the use of a mobile device to pay for goods or services at the point of sale or remotely, analogously to the use of a debit or credit card to affect an EFTPOS payment. Mobile Banking refers to provision and availability of banking- and financial services with the help of mobile telecommunication devices. The scope of offered services may include facilities to conduct bank and stock market transactions, to administer accounts and to access customized information."

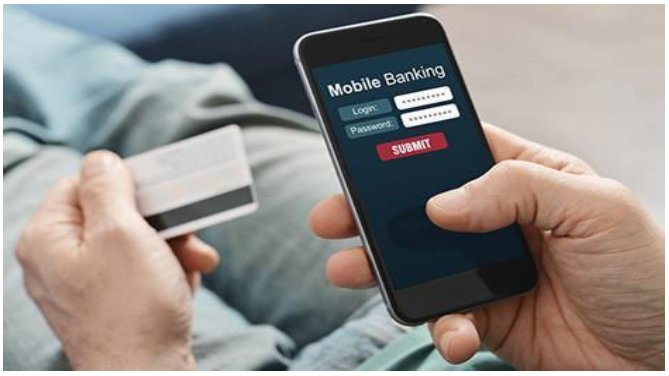

Figure 4 Mobile Banking

According to this model mobile banking can be said to consist of three inter-related concepts:

- Mobile accounting
- Mobile brokerage
- Mobile financial information services

Most services in the categories designated accounting and brokerage are transaction-based. The non-transaction-based services of an informational nature are however essential for conducting transactions - for instance, balance inquiries might be needed before committing a money remittance. The accounting and brokerage services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module. Mobile banking may also be used to help in business situations as well as financial [14]. Mobile banking shown in Figure 4.

3.1 Account Information

- Mini-statements and checking of account history
- Alerts on account activity or passing of set thresholds
- Monitoring of term deposits
- Access to loan statements
- Access to card statements
- Mutual funds / equity statements
- Insurance policy management

3.2 Transaction

- Funds transfers between the customer's linked accounts
- Paying third parties, including bill payments and third party fund transfers
- Check Remote Deposit

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

3.3 Investment

- Portfolio management services
- Real-time stock

3.4 Support

- Status of requests for credit, including mortgage approval, and insurance coverage
- Check (cheque) book and card requests
- Exchange of data messages and email, including complaint submission and tracking
- ATM Location

3.5 Content Services

- General information such as weather updates, news
- Loyalty-related offers
- Location-based services

A report by the US Federal Reserve (March 2012) found that 21 percent of mobile phone owners had used mobile banking in the past 12 months. Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more "tech-savvy" customer segment. A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill.

3.6 Challenges for a Mobile Banking Solution

There are a large number of different mobile phone devices and it is a big challenge for banks to offer a mobile banking solution on any type of device. Some of these devices support Java ME and others support SIM Application Toolkit, a WAP browser, or only SMS. Initial interoperability issues however have been localized, with countries like India using portals like "R-World" to enable the limitations of low-end java-based phones, while focus on areas such as South Africa have defaulted to the USSD as a basis of communication achievable with any phone. The desire for interoperability is largely dependent on the banks themselves, where installed applications (Java based or native) provide better security, are easier to use and allow development of more complex capabilities similar to those of internet banking while SMS can provide the basics but becomes difficult to operate with more complex transactions. There is a myth that there is a challenge of interoperability between mobile banking applications due to perceived lack of common technology standards for mobile banking. In practice it is too early in the service lifecycle for interoperability to be addressed within an individual country, as very few countries have more than one mobile banking service provider. In practice, banking interfaces are well defined and money movements between banks follow the IS0-8583 standard. As mobile banking matures, money movements between service providers will naturally adopt the same standards as in the banking world.

In January 2009, Mobile Marketing Association (MMA) Banking Sub-Committee, chaired by Cell Trust and VeriSign Inc., published the Mobile Banking Overview for financial institutions in which it discussed the advantages and disadvantages of Mobile Channel Platforms such as Short Message Services (SMS), Mobile Web, Mobile Client Applications, and SMS with Mobile Web and Secure SMS

4. Cyber Security in Banking Industry

There is a noticeable shift in the banking industry in the way customers deal with their transactions. There is a rapid increase in the usage of digital channels such as internet banking, digital wallets, mobile banking, ATM. This leads to the increase in exposure and thereby cyber-attacks which further may lead to financial and reputational losses. Banks may lose the customer confidence which can further increase the impact. The key influencers who makes it imperative for the banks to invest in security are: Increase in financial data losses including card data, personal identifiable information etc. Unauthorized access to bank’s network and systems. Key Drivers for Investment in Cyber Security shown in Figure 5.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

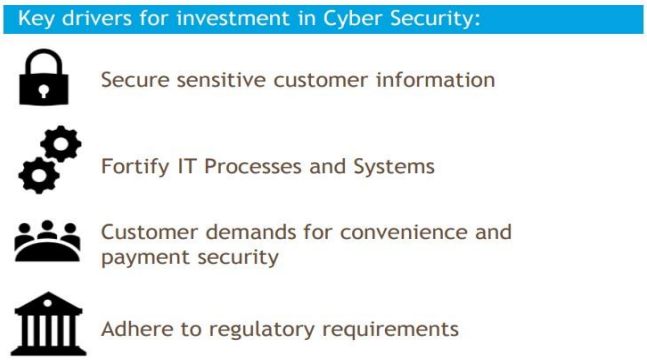

Figure 5 Key Drivers for Investment in Cyber Security

With increasing risks of cyber threats, banks are facing an unprecedented challenge of data breaches and are therefore strengthening their cyber security postures. The following are the noticeable trends in banking industry from cyber security point of view: Financial sector faced almost three times the cyber-attacks as compared to that of the other industries Data breaches (both internal through fraud and external through cyber criminals) leads to the exponential rise in costs It has been estimated that cost of implementing and managing the cyber security infrastructure will increase over 40% by 2025 There is an increase in biometrics and. tokenization as banks have begun to recognize that in addition to being a solution for payments these controls are also useful in security the sensitive data Customers are using biometrics for banking. Activities such as authentication for mobile banking, transaction at ATMs and payments with digital channels becoming the preference. Choice of customers for banking services, banks will also need to leverage advanced authentication and access control processes, without any compromise to customer experience. With the increase in the development of technologies the banking industry is evolving at an extraordinary rate. Unmanned aerial systems, the Internet of Things, Near Field of Communication (NFCs), and nearable devices are some of the technological advancements that banks will need to consider in the near future. Few of the top upcoming priorities for banks could be cloud based platforms, robotic process automation and cognitive technologies. Automation will drive new efficiencies across the security lifecycle, but require the creation of control mechanisms and strong governance. The above trends however pose their own set of challenges which are discussed in the next section.

4.1 Challenges

The exponential growth of digital payments platform in India and the push towards a cashless economy has renewed focus on the need to strengthen cybersecurity posture. Few of the major challenges faced by banks include:

- Strict compliance regulations: Managing regulatory compliances has become enormously challenging for the banks. Over the past few years the volume of regulations has increased dramatically. Along with the larger banks, smaller ones too are required to fulfill the regulatory obligations the struggle to secure.
- The struggle to secure customer data: There are number of ways in which violation of privacy can take place in banking sector like stolen or loss card data, unauthorized sharing of data with third parties and loss of client's personal data due to improper security measures
- Third party risk: Banks need to conduct due diligence on third parties they are associated with. As per Payments card industry data security standard, third parties need to report any critical issues associated the card data environment to the bank.
- Evolving cyber threat landscape: The development in technologies is leading to the latest cyber threats like next generation ransomwares, web attacks etc
- Transaction frauds: Fraud detection technologies should be in place with proper consideration of risks based on the business factors.
- Secure SDLC: Banks need to incorporate SDLC security for banking products and applications.

5. Regulatory Perspective

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

To ensure security in banking industries, the Reserve Bank of India removed a Circular DBS.CO.ITC.BC.No.6/31.02.008/ 2010-11 dated April 29 2011, where all banking institutions have to comply for. Some of the key features of the regulations are

- Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank
- Arrangement for continuous surveillance
- Comprehensive network and database security
- Protection of customer information
- Cyber security preparedness indicators
- Cyber Crisis Management Plan
- IT architecture should be conducive to security
- An immediate assessment of gaps in preparedness to be reported to RBI
- Cyber security awareness among stakeholders/ Top Management

6. Security Considerations

While each bank thinks distinctively on adopting various considerations it is imperative to assume that the theme remains the same for various banking channels:

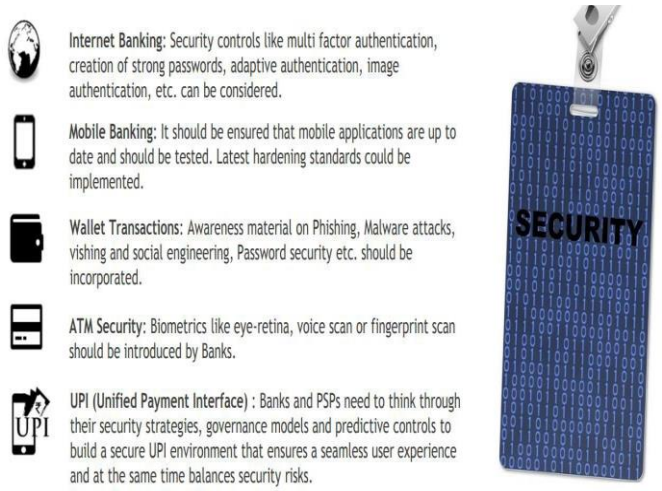

Figure 6

Banks must conduct regular drills, awareness programs and simulation exercises to keep their infrastructure secured.

6.1 Approach to Security

At BDO India, we Endeavour to provide expertise driven solutions to help and assist our client's business needs are met, through a well-defined risk based approach to adoption can have the following phases:

Plan: Discussing the scope of work, making a roadmap for the approach, formalizing leadership & project SPOC and to understand the policy and procedures all can be a part of the planning phase.

Build & Design: The build phase consists of requirements as a part of a systems engineering process. The main milestone of design phase would be matching the system specifications and the disposition of risk from the organization as shown in the framework.

Implementation: Gaps identified during the plan phase are implemented. Integration elements should be carefully planned.

Transition: A seamless transition and handover to the operations team should be taken into consideration.

Manage: This phase includes management, monitoring, and periodic reviews against security threats and frauds.

Figure 7

6.2 Cyber Security Trends

Blockchain is a technology that was initially developed for Bitcoin, the cryptocurrency. Blockchain could reduce banks infrastructure costs by US$ 15-20 billion per annum by 2022. Blockchain have the potential to transform how the business and the government work in vast variety of contexts.

- Banks will continue to leverage digital technologies to enhance customer experience.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

- Ongoing threats related to IoT devices will force banks to tighten security layers, including patchable firmware/software, secured authentication, and controlled privilege access. Today, most IoT devices are considered throw away devices and security patches are not issued. But, new regulations will be driven by large scale attacks using IoT to amplify the attack.

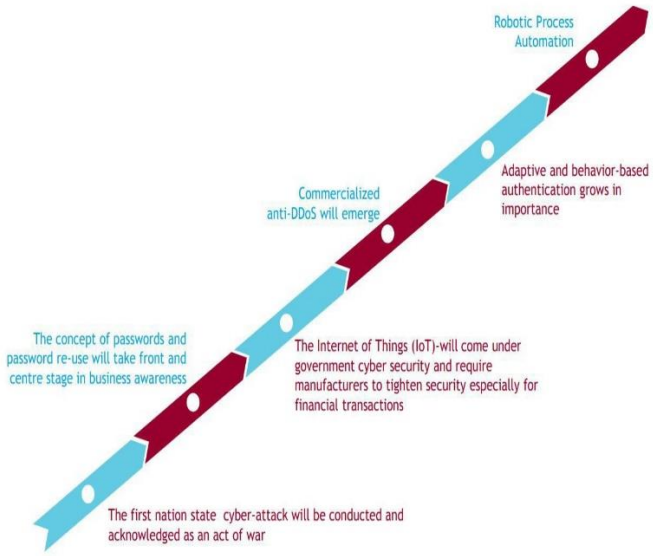

Figure 8

Conclusion

Banking systems have been with us for as long as people have been using money. Banks and other financial institutions provide security for individuals, businesses and governments, alike. Let's recap what has been learned with this tutorial: In general, what banks do is pretty easy to figure out. For the average person banks accept deposits, make loans, provide a safe place for money and valuables, and act as payment agents between merchants and banks. Banks are quite important to the economy and are involved in such economic activities as issuing money, settling payments, credit intermediation, maturity transformation and money creation in the form of fractional reserve banking. To make money, banks use deposits and whole sale deposits, share equity and fees and interest from debt, loans and consumer lending, such as credit cards and bank fees. In addition to fees and loans, banks are also involved in various other types of lending and operations including, buy/hold securities, non-interest income, insurance and leasing and payment treasury services. History has proven banks to be vulnerable to many risks, however, including credit, liquidity, market, operating, interesting rate and legal risks. Many global crises have been the result of such vulnerabilities and this has led to the strict regulation of state and national banks. However, other financial institutions exist that are not restricted by such regulations. Such institutions include: savings and loans, credit unions, investment and merchant banks, shadow banks, Islamic banks and industrial bank

References

[1]. Ahmad, K., "Bankers' perception of electronic banking in Pakistan", Journal of internet Banking and commerce, April 2008
[2]. Aladwani, A.M., "Online banking: A field study of drivers, development challenges and expectations", International Journal of information Management.
[3]. Agboola A. A., "Electronic payment systems and Tele banking Services in Nigeria",
[4]. Journal of Internet Banking and commerce
[5]. Eyadat, M. and Kozak, S., "The role of Information Technology in the profit and cost efficiency improvements of the banking sector", Journal of Academy of Business and Economics,
[6]. M.G, &Gebba T.R (2013) banking adoption an examination of TAM and Theory of Behavior, International Journal of Business Research and Development.
[7]. Cano M.D & Domenech-Asensi, G (2011). A Security energy- efficient m-banking application for mobile devices. The journal software.
[8]. https://www.wikipedia.org/
[9]. https://www.bankingfinance.in/impact-of-information-technology-in-indian-banking-industry.html

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0106
e ISSN: 2584-2854
Volume: 02
Issue: 04 April 2024
Page No: 774-784

[10]. https://www.rbi.org.in
[11]. http://www.banknetindia.com/
[12]. https://www.bankingfinance.in
[13]. https://www.hugedomains.com/domain_profile.cfm?d=india-bank&e=com
[14]. https://www.capgemini.com/resources/top-ten-trends-in-banking-2017/