VOLUME:2 ISSUE:1

IMPORTANCE OF CYBERSECURITY IN DIGITAL BANKING ERA

Mashhura Ruziboyeva
Jahon Iqtisodiyoti va Diplomatiya universiteti
Tashqi Iqtisodiy Faoliyat yo'nalishi magistranti

Annotation: *This article emphasizes the significance of cybersecurity in the context of digital banking. It highlights the potential consequences of security breaches, such as financial loss, identity theft, and reputational damage for both banks and their customers. The article may discuss the evolving nature of cyber threats, including phishing, malware, ransomware, and social engineering techniques, and how they specifically target the banking sector. Furthermore, the article may delve into the various cybersecurity measures and best practices that banks should adopt to mitigate risks. This could include implementing robust encryption protocols, multi-factor authentication, regular security audits, employee training programs, and establishing incident response plans. The importance of collaboration between banks, regulatory bodies, and cybersecurity experts may also be emphasized in the article. It may highlight the need for continuous monitoring, threat intelligence sharing, and staying updated with the latest security technologies and trends.*

Keynotes: *Cybersecurity, threats for cybersecurity, banking sector, digital technologies, machine learning, artificial intelligence.*

Introduction.

In today's rapidly evolving digital landscape, the banking industry has undergone a significant transformation. With the advent of online banking, mobile applications, and digital transactions, customers now enjoy unprecedented convenience and accessibility. However, this digital revolution has also brought forth new challenges, particularly in the realm of cybersecurity.

This article delves into the paramount importance of cybersecurity in the digital banking era. It explores the critical role it plays in protecting sensitive financial information, maintaining customer trust, and ensuring the overall stability of the banking sector. As cyber threats continue to evolve and grow in sophistication, banks must remain vigilant and proactive in safeguarding their systems and customer data.

The article highlights the potential consequences of security breaches in the digital banking realm. Financial loss, identity theft, and reputational damage are just a few of the devastating outcomes that can occur when cybersecurity measures fall short. By understanding the gravity of these risks, banks can better appreciate the urgency of implementing robust security measures.

Furthermore, the article delves into the evolving nature of cyber threats that specifically target the banking sector. From phishing attacks and malware infections to ransomware and social engineering techniques, hackers are constantly devising new methods to exploit vulnerabilities. It emphasizes the need for banks to stay ahead of these threats by adopting proactive security measures and staying informed about emerging trends.

The article also explores the various cybersecurity measures and best practices that banks should adopt to mitigate risks. Robust encryption protocols, multi-factor authentication, regular security audits, and employee training programs are just a few examples of the strategies that can help fortify a bank's defenses. Additionally, it emphasizes the importance of establishing comprehensive incident response plans to minimize the impact of potential breaches.

Collaboration is another key aspect highlighted in the article. It emphasizes the need for banks to work closely with regulatory bodies and cybersecurity experts to share threat intelligence, stay updated with the latest security technologies, and collectively combat cyber threats. By fostering a collaborative environment, the banking industry can enhance its collective resilience against cyberattacks.

Methodology

Security in banking is a critical aspect, given that banks process large volumes of sensitive information and perform financial transactions. Here are a few key security aspects in the banking sector:

- Data protection: Banks are required to ensure confidentiality customer data. Using modern encryption technologies to Protection of stored and transmitted information is mandatory.
- Authentication and Authorization: Banks must have strong systems authentication to confirm the identity of clients. Two-factor authentication (2FA) is becoming standard practice to improve security.
- Transaction monitoring: Transaction monitoring systems help detect suspicious activity and prevent fraud. Automated behavior analysis systems can quickly identify unusual or suspicious transactions.
- Protection against malware: Banks must use antivirus programs, anti-phishing filters and others tools for protection against malware and software attacks.
- Physical security: Physical facilities of banks such as offices and data centers must be reliably protected from unauthorized access. CCTV cameras, biometric authentication and other physical security are important role.
- Staff training: Training bank employees on the rules security and social engineering prevention methods are also extremely important. Employees must be alert and know how to recognize potential threats.
- Regular audits and security testing: Banks should conduct regular security audits and penetration testing to identify weaknesses in their systems and processes.
- Protection against denial of service (DoS): Banks must have mechanisms protection against DoS attacks to prevent blocking access to your online resources.

These measures help banks create resilient and secure systems, protecting your clients and your own reputation from various threats kind.

With the transition to a digital economy, cybersecurity in banking sector is becoming a serious problem. Use of methods and procedures designed to protect data is essential for successful digital revolution. The effectiveness of cybersecurity in banks affects security of our personal information (PII), whether unintentional a breach or well-planned cyberattack.

A set of technologies, protocols and methods called "cybersecurity", protects you from attacks, damage, malicious programs, viruses, hacking, data theft and unauthorized access to networks, devices, programs and data.

The main goal of cybersecurity in the banking sector is ensuring the protection of personal data and assets of clients, especially in conditions growing online banking and digital payments. People commit transactions using digital payment methods such as debit and credit cards that must be protected by funds cybersecurity.

Threats for Cybersecurity in Digital Banking Engage your Audience

The most common threats for cybersecurity in digital banking are unencrypted data, malware, third-party services, spoofing and phishing. Without a robust Cybersecurity measure in place, your sensitive data may be at risk.

Unencrypted data

It is one of the common threats faced by the banks where the data is left unencrypted, and hackers or cybercriminals use the data right away, thereby creating severe issues for the financial institution.

Malware

End to end-user devices like computers and mobile devices are mostly used for conducting digital transactions; therefore, it must be secured. If it is compromised with malware, then it may pose a serious risk to the bank’s Cybersecurity whenever they connect with your network.

Many banks and financial institutions use third-party services from other vendors to serve their customers better. However, if these vendors don’t have a tight Cybersecurity measure, then the bank that has employed them will suffer badly.

Spoofing

This is one of the newest forms of cyber threats faced by banks. The cybercriminals will impersonate a banking website’s URL with a website that is similar to the original one and functions the same way and when the user enters his or her login credentials that login credentials are stolen by these criminals and use it later.

This cyber threat has gone to the next level where new spoofing techniques have been employed by these criminals. In this, they use a similar URL and target users who visit the correct URL.

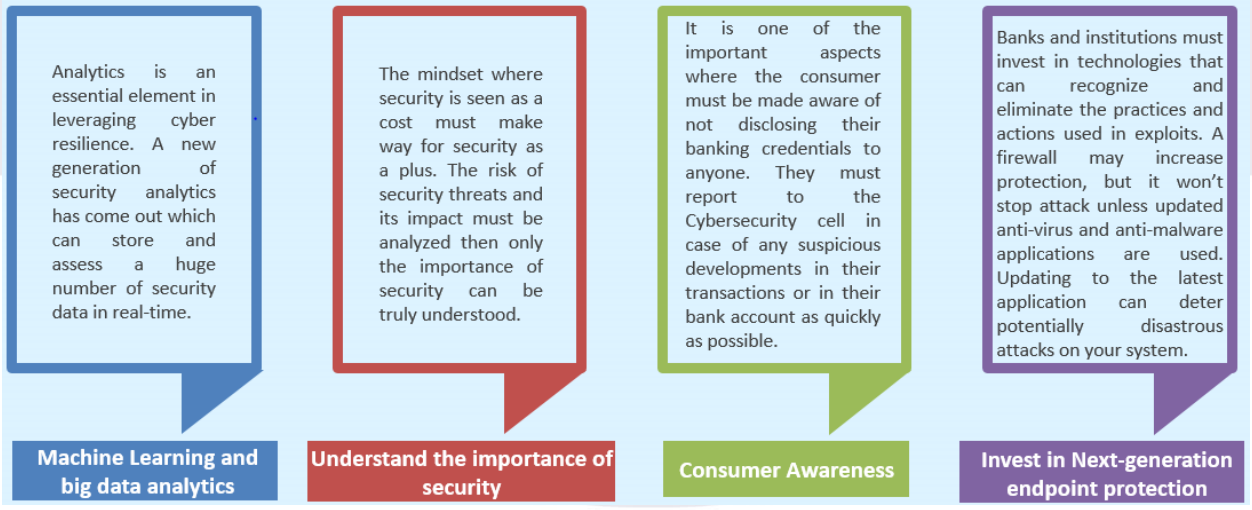
Awareness among the people regarding the Cybersecurity has been quite low, and not many firms invest in training and improving the overall Cybersecurity awareness among the people.

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. For example, On January 26, 2022, the TeaBot and FluBot banking trojans were detected to be targeting Android devices once again.

Rise of Ransomware

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

There are also solutions to the threat to the cybersecurity in digital banking sector.



Picture 1. Samples of solutions to the threats to the security of banking sector

Cases of Attack in Cybersecurity in Digital Banking

In India, banks have seen relentless attacks from organized criminals and hackers. It was illustrated in a recent case with Canara Bank where a hacker attacked and defaced the bank's site by inserting a malicious page and tried blocking some of the bank's e-payments.

Since November 2021, the banking trojan Zloader has been exploiting Microsoft's digital signature verification method to inject malicious code into a signed system dynamic link library (DLL).

On October 29, 2021, the National Bank of Pakistan suffered a destructive cyberattack, which is said to have impacted some of its services including the bank's ATMs, internal network, and mobile apps.

On September 8, 2021, the websites of various New Zealand financial institutions and the national postal service were down due to a suspected cyberattack.

On June 4, 2021, Fiducia & GAD IT, a German company that operates technology on the nation's cooperative banks, was hit by a DoS attack, disrupting more than 800 financial institutions in the country.

From May to August 2021, researchers from Cyren reported a 300% increase in phishing attacks targeting Chase Bank.

The Reserve Bank of New Zealand suffered a data breach after actors illegally accessed its information through one of the bank's third-party file sharing services.

Conclusion and Implications

Based on a review of existing literature, conclusion of the article on the importance of cybersecurity in the digital banking era would likely emphasize the need for a proactive and comprehensive approach to cybersecurity. It would highlight that cybersecurity is not just a responsibility of banks, but also of individual customers and regulatory bodies.

The implications of the article would include the following:

Heightened Awareness: The article would emphasize the need for individuals to be aware of the potential risks and take necessary precautions when engaging in digital banking activities. This could include regularly updating passwords, being cautious of phishing attempts, and monitoring account activity.

Regulatory Focus: The article may suggest that regulatory bodies should prioritize cybersecurity in their policies and regulations. This could involve setting minimum security standards for banks, conducting regular audits, and enforcing penalties for non-compliance.

Collaboration and Information Sharing: The article would likely stress the importance of collaboration between banks, cybersecurity experts, and regulatory bodies. Sharing information about emerging threats and best practices can help strengthen the overall security posture of the banking industry.

Investment in Technology: The article may imply that banks should invest in advanced cybersecurity technologies and solutions to protect their systems and customer data. This could include implementing artificial intelligence and machine learning algorithms for threat detection and prevention.

Continuous Improvement: The article would likely highlight that cybersecurity is an ongoing process and that banks should continuously update their security measures

to stay ahead of evolving threats. This could involve regular training for employees, conducting penetration testing, and staying updated with the latest security trends.

In conclusion, the article would emphasize that cybersecurity is a critical aspect of the digital banking era and that all stakeholders, including banks, customers, and regulatory bodies, must work together to ensure the security and integrity of the banking system.

List of used literature:

1. Kochayeva A.R. Yolliyev A.B. Journal of "SECURITY IN THE BANKING SECTOR: KEY ASPECTS AND ROLE OF CYBER SECURITY IN THE DIGITAL ECONOMY AGE", 2023, №5, pages 126-133. https://oaji.net/articles/2020/8467-1595185001.pdf
2. Alzoubi H. M. et al. Cyber Security Threats on Digital Banking //2022 1st International Conference on AI in Cybersecurity (ICAIC). – IEEE, 2022. – С. 1-4.
3. Rodrigues A. R. D. et al. Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework //Research in International Business and Finance. – 2022. – Т. 60. – С. 101616.
4. Abedin M. Z., Hajek P., Shilpa N. A. Cyber Security in Banking Sector //Cyber Security and Business Intelligence. – Routledge, 2023. – С. 37-45.
5. Stanikzai A. Q., Shah M. A. Evaluation of cyber security threats in banking systems //2021 IEEE Symposium Series on Computational Intelligence (SSCI).–IEEE, 2021. – С. 1-4 https://ieeexplore.ieee.org/abstract/document/9659862
6. Kumar, M. (2023). An Overview of Cyber Security in Digital Banking Sector. East Asian Journal of Multidisciplinary Research, 2(1), 43-52. https://journal.formosapublisher.org/index.php/eajmr/article/view/1671