International Journal of Core Engineering & Management

Volume-7, Issue-08, 2023, ISSN No: 2348-9510

GUARDING THE VAULT: DATA PROTECTION STRATEGIES FOR FINANCIAL INSTITUTIONS

Puneet Matai
Program Manager – Enterprise Data Privacy & Protection
UOB Group, Singapore
puneet.matai@gmail.com

Abstract

This whitepaper delves into data protection strategies vital for financial institutions amidst escalating cyber threats. The paper aims to offer comprehensive insights and practical guidance on data protection strategies, emphasizing their critical importance in financial institutions. It identifies key cyber threats faced by financial institutions, outlines foundational data protection strategies, and discusses advanced security technologies, regulatory compliance requirements, and strategies for maintaining compliance while enhancing security. The whitepaper indicates the necessity to continuously evaluate and adapt security measures to develop a security-first mindset. It is concluded that the strategies explored may help in safeguarding sensitive customer information and mitigating risks associated with cyber attacks.

Keywords: Data Protection, security, Encryption, Data Breaches, Cyber threats, Regulatory compliance, Cyber incident response, Security awareness training, Artificial Intelligence

I. ACCOUNTING AND FINANCIAL MANAGEMENT SYSTEM

Data protection is of paramount importance in financial institutions given the sensitive nature of the information they handle. Recent research by [12] highlights that FinTech companies face substantial compliance challenges due to evolving legal frameworks. This "Innovation Trilemma" raises the difficulty to balance innovation with data protection and market integrity.

The evolving cyber threat landscape presents challenges to financial institutions. Cyber attacks targeting these institutions are becoming more sophisticated, frequent, and diverse. Some of the common threats include:

International Journal of Core Engineering & Management

Volume-7, Issue-08, 2023, ISSN No: 2348-9510

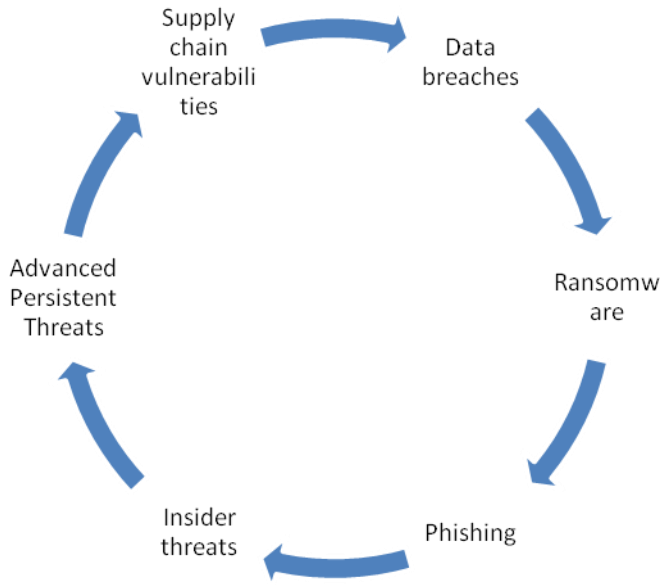

Figure 1: Common Threats

Cybercriminals are increasingly committing crimes via vulnerabilities in the networks, applications, and supply chain present in an organization. The dynamic threat landscape requires financial organizations to stay vigilant and adopt security measures.
This whitepaper aims to provide comprehensive insights into data protection strategies for financial institutions. The purpose of this whitepaper is to address the critical importance of data protection in financial institutions and offer practical guidance on mitigating cyber threats effectively.

II. THE THREAT SPECTRUM

Cyber attacks targeting financial institutions continue to evolve which presents a constant challenge to organisations to safeguard sensitive data and maintain customer trust. For example, the Equifax data breach in 2017 exposed the personal information of 147 million people which led to a global settlement with up to $425 million for affected individuals [1]. This breach compromised sensitive data such as Social Security numbers and birth dates. One prevalent avenue of attack is through removable media such as flash drives, which hackers can exploit to introduce viruses and gain unauthorised access to systems.

- Brute-forte attacks [2], another common tactic, involve exhaustive attempts to crack encryption keys or user logins which often succeed through persistence and automated tools.

- Web and email-based attacks remain persistent with phishing campaigns and spoofed websites tricking users into revealing login credentials or downloading malicious software.
- The loss or theft of devices is a tangible risk which exposes sensitive information even with strong passwords.
- Distributed Denial-of-Service (DDoS) attacks further disrupt operations by overwhelming servers with traffic [3], often motivated by financial gain or extortion.
- Automated Teller Machine (ATM) cash-outs demonstrate the physical impact of cyber threats on financial infrastructure, also called ATM Skimming.
- Vulnerabilities in third-party software, services, or supply chains can be exploited to gain access to financial institutions' networks or data.

III. FOUNDATIONAL DATA PROTECTION STRATEGIES

3.1 Principles of Securing Sensitive Customer and Financial Data

3.1.1 Principle: Data Categorization System and Employee Education

The aim is to establish a systematic data categorization system. It classifies sensitive data such as personal and financial information. It is important to educate the employees on the importance of data protection and their roles in maintaining security measures.

3.1.2 Principle: Regular Backup and Physical Protection

Implementation of a continual file backup system with automated scheduling helps in ensuring regular backups. Moreover, storing backup copies in fireproof safes or secured off-site locations helps protect against physical threats.

3.1.3 Password Management and Access Control

The use of multiple passwords for different data segments restricts access which is based on department or rank. Implementation of multi-factor authentication for enhanced security and regularly rotating passwords using random generators are essential.

3.1.4 Proactive Security Measures

Prepare for worst-case scenarios by proactively addressing insider threats and external attacks. Familiarize the employers with security tools provided by software vendors to develop security controls.

3.1.5 Employee Engagement and Transparency

Organizations should engage with employees to understand their access needs while maintaining a secure environment. Also, avoid overly restrictive measures that may lead to non-compliance and vulnerabilities.

International Journal of Core Engineering & Management

Volume-7, Issue-08, 2023, ISSN No: 2348-9510

3.2 Role of Encryption, Access Controls, and Data Masking

In financial institutions, safeguarding sensitive data is paramount. Encryption is important for converting data into a secure format that can only be deciphered with the right keys, thwarting unauthorized access. In the financial service sector, 98% successfully retrieved their encrypted data, while 69% relied on backups for data recovery [4]. Access controls further fortify this defence by restricting data access based on user roles and permissions. This prevents data leaks or misuse.

On the other hand, data masking shields sensitive information by replacing actual data with masked values while retaining format and structure for operational purposes. According to Swire, internet commerce relies heavily on traceable credit cards since cash and checks are impractical online [10].

While anonymous transactions are possible, law enforcement and market factors favour traceability to prevent money laundering. Thus, the demand for advanced data masking solutions is expected to surge.

IV. ADVANCED SECURITY TECHNOLOGIES

4.1 Cutting-edge tools and technologies in Cyber security

Cyber security involves protecting systems, networks, and data from cyber threats which assists in encryption, access controls, and threat detection. Fintech Cyber security is the term coined for safeguarding financial technology platforms, applications and data.

According to KPMG's report, around 43% of banking and fintech companies are ill-equipped and potentially susceptible to data breaches in 2022 [5]. This highlights the need for robust cyber security measures. The cutting-edge tools and technologies in cyber security are:

4.1.1 Artificial intelligence

Artificial intelligence (AI) is revolutionizing cyber security in finance by automating threat detection, response, and prediction. For example, AI algorithms can detect unusual transactions or behavioural patterns that may signal fraudulent activities.

Literature [9] identifies the security technologies for protecting data at the AI level. The key approaches explored are cryptographic hash functions, block-chain for tamper-evident logs, and encryption techniques to prevent unauthorized access and to ensure privacy.

4.1.2 Block-chain

Block-chain offers security features which are beneficial for cyber security in finance. It is a decentralized and immutable ledger structure which ensures data integrity, transparency, and traceability which reduces the risk of data tampering. In finance, block-chain enhances transaction security and strengthens identity verification mechanisms.

4.1.3 Cloud-based Security Platforms

Cloud-based security platforms provide centralized solutions for cyber security in finance. These platforms offer advanced threat detection, real-time monitoring, and automated response capabilities for cloud infrastructure's scalability. Financial institutions benefit from enhanced data protection, and secure access controls, and have continuous compliance management in cloud environments.

V. REGULATORY COMPLIANCE AND DATA PROTECTION

5.1 Overview of Key Regulations

5.1.1 General Data Protection Regulation (GDPR)

GDPR was enforced by the European Union (EU) and establishes rules regarding data processing, storage, and transfer emphasizing data privacy, transparency, and user consent. GDPR mandates stringent data protection measures including encryption, access controls, and data minimization which are crucial for safeguarding sensitive financial data. GDPR imposes strict penalties for non-compliance with fines up to €20 million or 4% of global annual turnover, whichever is higher [6].

5.1.2 California Consumer Privacy Act (CCPA)

Enacted in California, CCPA focuses on enhancing consumer privacy rights. It grants consumers the right to know, delete, and opt out of the sale of their data, with penalties for non-compliance. CCPA applies to businesses that collect or process personal information of California residents.

5.1.3 Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is developed by the payment card industry security standards council which sets requirements for securing payment card data. It applies to businesses that handle credit card information which requires them to implement security controls such as encryption, access controls, and network monitoring.

In February 2003, Data Processors International, which handles credit card transactions, lost between five to eight million credit card account numbers. This happened because their computers were hacked. It was estimated that it would cost the credit card companies involved around $200 million to replace all the affected cards [11].

5.2 Strategies for maintaining compliance while enhancing security

5.2.1 Compliance Alignment

Align security posture with regulatory requirements such as GDPR, PCI DSS etc. [13] explores regulatory compliance issues for large public entities. Information governance helps the entities to take necessary action during major breach of clients' personally identifiable information. No governance plan can make the loss felt both personally and financially.

5.2.2 Certification Pursuit
Pursue certification like ISO 27001, SOC 2, or PCI DSS to demonstrate commitment to cyber security best practices, independent evaluations, and effective protection of sensitive information.

5.2.3 Resource Management
Address the resource constraints by allocating funding, manpower, and expertise effectively to create and maintain robust security controls.

5.2.4 Threat Awareness
Stay abreast of evolving threats through continuous monitoring, threat intelligence, and technology updates to adapt security posture accordingly.

5.2.5 Continuous Improvement
It is crucial to conduct regular risk assessments, and audits to identify weaknesses, and prioritise security enhancements to develop resilience in cyber security.

VI. BUILDING A RESILIENT CYBERSECURITY CULTURE

6.1 Importance of Staff Training and Awareness Programs

To build a resilient cyber security culture, training and awareness becomes important because:
Security awareness training equips employees with the knowledge and skills to recognize potential cyber threats like phishing attempts which are a crucial contributor to data breaches.
A well-implemented security awareness program creates a culture of security within the organization. A study by [14] presents cyber resilience framework to strengthen organizational defences against cyber threats. The key components include governance and leadership, collaboration, and continuous monitoring.
While technological defense is crucial, they are only as effective as the people who manage them. Security training complements technological defences by ensuring that employees understand how to use security tools effectively by following secure protocols and reporting suspicious activities promptly.

6.2 Tips for Developing a Security-First Mindset

JP Morgan is often cited as one of the banks in America with a strong security-first mindset [7]. The company has proactively addressed emerging cyber threats and collaborated with industry leaders to enhance cyber security practices.
Here are some of the tips for developing a security-first mindset in financial organizations [8]:

- Understand your customer's security concerns as a financial organization by conducting surveys, interviews, or focus groups.

- Develop a cyber incident response plan tailored to specific risks faced by the organizations.
- Allocate sufficient funds and resources in the budget for cybersecurity initiatives.
- Security awareness training should consist of topics on phishing awareness, data protection best practices, and incident reporting procedures.

VII. CONCLUSION

- The critical importance of robust data protection strategies for financial institutions is emphasized due to the sensitive nature of the information they handle.
- The whitepaper highlights the increasing sophistication, frequency, and diversity of cyberattacks targeting financial institutions.
- The paper stresses the necessity of aligning security measures with key regulations such as GDPR, CCPA, and PCI DSS, with the benefits of pursuing certifications like ISO 27001.
- Overall, this study depicts the need for a comprehensive and adaptive approach to data protection and cybersecurity in financial institutions to safeguard sensitive information and ensure business continuity.

REFERENCE

1. Federal Trade Commission. 2022. Equifax Data Breach Settlement. Federal Trade Commission. Available: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
2. Fortinet. 2023. What is Brute Force Attack? | Definition, Types & How It Works. Fortinet. Available: https://www.fortinet.com/resources/cyberglossary/brute-force-attack#:~:text=A%20brute%20force%20attack%20is
3. Imperva. What does DDoS Mean? | Distributed Denial of Service Explained. Imperva Learning Center. Available: https://www.imperva.com/learn/ddos/denial-of-service/
4. P. Mahendru. 2023. The State of Ransomware in Financial Services 2023. Sophos News, Jul. 13. Available: https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/
5. KPMG. 2022. Cybersecurity: 2022 Banking Industry Survey. KPMG. https://kpmg.com/us/en/articles/2022/cybersecurity.html
6. IT Governance. 2023. GDPR Penalties & Fines | What's the Maximum Fine in 2023? itgovernance.co.uk. Available: https://www.itgovernance.co.uk/dpa-and-gdpr-penalties#:~:text=Higher%20level%20of%20GDPR%20penalties

7. JP Morgan. 2021. Fraud +Cybersecurity. Available: https://www.jpmorgan.com/content/dam/jpm/commercial-banking/solutions/fraud/1071733_2021_fallcybermag_issue11-ada-final.pdf

8. C. Novak. 2023. Council Post: Creating A Security-First Mindset. Forbes. Availablehttps://www.forbes.com/sites/forbestechcouncil/2021/10/28/creating-a-security-first-mindset/?sh=c30447e1bed7

9. C. Meurisch and M. Mühlhäuser. 2021. Data Protection in AI Services. ACM Computing Surveys, vol. 54, no. 2, pp. 1–38, Apr. DOI: https://doi.org/10.1145/3440754.

10. P. P. Swire. 1999. Financial Privacy and the Theory of High-Tech Government Surveillance. Washington University Law Quarterly, vol. 77, p. 461. Available: https://heinonline.org/HOL/LandingPage?handle=hein.journals/walq77&div=21&id=&page=

11. J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle, and V. Singh. A Survey of Payment Card Industry Data Security Standard. IEEE Journals & Magazine. Available: https://ieeexplore.ieee.org/abstract/document/5455788

12. T. Oyewole, B. Oguejiofor, None Nkechi Emmanuella Eneh, None Chidiogo Uzoamaka Akpuokwe, and S. Bakare. 2024. DATA PRIVACY LAWS AND THEIR IMPACT ON FINANCIAL TECHNOLOGY COMPANIES: A REVIEW. Computer Science & IT Research Journal, vol. 5, no. 3, pp. 628–650, Mar. DOI:https://doi.org/10.51594/csitrj.v5i3.911.

13. J. G. Iannarelli and M. O'Shaughnessy. 2014. Information Governance and Security: Protecting and Managing Your Company's Proprietary Information. Butterworth-Heinemann.
Available:https://books.google.co.in/books?hl=en&lr=&id=FiSOAwAAQBAJ&oi=fnd&pg=PP1&dq=Guarding+the+Vault:+Data+Protection+Strategies+for+Financial+Institutions

14. AL-Hawamleh. 2024. Cyber Resilience Framework: Strengthening Defences and Enhancing Continuity in Business Security. International Journal of Computing and Digital Systems, vol. 15, no. 1, pp. 1315–1331, Mar. DOI: https://doi.org/10.12785/ijcds/150193.