Understanding Cyber Security And Privacy Issues: Challenges And Solutions In Financial Services

Hetal Chaniyara
Research scholar, Saurastra University, Rajkot.

ABSTRACT:

This paper discusses how cyber security and privacy are important in various types of financial services. The first section contains the introduction part and recent trend in digital transaction. The second section contains the motivation for the research as the need of cyber-security at all levels like individual, corporate level, State and national level. Third section contains the issues related to cyber-security, and the fourth section, which focuses on the awareness program and various types of solutions in the financial services are the main core of the paper.

Key words: Cyber Security, Privacy

INTRODUCTION

The Cyber security plays an important role in the development of information technology, as well as Internet services. Today, we can see that internet is one of the fastest-growing areas of technical infrastructure development. In today's business environment, such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online. Today, about more than 80% of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Protecting critical information and enhancing cyber security are essential to each nation's security and economic well-being. The world has become dependent on cyber systems across the full range of human activities including finance, health care, energy, entertainment, commerce, communications, and national defense.

India has seen a series of significant and unprecedented events during the last years, which have brought the issue of cyber security for the Indian banking sector to the fore like never before. The most significant factor in this regard has been the ongoing initiative of the Government of India, through its flagship Digital India program a vision to transform India into a digitally empowered society and knowledge economy. The continued increase in penetration of inclusive banking through the Pradhan Mantri Jan Dhan Yojana (PMJDY) with the total number of accounts crossing 37.95 crore[1], brought the uninitiated and new users into the fold of banking services. The recent report of Reserves Bank of India says that Digital transactions set to rise four times by 2021.[2]

While most industries around the world are affected by cyber threats, the banking sector has always been the worst hit. Financial institutions face a growing pressure threat from cyber-attacks, which can take many different forms across a wide range of channels. A typical attack will be committed by a criminal in a remote and safe location who tries to get inside the systems of a bank or of its clients. Other attacks include attempts to divert payments into the accounts of criminals.

[1] https://www.pmjdy.gov.in/account/as on 22/01/2020

[2] https://indianexpress.com/article/business/economy/digital-transactions-set-to-rise-four-times-by-2021-reserve-bank-of-india-5783553/

TRENDS IN DIGITAL TRANSACTION

The pace of digitization of financial transactions in India continues to gather pace. It is estimated that noncash payment transactions, which today constitute 22 percent of all consumer payments, will overtake cash transactions by 2023.[3] The technology infrastructure continues to build up, with 100 crore mobile connections in the country, of which 24 crore are of smart phone users. The number of smart phones is expected to increase to 52 crore by 2020. Around 90 percent of all devices are internet enabled and the number of internet users is set to double to nearly 650 million by 2020 from the erstwhile 300 million in 2015.

An important factor in the exciting growth of the payment ecosystem is Indian FinTech companies, which are scaling up in number and sophistication. These companies are likely to leverage technology and establish interfaces with banks and the Aadhaar database. Some of the active areas include payment systems, peer to peer and cross border transactions as well as mobile PoS processing; robo-advisory and brokerage for personal finance management; crowd-funding, P2P lending, alternative lenders and market places and credit scoring, analytics and risk management.

OBJECTIVES OF THIS RESEARCH PAPER

- To through some light on the concept of cyber security and privacy in financial services.
- To know about what are some of the main privacy issues that businesses have to deal with in financial services.
- To know about how do companies or organizations manage cyber security and privacy issues to protect their financial services.

DEFINING CYBER SECURITY AND PRIVACY

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Privacy concerns the expression of or adherence to various legal and illegal norms regarding the right to private life. Here Information privacy is the privacy of personal information and usually relates to personal data stored on computer systems. The need to maintain information privacy is applicable to collected personal information, such as medical records, financial data, criminal records, political records, business related information or website data. Information privacy is also known as data privacy.

[3] https://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1

NEED OF CYBER SECURITY

Before addressing cyber security needs in the financial services researcher tries to defining the necessity of cyber security in terms of need of cyber-security in the current Indian security system.

Information is the most valuable asset with respect to an individual, corporate sector, state and country. With respect to an individual the concerned areas are:

1) Protecting unauthorized access, disclosure, modification of the resources of the system.

2) Security during on-line transactions regarding shopping, banking, railway reservations and share markets.

3) Security of accounts while using social-networking sites against hacking.

4) One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defenses.

With respect to the corporate sector the concerned areas are:

1) Securing the details of the employees.

2) Securing confidential reports at managerial level.

3) Permitted access at various level of the organization.

4) Secured flow of information within and outside the organization.

5) Strong administration level strategies against any disclosure of information.

6) Need of separate unit handling security of the organization.

7) Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness.

8) In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered.

With respect to state and country:

1) Securing the information containing various essential surveys and their reports.

2) Securing the data basis maintaining the details of all the rights of the organizations at state level.

CHALLENGES OF CYBER SECURITY

Much of Bank and Financial Institution's operations take place with the use of technology including through the internet. For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. There are number of challenges of cyber security which are as follow:

1. Awareness remains low:

Awareness amongst internal employees remains the first line of defense. However, not many firms invest in training and improving the cyber security awareness levels within the enterprise.

2. Poor Identity and Access Management:

Identity and access management is the fundamental element of cyber security. In an era where hackers seem to have upper hand, it requires only one hacked credential to gain entry into an enterprise network. Despite some improvement, there remains a lot of work to be done in this area.

3. Lack of capital and Lack of Top Management support:

Budgets are usually driven by business demands and low priority is accorded to Cyber security. Top management focus also remains a concern, support for cyber security projects are usually given low priority. This is primarily due to the lack of awareness on the impacts of these threats.

4. Distributed denial of service (DDos) attack:

With the advent of IoT-powered botnets, destructive DDoS attacks are inevitable and have intensified in volume and frequency. Organizations in India need to improve their response capability to mitigate DDoS risks.

5. Social Media:

Growing adoption of social media leads to more potential for hackers to exploit. Many a user puts her data out for anyone to see, which can be potentially exploited to attack the user's organization. Use of social media to propagate fake news can impact banks' reputations in an insidious manner.

6. Mobile devices and Apps:

As organizations move towards adopting mobile devices as its preferred channel for doing business, it also becomes the ideal choice for hackers to exploit as the base increases. Since financial transactions can be done on mobile apps, the mobile phone is becoming an attractive target leading to an increase in mobile malware. The risk of jail-broken and rooted devices used for financial purposes increases the scope of attack.

7. Ransomware on the Rise:

The recent episodes of malware attacks, viz. WannaCry and Petya, brought home the rising menace of ransomware. As more users recognize the risks of ransomware attack via email, criminals are exploring other vectors. Some are experimenting with malware that reinfects later, long after a ransom is paid, and some are starting to use built-in tools and no executable malware at all to avoid detection by endpoint protection code that focuses on executable files. Ransomware authors are also starting to use techniques other than encryption, for example deleting or corrupting file.

8. **Regulatory Concerns:**Financial services firms face stringent cyber security regulations, which places more accountability on senior executives. Also, as financial organizations adopt hybrid cloud, they face more scrutiny by regulators and must ensure workloads in the cloud meet new security standards.

9. Too Many Disparate Tools:

Many institutions have numerous, siloed security tools that add complexity rather than providing insight. When these tools don't integrate or communicate efficiently, they don't provide the visibility security teams need to establish seamless, holistic protection, which is required to keep up with today's threats.

10. Talent Gaps:

The financial services industry, like other industries, is grappling with substantial talent gaps. In contrast, cybercriminals targeting the sector are growing in number, becoming industrialized and beginning to leverage advanced technologies such as artificial intelligence (AI) in their arsenal.

11. Competitive Threats and Margin Pressures:

Financial services institutions strive to continuously innovate and offer differentiated digital experiences while simultaneously demonstrating advanced, but nonintrusive security capabilities. Success across these factors reduces churn and allows institutions to alleviate operational costs.

12. Inadvertent Insiders and Lack of Attention to Security Fundamentals:

Frequently, companies lack discipline with elemental security responsibilities. Also, as mentioned in the "IBM X-Force Threat Intelligence Index", "two of the most prolific ways X-Force researchers have observed inadvertent insiders leaving organizations open to attack is by falling for phishing scams or social engineering, and through the improper configuration of systems, servers, and cloud environments, and by foregoing password best practices."

13. Insufficient Capabilities and Preparation for Right of Boom:

As executives realize that it is not a question of if they will face a cyberattack, but when the lack of investment right of boom - in the response and management of a cyberattack after it occurs — raises considerable concern. Often, personnel on the front lines don't have capabilities such as AI, machine learning and intelligent orchestration and face an increasingly difficult task to diagnose a breach, assess the size and scope, and respond in the timeframe required by the General Data Protection Regulation (GDPR).

For many firms, the company's success depends on one or a few individuals who may not have adequate information or experience to take the best actions during the hectic moments of a breach. In addition, many institutions are not prepared to address the increasingly common scenario of attacks launched by internal resources.

SOLUTIONS TO IMPROVE CYBER SECURITY IN THE FINANCIAL SERVICES:

As per PwC's Global Economic Crime Survey[4] , cyber crime has jumped to the second position as the most reported economic crime and financial institutions are prime targets. As cybercriminals find new ways to attack, organizations need solutions that assess their own and their vendors' vulnerabilities in real-time. Here are some great steps to improve cyber security in the financial services:

1. **Strengthen defense strategy:**

   Use capabilities such as advanced data intelligence gathering and security analytics optimized with automation and AI to force-multiply your teams' efforts and assess advanced threats that may have bypassed your controls.

2. **Collaborate with industry peers and experts:**

   Don't go it alone as you prepare to battle threats to individual institutions as well as the industry ecosystem. Leverage communities, cyber range facilities, professional services and intelligence analysis tools to hunt and battle threats and assess and improve your readiness.

3. **Practice incident response:**

   Develop and maintain dynamic response playbooks that use AI and machine learning to automatically leverage threat intelligence information and practice your incident response plans with rigor.

4. Increase attention on fundamentals:

Focus on core responsibilities, including knowing your assets and inventory, understanding your firm's vulnerabilities and attack surfaces, classifying sensitive data and tracking usage patterns, using multilevel authentication and layered defenses, ensuring device security, improving patch management and more.

5.**Build digital trust:**

Adopt new approaches to identity and access management (IAM) to enable authentication without imposing on the customer experience. Technologies include passive behavioral biometric approaches that focus on what and who you are rather than what you know.

6. Innovate while improving defenses and manage risk with enterprise cloud security: Pursue accelerated growth and the benefits of hybrid cloud while securing data and workloads in the cloud.

7. Get ahead of compliance:

Leverage technology to understand how your firm's regulatory obligation exposure is changing over time.

[4] https://www.csoonline.com/article/3083798/cybersecurity-spending-outlook-1-trillion-from-2017-to-2021.html

8. Foster a security-oriented culture and expand executive involvement:

Work to make security a central focus for all employees and elevate security beyond the responsibility of the chief information security officer (CISO) alone.

9. Periodic Newsletters on Cyber security:

Target audience would include key stakeholders from RBI (CGM and above) as well as CIOs, Executive Directors, business unit heads, heads of internal audit, operational risk, compliance and fraud management from all of the financial institutions regulated by RBI. Readership is aimed at top rungs of the leadership who would be keen on the most important news and would also be able to influence the latest thinking and action around cybersecurity policy within their respective organizations.

10. Move from security as a cost, to security as a plus:

The mindset of seeing security as a cost needs an overhaul. The risks associated with security threats and the potential impact to business should make organizations see the benefits of proactive security.

CONCLUSION:

Cyber security depends on the care that people take and the decisions they make when they set up, maintain, and use computers and the Internet. Cyber-security covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means. Albert Einstein was quoted as saying "Problems cannot be solved with the same level of awareness that created them." The problem of End-User mistakes cannot be solved by adding more technology; it has to be solved with a joint effort and partnership between the Information Technology community of interest as well as the general business community along with the critical support of top management.

Indian citizens must identify the best techniques in order to protect the information and system, as well as the network in which they work. The IT industry has been playing catch-up with hackers and cyber criminals for decades. Thus there is a need of cyber –security curriculum in the near future which will in-build the cyber-security understanding in the current youth and finally the IT sector will get more profound, securely skilled professionals not only in the security sector but also in the every sector, thus enhancing the communication, the brain compatibility skills of the employees and the employers. Effective cyber-security policies, best practices must be planned and most-important must be implemented at all levels.

REFERENCES:

1. Atul M. Tonge, Suraj S. Kasture, Surbhi R.Chaudhari (2013), "Cyber Security: Challenges For Society – Literature Review", IOSR journal of computer engineering, Vol. 12, Issue 2, pp-67-75.
2. Priti Saxena, Bina Kotiyal, R H Goudar, and Senior Member, IACSIT (2012),"A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India", International Journal of Information and Education Technology, Vol. 2, No. 2, pp-167-170.

3. Debabrata Nayak (2012), “Understanding the Security, Privacy and Trust Challenges of Cloud Computing”, Journal of Cyber Security and Mobility, Vol. 1, pp-277–288.
4. Institute for Defence Studies and Analysis task force report (2012), “India's Cyber Security Challenges”.
5. https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security
6. https://securityintelligence.com/challenges-and-opportunities-to-close-the-cybersecurity-gap-in-the-financial-services-industry/