DATA PROTECTION AND CYBER SECURITY IN BANKING COMPLIANCE, BREACHES, LIABILITIES

By author

K.Dharshini

B.Vishnupriya

P.L.Shariya

M.Guruharini

Mr .C.Ajay , Assistant professor

School of law, Dhanalakshmi Srinivasan University Trichy-621112

ABSTRACT

The digital development of the banking industry, driven by AI, cloud computing, and blockchain, has increased efficiency and accessibility but also raised several challenges related to data protection and cybersecurity, such as phishing, ransomware, and breaches that have caused billions of dollars in losses, with more than 20,000 attacks worldwide that resulted in losses of over US$12 billion. Some of the ways banks can effectively respond to such threats include data encryption, multi-factor authentication, real-time monitoring, employee training, and adherence to different regulations like GDPR, PCI-DSS, and India's IT Act 2000 to protect sensitive data and guarantee the stability of finances and customer trust. Stronger plans not only reduce risks but also provide businesses with competitive edges, underlining adaptive governance in the face of increasing digital adoption

Key words : Data Protection,cyber security,Multi factor Authentication,Ransomware

INTRODUCTION

In the current digital era, a vast number of customers who primarily rely on online and mobile platforms for daily transactions entrust banking and financial institutions with their sensitive data. The banking industry has a critical duty to safeguard financial and personal information against various cyberthreats that aim to steal customer data. Protecting sensitive information and securing banking systems from cyber threats is not just a choice but a necessity in the age of advancing technologies.Banks depend on cybersecurity and data protection as their primary defenses against financial fraud, unauthorized access, and data breaches. Therefore, understanding and implementing effective data protection and cybersecurity practices are crucial not only for safeguarding sensitive data but also for preserving customer trust. To protect consumer data, financial assets, and a bank's reputation from online threats such as fraud, ransomware, and hacking, strong cybersecurity measures are essential. These act as the core safeguards that banks rely on to prevent

fraud, unauthorized access, and data breaches, thereby ensuring resilience and confidence in the banking system. Recent developments in 2025 focus on strengthening cybersecurity frameworks, compliance with evolving regulations such as India's Telecommunication Cyber Security (TCS) Rules 2024 amendments, and the new Data Protection Board of India under the Digital Personal Data Protection Rules 2025. Compliance breaches in banking can lead to significant liabilities including financial penalties, reputational damage, and legal consequences.

Meaning

Data protection in banking entails protecting client financial and personal information using techniques like encryption, access controls, and regulatory compliance. Because banks deal with sensitive information like identities and transaction details, privacy controls are crucial to preventing identity theft and legal repercussions.Strict third-party vendor standards and confidential computing, which encrypts data during processing, are two strategies.

Cybersecurity in banking refers to technologies and practices that defend digital systems against hacking, phishing, malware, and ransomware attacks. Banks implement multi-factor authentication, firewalls, intrusion detection, and real-time fraud monitoring to protect networks and operations. Therefore, this protects assets, ensures continuous services, and retains customer trust in the growing digital transactions**.**

Importance

Data security and cybersecurity represent the foundation of modern banking, wherein huge volumes of sensitive customer information-such as personal identifiers, transaction histories, credit scores, and financial records-are kept safe from ever-escalating threats of phishing, ransomware, malware, hacking, and insider attacks that have inflicted billions of dollars in losses across the sector in recent decades.

In this era of digital transformation with the proliferation of mobile banking, AI-driven services, cloud computing, and blockchain integrations, banks must operationalize a multilayered defense comprising of robust encryption for data at rest and in transit, multi-factor authentication, zero-trust architecture, which verifies every user and device continuously, firewalls, intrusion detection systems, network segmentation, and real-time AI-powered threat monitoring to prevent unauthorized access, data leaks, and lateral movement by an attacker. Regulatory compliance is given, with international standards like the PCI DSS imposing penalties of $5,000 to $100,000 per month for the failure to handle credit card data securely. ISO/IEC 27001 demands an information security management system; SWIFT CSP fortifies messaging networks; GDPR extends to breach notification in 72 hours and privacy-by-design; GLBA has strict access policies for all U.S. institutions; PSD2 regulates electronic payments in the EU; FINRA prescribes guidelines for broker-dealers; BSA has guidelines to combat money laundering through incident response plans; and region-specific frameworks like India's DPDP Act 2023, RBI cyber security guidelines, and CERT-In directives ensure data localization and quick reporting.

These measures protect against catastrophic breaches, as over 20,000 documented attacks disrupted operations and eroded financial stability; mitigate fraud like identity theft, supply chain vulnerabilities, and APTs; and allow DLP tools to monitor outflows and maintain granular access controls. Beyond risk reduction, prioritizing such protections fosters undeviating customer trust and loyalty through transparent privacy policies, secure digital platforms, and proactive education against scams. This allows banks to innovate with confidence in fintech collaborations, remote access environments, and third-party ecosystems without compromise on resilience. Regular vulnerability assessments, penetration testing, employee training, software patching, comprehensive backups, and swift incident response plans further ensure operational continuity by minimizing downtime and reputational damage in a landscape where non-compliance invites fines, legal actions, and loss of market edge. By doing all this, the integrity of the global financial system is upheld, economic stability is sustained, and banks remain trustworthy stewards of data in a hyper-connected world.

Objectives

The main goals of data protection and cybersecurity in the banking industry are to protect sensitive information of customers, such as personal identifiers, transaction history, and other financial records, from unauthorized access, breach, and cyber threats like phishing, ransomware, and malware, which will prevent identity theft, fraudulent transactions, and huge financial losses. These guarantee regulatory compliance with laws such as GDPR principles for data minimization, purpose limitation, accuracy, and a 72-hour breach notification; PCI DSS for the protection of cardholder data from a data breach; GLBA for strict access controls; ISO/IEC 27001 for information security management; and region-specific rules, such as India's DPDP Act and RBI guidelines, avoiding $100,000 per month penalties while enforcing encryption, multifactor authentication, and audit logging. Other goals include gaining customer trust and loyalty via transparent privacy policies and digitally secure platforms; enabling operational resiliency through real-time monitoring of threats, intrusion detection, zero-trust architecture, and incident response plans with minimal operational downtime and disruptions; and managing third-party risks in cloud and vendor ecosystems for supply chain integrity.

Major threats to Data Protection and cyber security

- **Phishing and Spear-Phishing**:

Attackers send deceptive emails or messages to trick employees and customers into revealing credentials or installing malware, often leading to APTs with prolonged unauthorized access and data exfiltration

- **Ransomware and DDoS Attacks:**

Criminals encrypt systems or overwhelm networks to demand ransoms, causing service disruptions and financial losses exceeding billions annually across global banks

- **AI-Driven Threats**:

Deepfakes bypass voice biometrics, while AI enhances phishing and vulnerability scanning, targeting fintechs and retail banks for credential theft and fraudulent transactions.

- **Mobile and Overlay Malware:**

Trojans overlay fake screens on banking apps, intercept SMS codes, or log keystrokes to compromise customer accounts via fake apps or phishing links.

- **Supply Chain and Cloud Risks:**

Hackers breach vendors for indirect access, exploit unpatched cloud workloads or insecure APIs/S3 buckets, exposing customer data and core banking systems

- **Zero-Day Exploits and APTs:**

Nation-states or criminals use unknown vulnerabilities for espionage in large banks, stock exchanges, or SWIFT networks, aiming for geopolitical or economic gains.

Compliance in Data Protection and cyber security

Banks have to adhere to the data protection and cybersecurity standards in the banking sector primarily through India's Digital Personal Data Protection Rules 2025, besides RBI guidelines, demanding explicit consent notices, data minimization, purpose limitation, and lifecycle management with automated erasure tools. Cybersecurity requirements include encryption, tokenization, access controls, audit logs, AI-driven threat detection, and breach reporting to the Data Protection Board within 72 hours plus immediate user notifications, with penalties up to ₹250 crore for violations. Banks have to appoint Data Protection Officers, conduct impact assessments, overhaul legacy systems via privacy-by-design, and adopt phased implementation-immediate consents followed by 12-18 months .

Some regulatory frameworks are

1.The Digital Personal Data Protection(DPDP) Rules, 2025

It forms a new regulatory requirement in India for the banking industry, among others. They detail key responsibilities under the core DPDP Act 2023, concerning protection of personal data of customers through designation of a DPO, clear customer consent on the uses of data, secure data flows, and vendor contract compliance. Banks will have to upgrade their data privacy, consent management, breach reporting, and adherence to data minimization and cross-border transfer limits.

Key Responsibilities of Banks under DPDP Rules 2025

- Appointing an India-based DPO, reporting to the board, whose contact is publicly listed.
- Mapping and auditing all data flows related to KYC, lending, and marketing.
- Apply explicit, informed consent to every purpose of data usage.
- Multilingual privacy notices to improve accessibility.
- Allow for customers to withdraw consent and have their data deleted.
- Implement contract requirements for compliance and audits with all vendors handling customer data.
- Punctually report data breaches to the Data Protection Board of India.
- Follow the principle of data minimization: delete data when it is no longer needed, except when laws such as RBI guidelines provide otherwise.
- Restrictions on cross-border data transfers unless approved by the government with customer.

2.Information Technology Act,2000

This Act is the India's prime law which governs cybercrime and electronic commerce.It provides legal validity to electronic transactions and digital signatures and establishes penalties for cybercrimes,and makes a framework for electronic governance.The Act was enacted on October 17,2000 and was amended in 2008

Section 43A- Responsibility of banks to protect customer data

Section72- breach of confidentiality and privacy , penalty upto ₹5 lakhs

Section 72A- penalty upto ₹25 lakhs for disclosing information in breach of law contracts to third parties

Section 66 - Addresses cybercrime like hacking and data damage, with imprisonment up to 3 years and fine up to ₹5 lakhs

3.RBI guidelines on digital payment security

- The RBI has also given comprehensive guidelines on digital payment security and data protection to ensure robust cybersecurity in the banking and payments ecosystem.
- The main framework is the Master Direction on Digital Payment Security Controls, which was issued on 18 February 2021 and prescribes strong security governance and controls in line with internationally recognized standards such as OWASP, NIST, ISO, and PCI for implementation by regulated entities like banks, payment banks, small finance banks, and card-issuing NBFCs.

- Key Provisions of RBI Digital Payment Security GuidelinesTwo-factor authentication (2FA) needs to be implemented for all digital payment transactions, with a migration to risk-based authentication models that evaluate different signals such as device behavior and transaction history for fraud reduction and increasing user convenience.
- Confidentiality, integrity, and backup of customer data in respect of all digital payment products and services need to be implemented through encryption, secure communication protocols, web application firewalls, and protection against denial-of-service attacks.
- Dedicated policies should be laid down for digital products covering the security of the entire payment lifecycle, starting points, critical stages, validation, and exception handling.
- Incident management/customer grievance redressal mechanisms are also very important and should provide for fraud risk monitoring, control validation, and resolution processes in a timely manner.

Breaches

The banking industry has been one of the major sectors suffering from data protection and cybersecurity breaches, mainly characterized by supply chain attacks, ransomware, and phishing in 2024 and 2025. Some of the largest banks in the world, such as Santander and DBS Bank, have been breached without their systems being hacked directly, showing how vulnerable third-party vendors can be. Attacks generally target PII and financial data from customers, which are highly valued for identity theft and fraud. The most common methods of data breaches in this regard involve encryption via ransomware, social engineering through phishing attacks, and software system vulnerabilities in vendors.

India's banking sector has seen over 248 confirmed data breaches and a 15% surge in cyberattacks in 2025 alone, emphasizing the global scale and urgency of strengthening cybersecurity measures in financial institutions. Large-scale breaches impact customer trust, incur regulatory penalties, and demand costly compensations and security overhauls from affected banks. The banking industry's increasing reliance on digital processes and third-party vendors creates expanded attack surfaces for cybercriminals to exploit.These incidents highlight the critical need for banks to implement comprehensive cybersecurity protocols, ongoing employee security training, rigorous vendor risk management, and proactive incident response plans to protect sensitive financial data and maintain regulatory compliance

Liabilities

Liabilities related to data protection and cybersecurity in the banking sector usually flow from the bank’s obligation to secure sensitive information relating to customers and to conform to applicable legal and regulatory frameworks.

The primary liability of banks is related to any breach of customer data, including PII and financial information, more so when they act as data controllers in processing such information. This also includes

strict legal liability pursuant to data protection laws, such as India's Information Technology Act, 2000, which mandates a reasonable security practice and provides for a claim for compensation in the case of wrongful loss on account of negligence or failure to secure such sensitive data. Apart from regulatory fines, banks can also be civilly liable for lawsuits filed by affected customers, shareholders, or creditors for negligence or breach of fiduciary duties concerning cybersecurity.

Under the Companies Act, directors and officers have a duty of care to ensure adequate cybersecurity governance; failure to do so may attract penalties or legal action for breach of duty. Further, banks have the liability of ensuring compliance by third-party service providers and data processors, as outsourcing of services does not discharge their liability in case of failure on data protection.

Contractual liabilities would arise in case of breach of confidentiality or data protection clauses under agreements with customers, vendors, or partners, which might lead to damages, arbitration, or even contract termination. The fines that could be levied by regulatory agencies can be pretty huge, sometimes running into hundreds of crores in Indian currency, apart from reputational loss and disruption in operations. Thus, banks need to implement strong data security measures, periodic audits, employee training, and robust incident response plans to manage these liabilities effectively and maintain regulatory compliance.

CONCLUSION

In conclusion, Digital banking has expanded in India,which rapidly provide critical data protection and cybersecurity.It enables secure financial transactions. This study mainly focuses on adherence to the regulations, common breaches, and liability concerns within the Indian banking system. The main objective is to test cybersecurity measures Which are Adopted by banks, evaluate regulatory frameworks, and identify possible vulnerabilities. The results that show that while regulatory bodies like RBI and CERT-In have established strict guidelines of cybersecurity, financial Data breaches and cyber-attacks persist across institutions due to rapidly evolving threats and weak enforcement mechanisms, and inconsistent security practices.Lack of proper customer awareness and inadequate investments in infrastructures which increase the possibility of fraud and financial loss.

The future scope of this study is to highlight the importance of AI-driven fraud detection, blockchain-based secure transactions, biometric authentication, and more cybersecurity laws to enhance digital banking security. Other suggestions include mandated cybersecurity audits,improved customer awareness campaigns, more stringent regulatory penalties for non-compliance and increased coordination between financial institutions and cybersecurity experts.Besides, banks must invest in real-time threat monitoring.Advanced encryption technologies, and multi-layered Security frameworks in place to avoid cyber perils.

Finally, while India has taken great strides in securing Digital banking, continuous technological development,Proactive regulatory updates, and strengthened Cybersecurity measures would

be critical. According to the report, innovation, compliance, and collaboration are necessary in building an Resilient, secure, and trustworthy digital banking ecosystem.Ensuring customer confidence and safeguarding financial data against evolving cyber threats. Traditional encryption alone is too little, as data in active process is vulnerable; hence, advanced solutions like encryption-in-use technology have to be brought into play to give comprehensive protection across the lifecycle of data. This will further facilitate compliance with the increasingly demanding regulations, such as the Digital Operational Resilience Act of the EU, alongside mitigating breach-related risks and strengthening customer trust. Banks should ensure solid technical measures, including multi-factor authentication, real-time threat monitoring, behavioral analytics, secure APIs, and tight vendor risk management. In addition, they must have ongoing employee training, incident response planning, and collaboration with regulators and law enforcement for an effective combat against cyber risks. Any improper protection of data may lead to devastating reputational damage, harsh regulatory penalties, and financial loss. Therefore, the integration of sophisticated cybersecurity technologies with robust governance and compliance is essential for banking organizations to keep sensitive financial information safe, ensure regulatory compliance, and ultimately hold on to customer confidence in a digitized and threatening environment.