CYBER SECURITY- SECURITY PROTOCOLS AND MEASURES IN BANKING SECTOR

P.Maheshwari[1]

Abstract

Digital transformation is not only adopting new software, technologies, and processes that are more efficient and automated than traditional business practices and processes; it's an entirely new, innovative way of doing something that is core to your business. That means organizations must consider everything when taking on a digital transformation initiative – from how people will react to the change, how it will impact customer relations, the cost, how it will align to business goals, and so forth. Digital transformations empower organizations to take their business into the future, and position companies to withstand competition and grow into new areas. The 1970s saw the actual start of cyber security. It was an important decade in the evolution of cyber security. The Advanced Research Projects Agency Network (ARPANET) was the initial endeavor in this. Before the internet was created, this connectivity network was constructed.

Cyber security refers to every aspect of protecting an organization and its employees and assets against cyber threats. As cyber attacks become more common and sophisticated and corporate networks grow more complex, a variety of cyber security solutions are required to mitigate corporate cyber risk. In the banking sector, cyber security and security protocols are crucial to ensure the confidentiality, integrity, and availability of sensitive financial data and transactions. Some of the specific security protocols used in the banking sector include Access Control, Encryption, Two-Factor Authentication (2FA), Firewalls, Intrusion Detection and Prevention Systems (IDPS), Virtual Private Network (VPN), Anti-virus and anti-malware software.

Keywords: Cyber security, Security protocols, Data breaches, Cyber threats, Encryption.

1 Assistant Professor, Lal Bahadur College, Warangal, Email:maheswari.makula@gmail.com

Introduction

With an increase in digitalization, Cyber security threats have also grown tremendously. You may have heard recently about billions of dollars being skimmed off belonging to the largest financial institutions. As the world is being increasingly connected digitally, it has also opened up entry points for cybercriminals; therefore, Cyber security in digital banking is the need of the hour. There have been breaches of data of technologically savvy banks. In the banking sector, cyber security and security protocols are crucial to ensure the confidentiality, integrity, and availability of sensitive financial data and transactions. Some of the specific security protocols used in the banking sector.

Access Control: Access control refers to the process of managing access to computer systems, networks, and data. Banks use access control measures, such as passwords, biometric authentication, two-factor authentication, and other security protocols, to ensure that only authorized personnel have access to sensitive data and systems.

Encryption: Encryption is the process of converting plaintext data into cipher text to protect it from unauthorized access. Banks use various encryption methods, such as symmetric encryption, asymmetric encryption, and hashing, to secure sensitive data, such as passwords, PINs, and transaction details.

Two-Factor Authentication (2FA): 2FA is a security protocol that adds an extra layer of authentication beyond a username and password. Banks use 2FA methods, such as biometric authentication (such as fingerprints or facial recognition), physical tokens (such as smart cards), or one-time codes sent via SMS or email, to ensure that only authorized users have access to sensitive data and systems.

Firewalls: A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Banks use firewalls to prevent unauthorized access to their networks and protect against malware and other cyber threats.

Intrusion Detection and Prevention Systems (IDPS): IDPS is a security protocol that monitors network traffic for suspicious activity and blocks threats such as viruses, worms, and malware. Banks use IDPS to detect and prevent attacks such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.

Virtual Private Network (VPN): A VPN is a network protocol that allows users to connect to a private network over a public network securely. Banks use VPNs to provide remote access to employees while ensuring the security of their network.

Anti-virus and anti-malware software: Banks use anti-virus and anti-malware software to protect against malicious software, including viruses, worms, and trojans. These tools are used to scan their systems for malware and prevent attacks. Overall, the use of cyber security and security protocols in the banking sector is crucial to prevent data breaches, protect against cyber threats, and ensure the privacy and security of sensitive financial data and transactions.

Review of Literature

Cyber security refers to the organization of technologies, procedures, and methods designed to prevent networks, devices, programs, and data from attack, damage, malware, viruses, hacking, data thefts or unauthorized access. The main objective of Cyber security in banking is to safeguard the user's assets. As individuals go cashless, further actions or transactions are done online. Individual's use their digital money like debit cards and credit cards for transactions that require to be safeguarded under Cyber security. Cyber security is not only restricted to IT organizations, it is important for every single business. But, for banks, it holds important value. Banks deal in millions of transactions on a regular basis. Hence, it is very important for banks to take protective security procedures to safeguard their data against cyber attacks. Here are some reasons why cyber security is essential for banks.

Objectives

1. To know the Cybercrime, Risks and Prevention
2. To examine to Avoid Most Types of Cybercrime
3. To create awareness how to protect yourself against cybercrime

The threats countered by cyber-security are three-fold:

Cybercrime: It includes single actors or groups targeting systems for financial gain or to cause disruption.

Cyber-attack: It often involves politically motivated information gathering.

Cyber terrorism: It is intended to undermine electronic systems to cause panic or fear. So, how do malicious actors gain control of computer systems.

Malware: Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

Ransom ware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware: Advertising software which can be used to spread malware.

Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

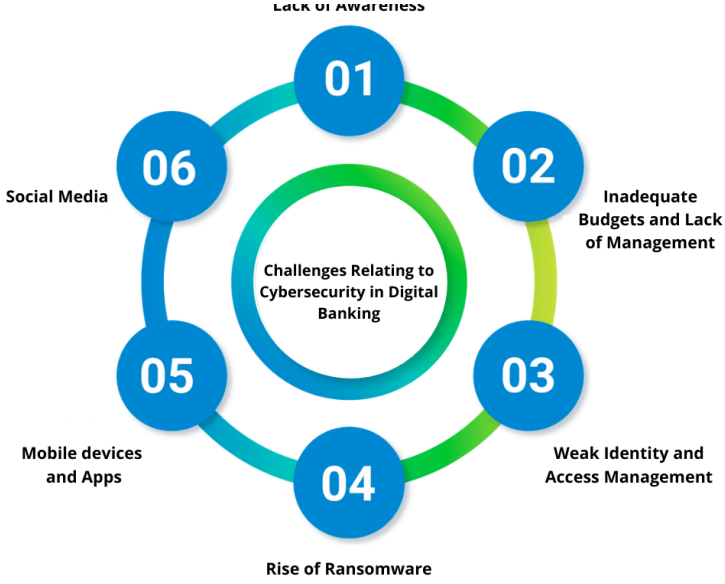
SQL injection: An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing: Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack: A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack: A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Challenges relating to Cyber security in digital banking



Lack of Awareness: Awareness among the people regarding the Cyber security has been quite low, and not many firms invest in training and improving the overall Cyber security awareness among the people.

Inadequate Budgets and Lack of Management: Cyber security is accorded low priority; therefore, they are most of the time neglected in the budgets. Top management focus also remains low on Cyber security, and support for such projects is given low priority. This may be because they misjudge the impact of these threats.

Weak Identity and Access Management: Identity and access management has been the fundamental element of Cyber security and especially in these times when the hackers have the upper hand; it may require only one hacked credential to enter into an enterprise network. There

has been a slight improvement in this regard, but still, a lot of work remains to be done in this area.

Rise of Ransom ware: The recent events of malware attacks bring our focus to rising menace of ransom ware. Cybercriminals are starting to use methods that avoid them to be detected by endpoint protection code that focuses on executable files.

Mobile devices and Apps: Most of the banking institutions have adopted mobile phones as a medium to conduct business. As the base increases each day, it also becomes the ideal choice for exploiters. Mobile phones have become an attractive target for hackers as we see a rise in mobile phone transactions.

Social Media: Adoption of social media has led to hackers to exploit even more. Less aware customers put out their data for anyone to see which is exploited by the attackers.

Protect against cyber attacks

- Update your software and operating system: This means you benefit from the latest security patches.
- Use anti-virus software: Security solutions will detect and removes threats. Keep your software updated for the best level of protection.
- Use strong passwords: Ensure your passwords are not easily guessable.
- Do not open email attachments from unknown senders: These could be infected with malware.
- Do not click on links in emails from unknown senders or unfamiliar websites. This is a common way that malware is spread.
- Avoid using unsecure WiFi networks in public places: Unsecure networks leave you vulnerable to man-in-the-middle attacks.

Conclusion

Cyber security is a global area designed to protect and monitor networks, computers, data, and applications from unauthorized access or abuse. The most important task of a cyber security analyst is to protect the network against damage. In this study, we describe cyber-attacks related to information, threats, major challenges, as well as solutions to crime control, some

cyber-security attacks, and solutions to overcome cyber-attacks. In addition, we introduce and discuss cyber security and its importance. In addition, it analyzes the security of related information, cybercrime and cyber-attacks. Banks are the financial backing of the country and the tools available to individuals and institutions. A healthy banking institution / bank credit should not be compromised in any way. Now is the time for banks to move beyond their traditional banking framework and work in a team spirit with new technology and new perspectives to eliminate or minimize cyber threats in the system. Overall, the use of cyber security and security protocols in the banking sector is crucial to prevent data breaches, protect against cyber threats, and ensure the privacy and security of sensitive financial data and transactions.

References

1. https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security
2. https://intellipaat.com/blog/cyber-security-in-banking
3. https://www.researchgate.net/publication/358093947_Evaluation_of_Cyber_Security_Threats_in_Banking_Systems