International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Data Breach as a Threat in the Banking Sector and Steps to Avoid It

Priyanka Gowda[1], Ashwath Narayana Gowda[2]

America First Credit Union, UT
Email: *an.priyankagd[at]gmail.com*

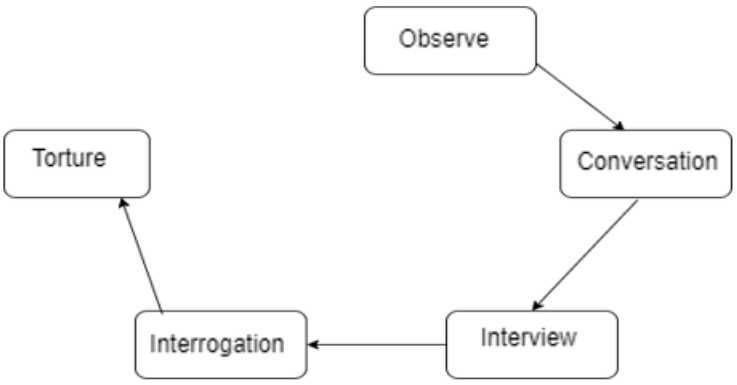
Abstract: ***Following the COVID19 pandemic, the frequency of cyberattacks has surged, significantly impacting the banking sector. This paper examines various types of cyber threats including phishing, malware, ransomware, insider threats, SQL injection, crosssite scripting XSS, maninthemiddle attacks, and unpatched software vulnerabilities. These threats pose significant risks to financial institutions by compromising sensitive information and disrupting operations. The role of software developers is critical in mitigating these risks through secure software development practices, including encryption, multifactor authentication, regular system upgrades, and the use of intrusion detection systems. This paper emphasizes the importance of a collaborative approach among software developers and stakeholders to safeguard banking systems against cyberattacks.***

Keywords: cyberattacks, banking sector, phishing, malware, software security

Introduction

Following the COVID 19 pandemic, cyberattacks increased exponentially [1]. This led to increased losses by companies in the recent days. From the Global Financial Stability Report of 2021, there exists an increased predisposition to extreme losses that result from cyberattacks. This calls for software developers and other key stakeholders in this sector to harmoniously work together and ensure the banking sector is protected from losses that result from cyberattacks. Software developers play a significant role in the banking sector. They develop and install secure software on behalf of the banking entities. Such software should be secure enough. Therefore, those tasked with development and installation of the software should ensure that the software installed is resistant to cyberattacks and therefore secure enough for banking companies.

First, we will discuss different types of threats in the banking sector. These threats include: phishing attacks, malware and ransomware, insider threats, SQL injection, cross - site scripting, man - in - the - middle attacks and un - patched software. Phishing attacks have been on the rise in the recent days. They involve sending of fake emails, text messages and even direct communication through phone calls to legitimate bank account holders tricking them to share sensitive information with fraudsters. Unlike other cyberattack measures, phishing attacks are a form of social engineering that directly targets one's psychology [2]. In a typical case, the fraudster poses as a colleague or someone that the victim trusts. The hacker sends a message that calls for a direct payment of a specific invoice from the victim. Just a simple click on the purported invoice shares personal information with the hackers and they can empty the victims account in seconds. Phishing as a form of cyberattacks is a highly effective social engineering tool. Social engineering tools require building of a relationship based on trust and follows the steps below:



The employment of malware and ransomware is another threat in the banking sector. Malware is a form of malicious software that is designed to damage or gain access to secure computer systems. Ransomware on the other hand is meant to encrypt personal customer information and demands payment for the decryption key. There includes many types of malware and ransomware. These are: Trojans, spyware, and keyloggers. Trojans are used in disguising legitimate payments and deliver malicious payloads. Spyware collects sensitive information without the knowledge of the user and sends it to fraudsters who misuse it in making fraudulent transactions. Keyloggers on the other hand record keystrokes that capture sensitive customer data like passwords that are essential in accessing the necessary account information to enable fraudulent transactions. If the malware or ransomware is directed towards a banking company it can result in

financial loss, disruptions in operations and even a damage in company reputation.

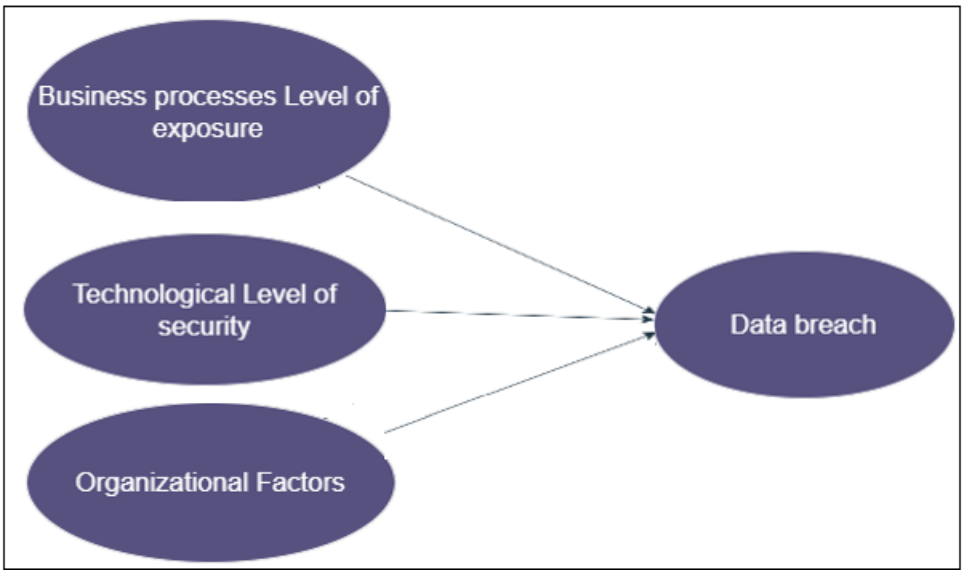
Insider threats majorly arise from employees or trusted individuals within the company. They misuse their selective privilege in accessing the organizations data and secure systems. They can either intentionally bring harm to the company by stealing sensitive data or damaging the data, they can also unintentionally cause harm through the careless handling of data, or be compromised insiders who steal the organizations data and trade it to external attackers. This can result in operational disruptions and financial losses if the stolen data is used by the fraudsters. SQL injection on the other hand occur when fraudsters insert malicious SQL codes in an input field that then exploits the vulnerabilities in the applications database layer. Different methods of SQL injections are available. These include: classic SQL injection that involves the manipulation of SQL queries to gain unauthorized access to retrieve sensitive data, and blind SQL injection that exploits the database by sending queries that give no visible result and are used to get information based on the applications behavior. Such unauthorized access to sensitive information make it easy for fraudsters to conduct financial fraud among other economic crime to the banking company.

Cross - Site Scripting or otherwise what is termed as XSS is a form of cyberattack that involves the use of malicious scripts that are injected into web applications. These scripts are the executed in the browsers of users who visit the compromised web page. Different types of Cross - Site Scripting exist. These include: stored XSS, reflected XSS, and DOM - based XSS. For stored XSS the malicious script is normally stored on the server and served to users. Reflected XSS involves the reflection of the script off a webserver via URL link. DOM - based XSS on the other hand manipulates the document object model of the page and executes the malicious scripts making it easy for fraudsters to engage in data theft, hijacking of sessions, and even the defacement pf the website.

Man in the middle attacks is type of cyberattacks when a single cyber attacker interferes with the communication between two parties without the knowledge of either party. This can lead to sharing of personalized information with the wrong party and therefore allow the committing of financial fraud. Different methods to conduct Man in the Middle attacks are available. They include: eavesdropping, session hijacking, and SSL stripping. Eavesdropping involves listening or reading of the data being exchanged in a passive manner. This often goes unnoticed. Session hijacking involves the taking over of active sessions between the client and the server and therefore result in the theft of sensitive information. SSL stripping involves the downgrading of HTTPS connections which are secure to HTTP which are relatively insecure with an aim of intercepting traffic to these sites. This attack results in compromised communication and breeds ground for financial fraud.

Finally, un - patched software involves taking advantage of the vulnerabilities in outdated systems by attackers. They manipulate these systems and get unauthorized access to steal sensitive information necessary in conducting a transaction. They can also do this and result in session interruptions in banking companies which steadily rely on the installed software to function properly i. e. is essential in guiding customers to the proper stands. Different methods of conducting un - patched software are in existence, one such method is exploitation of known vulnerabilities where publicly available information about software vulnerabilities can be used to launch attacks. Another method is Zero - day exploits where attacks are launched on vulnerabilities that are unknown to the software developer and vendor and therefore lack a remedy to it.

We also need to understand the conceptual model of data breach factor. Below is a diagram showing the conceptual model of data breach factors:



The above - mentioned factors are key to software developers as they are mostly considered to ensure the system developed is secure.

Understanding of how cyberattacks are conducted is very essential for software developers as it enables them to understand areas of vulnerability that are manipulated by

fraudsters when committing financial crimes. This will ensure proper patching up and care when developing software for the banking sector. To ensure mitigation of data breaches in the banking sector, software developers need to employ secure coding practices. This is essential in the protection of sensitive bank information. Software developers need to validate the inputs to ensure that it is correct and free from malicious content such as SQL injections and also vulnerabilities to Cross - Site - Scripting attacks. Prior to installation of a software, different parameterized queries that check for vulnerability to SQL injection should be used [3]. Furthermore, the use of multi - factor authentication methods before accessing sensitive information will further secure bank information. These should be incorporated by software developers to ensure that the installed software is safe and relatively resistant to cyberattacks.

Developers should also ensure that sensitive information is encrypted as a way of maintaining the integrity of the data. Encryption is one of the effective ways of preventing data breaches. As a tool for data security, encryption converts plaintext data to cipher - text data and therefore makes it unreadable to unauthorized individuals. This maintains the confidentiality of sensitive data by making it unreadable to unauthorized individuals. Software developers therefore need to use strong encryption codes that will help banking companies to safeguard sensitive information. Furthermore, these encryption codes should not only prevent unauthorized access during storage but also during transmission to avoid Man in the Middle Attacks. The encryption codes used should properly authenticate entities and verify their identity before allowing access to sensitive information. The use of Public Key Infrastructure (PKI), can be used to establish trust between parties by using asymmetric encryption algorithms. This ensures that only trusted individuals can access sensitive data. This ensures that data stored and transmitted is very safe and free from cyberattacks.

As a software developer, advocating for regular system security checks and upgrading should be my topmost priority. Being the knowledgeable expert in matters technology, I should advice banking companies that buy software to always ensure that their systems are regularly upgraded to the latest version and they are also checked for being secure or not. As a developer, conducting code audits or reviews will help in uncovering potential issues in the code. Furthermore, conducting penetration tests will also come in handy. These tests mimic real-world attacks [4]. This therefore aids in identification of vulnerabilities of the code before its incorporation in a banking system. Software developers should also work to incorporate automatic security testing tools in the software. This allows for early detection of security breaches or weaknesses of the software after its incorporation in a functioning banking system.

Continuous monitoring of the installed system and having an appropriate incident response plan is essential for early detection and mitigation of data breaches on an operational banking system. Intrusion Detection Systems are good at monitoring suspicious activity in an installed software. Two types of Intrusion Detection Systems are available and in use. They include the network-based intrusion detection systems and the host based intrusion detection systems. The former deals with analysis of traffic across network. These systems are placed at specific points within the network to ensure their efficient functionality. It employs signature-based detection methods and anomaly-based detection methods. The former also compares real time network traffic against a database of known attack signature. However, it has a lower level of specificity [5]. The latter establishes a baseline of normal network behavior and flags any slight deviation from the normal. Host based intrusion detection systems on the other hand monitor the activity and state of individual hosts and devices. The check for file integrity by monitoring important files and configurations for unauthorized changes. It also does log analysis where it examines the system and application logs for any sign of suspicious activity. This helps in early detection of threats or potential threats, and therefore allows time for early response and mitigation of threats.

The use of secure software development cycle is also important in minimizing data breaches. As a software developer, incorporation of security measures in to every cycle of software development is helpful in the mitigation of security risks after the use of a software. Right from the beginning of software development, measures should be in place to ensure the system developed is as secure as possible. First, conduction of threat modeling during the design phase is critical. This aids in the identification of potential security risks to the software. With created awareness, care is taken to ensure that the system is free and resistant from these risks. Furthermore, making security as a priority during the development of the software will prove beneficial.

Software developers play a crucial role in ensuring the safety of the software in the banking sector. Right from the design phase to the implementation phase security of the software should be a priority. Therefore, as software developers, the use of encryption algorithms, conduction of security testing, and constant monitoring of the installed software are key areas of focus in ensuring the safety of their software. This not only protects their interests and reputation as developers but also ensures their customers are satisfied and run their businesses smoothly without interference from hackers.

References

[1] Chigada, J. & Madzinga, R. (2021, February). Cyberattacks and Threats During COVID - 19: A Systematic Literature Review. SA Journal of Information Management. https: //www.researchgate. net/publication/349448944_Cyberattacks_and_threats_ during_COVID - 19_A_systematic_literature_review
[2] Andress, J. & Winterfeld, S. (2011). Cyber Warfare: Chapter 7 - Psychological Weapons. Pg 139 - 153 https: //www.sciencedirect. com/science/article/abs/pii/B9781597496377000071
[3] Turpin, K. & Gadsden, J. (2019). OWASP Secure Coding Practices Quick Reference Guide. https: //owasp. org/www - project - secure - coding - practices - quick - reference - guide/
[4] Johnson, L. (2020). Security Controls Evaluation, Testing, and Assessment Handbook 2nd Edition: Chapter 10 - System and Network Assessments.

https: //www.sciencedirect. com/science/article/abs/pii/B9780128184271000100
[5] Wilhelm, T. & Andress, J. (2011). Ninja Hacking: Chapter 8 - Use of Timing to Enter an Area. https: //www.sciencedirect. com/science/article/abs/pii/B9781597495882000081