Review

Cybersecurity & Data Privacy in Fintech

Rajath Karangara * and Otilia Manta *

Posted Date: 31 January 2024

doi: 10.20944/preprints202401.2194.v1

Keywords: Fintech; Cybersecurity; Data Privacy; Information Security; Regulatory Compliance

Review

Cybersecurity & Data Privacy in Fintech

Rajath Karangara [1,*] and Otilia Manta [2,3]

[1] American Express, Florida, United States of America (R.K)
[2] Romanian Academy, Victor Slăvescu" Centre for Financial and Monetary Research, Bucharest, 050711, Romania (O.M.); otilia.manta@icfm.ro
[3] Romanian American University, Bucharest, 012101, Romania (O.M.)
* Correspondence: rajathk2003@yahoo.co.in

Abstract: With the fintech industry growing at an unprecedented rate, it is critical to protect cybersecurity and ensure data privacy. The research presented here offers a thorough examination of the challenges faced by financial technology companies, highlighting the growing risks posed by malware, phishing, and network vulnerabilities. As essential components of a proactive defense plan, the report promotes strong cybersecurity measures like frequent security assessments, encryption, and stringent access controls. The findings highlight how important it is for fintech companies to give cybersecurity equal importance with open and honest data privacy policies in order to win over customers. In order to protect the industry from cybersecurity risks regulatory compliance, intrusion detection systems, and collaborative information sharing are considered essential components. The article advises businesses to include cybersecurity and data privacy into their core business operations and customer relations, highlighting the critical role these factors play in sustaining success in the rapidly evolving fintech industry.

Keywords: fintech; cybersecurity; data privacy; information security; regulatory compliance

1. Introduction

The rise of fintech has revolutionized the banking industry, offering unprecedented convenience and accessibility to consumers. However, with this advancement comes the increased risk of cybersecurity breaches and data privacy concerns. Fintech companies deal with sensitive financial information, making them attractive targets for cybercriminals. (Gai et al., 2018) As highlighted in the sources, the adoption of financial technology (fintech) has significantly impacted the banking industry. This paper provides a high-level overview of the challenges and considerations surrounding cybersecurity and data privacy in the fintech world.

Literature Review

Cybersecurity and Data privacy in the fintech industry have emerged as critical issues that demand attention. The rapid growth of fintech has raised concerns about the security and protection of sensitive financial data. The increasingly heavy reliance on digital platforms and mobile applications for financial transactions has created vulnerabilities that can be exploited by threat actors. The World Bank and CCAF report highlights that cybersecurity risks are the biggest concern for financial regulators in the fintech industry. Furthermore, the implementation of financial insurance and the understanding of cyber risks pose challenges for fintech companies.

"FinTech", a contraction of "Financial technology", refers to technology enabled financial solutions. It is often seen today as the new marriage of financial services and information technology (Arner, D. at all, 2016). In (Gai, K., at all, 2020), the authors investigate the definition of Fintech and measure the extent of the impact of Fintech variables on the Cybersecurity as the dependent variable. (Cukier, K., at all, 2018) a major theme in this book is that "big data" will become the dominant scientific paradigm, and change society—and it may yet. Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of

 doi:10.20944/preprints202401.2194.v1

Regulation (EU) No 1093/2010 to whom Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions (European Banking Authority, 2018). Special consideration is given to how blockchain-based identity and access management systems can address some of the key challenges associated with IoT security (Kshetri, N., 2017). Consumers, increasingly aware of their rights to privacy, may choose to seek alternative products and services in the absence of appropriate protections (International Association of Privacy Professionals, 2019). The Council is charged with identifying risks to the financial stability of the United States; promoting market discipline; and responding to emerging risks to the stability of the United States' financial system (Financial Stability Oversight Council, 2020). For example, in the paper (Smith, A. N., & Smith, B. L., 2018) they investigate the definition of Fintech and measure the extent of the impact of Fintech variables on Cybersecurity as the dependent variable. Beyond individual organizations, cyber risk is a systemic challenge and cyber resilience a public good. Every organization acts as a steward of information they manage on behalf of others. And every organization contributes to the resilience of not just their immediate customers, partners, and suppliers but also the overall shared digital environment (World Economic Forum, 2019). This study (Apostu, S. A., at all, 2022) may also help policymakers and regulators to structure and improve their policies toward investing in financial markets, as cryptocurrencies require multiple risk-mitigation approaches for investors and financial markets. As researchers and practitioners alike seek to identify new ways to solve business challenges, inspire financial innovation, and create and seize new opportunities, insurers around the world are increasingly teaming up with insurtechs, and other tech startups (Manta O, at all, 2023). There has been an increased recognition that more attention needs to be paid to AI, the internet of things, environmental, social, and governance (ESG), sustainability, adoption, and intelligent automation (Tong L, at all, 2022). Also in the specialized literature, we identified the work (Brooks C. J., et all, 2018), which offers clear and comprehensive details on cyber security, with a direct orientation towards current challenges, namely: how to secure the infrastructure, how to secure and control devices, how to secure of local and global networks, as well as securing and protecting the perimeter. This scientific work deals with each of these challenges and demonstrates to us through the analyzed scenarios, those vulnerabilities (Brooks C. J., et all, 2018), that each of the users of the systems may face in their daily professional life. It is particularly important that in the digital age, individual autonomy should prevail, and this aspect must be carefully protected through clear tools and mechanisms. (Becker, M., 2019) starts from the privacy debates, and through the aspects mentioned by the author helps us how to protect personal autonomy in the digital age, an essential aspect especially in the context of fintech financial instruments. As also presented by (Yuchong Li et all, 2021)), cyber security "tracks real-time information about the latest IT data". It is obvious that at the global level, especially in the context of AI, researchers at the international level propose tools, various methods, models to prevent and limit cyber-attacks, but above all to limit the damage generated by these attacks.

Cybersecurity and Data Privacy Concepts and Definitions

To understand the challenges and considerations surrounding cybersecurity and data privacy in the fintech world, it is important to define some key concepts.

Threat landscape: The Fintech sector is continuously experiencing a wide range of evolving and diverse threats that pose significant risks to the security and privacy of sensitive data. These include cyber-attacks, data breaches, compliance issues with regulations, and new technologies that introduce vulnerabilities.

Risk management: It includes the systematic identification, analysis, evaluation, and reduction of potential vulnerabilities and threats to guarantee a strong security infrastructure. Strict protocols for privacy management involve in-depth data protection within complex financial processes by methodically identifying risks, analyzing vulnerabilities, and evaluating threats to ensure effective security measures., and maintaining strict privacy protocols for sensitive data within fintech organizations.@(Uddin et al., 2020)

 doi:10.20944/preprints202401.2194.v1

Encryption: The process of converting sensitive data into unreadable code to prevent unauthorized access by using encryption techniques and algorithms. This helps in ensuring that only authorized individuals or systems with the proper decryption key can access and understand the information, thus safeguarding it from potential security breaches.

Authentication: The process of verifying the identity of users or devices to ensure only authorized access to sensitive information and systems, often through multifactor authentication and security protocols. This includes confirming identities through biometric data, passwords, tokens, smart cards, or other secure methods while considering potential threat scenarios such as phishing attacks and social engineering tactics. (Varshney et al., 2020)

Security breach: Unauthorized access refers to the act of gaining entry to sensitive data without proper authorization, while disclosure involves the release of this information to unauthorized individuals. Alteration pertains to any unauthorized changes made to the data, and destruction indicates the intentional or accidental elimination of sensitive data.

Compliance: Ensuring that fintech organizations strictly adhere to a comprehensive set of regulatory requirements and industry standards, meticulously designed to safeguard customer information and uphold the highest levels of data privacy. (Suryono et al., 2020)

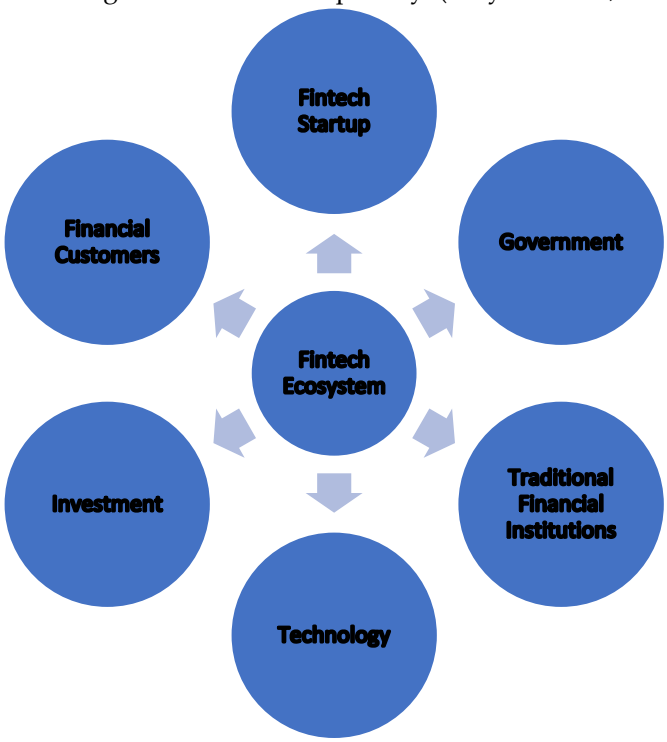

Figure 1. Ecosystem for Fintech. *Source: own processing*.

Common Cyber Security Threats for the Fintech

Phishing and social manipulation attacks are among the main reasons for security breaches due to human error. According to IBM's 2022 report on the Cost of a Data Breach, these attacks can also be very costly, with an average impact of USD 4.91 million for phishing and USD 4.10 million for social engineering. In such cases, attackers try to deceive users in order to obtain sensitive information like login credentials or banking details through email messages. Clicking on any compromised links or attachments in phishing emails can result in the installation of malicious software on the targeted computer system or lead users to a fraudulent webpage designed to collect login credentials. ((Oraca) & (Craciun), n.d)

Another significant risk faced by financial technology companies is the presence of malware and ransomware attacks. Malware pertains to harmful software designed to disturb or obtain unauthorized entry into computer systems. Such attacks can jeopardize user data, disrupt services, or facilitate unlawful access to financial systems. Typically, attackers utilize malware to infiltrate

 doi:10.20944/preprints202401.2194.v1

systems and gain unauthorized access to information before deploying ransomware that encrypts the company's data. To prevent public exposure or avoid complete deletion of the company's database in some instances, threat actors demand a payment in exchange for releasing it.

Due to the valuable customer and intellectual property information, it holds, ransomware groups find the financial services industry highly attractive. Furthermore, FinTech platforms are vulnerable to various types of malwares, including viruses, ransomware, and spyware. The risk of exposing this data on the dark web and the subsequent harm to reputation and business prospects often forces many financial services organizations to give into ransom demands even if official recommendations go against such practices.

Distributed Denial of Service (DDoS) Attacks is another threat which target the resources of a FinTech platform, rendering it inaccessible to legitimate users. By flooding the system with a massive volume of traffic or requests, attackers disrupt services, cause financial losses, and damage the reputation of the targeted platform. To address these cybersecurity risks, the financial technology industry must prioritize the implementation of robust cybersecurity frameworks and standards.

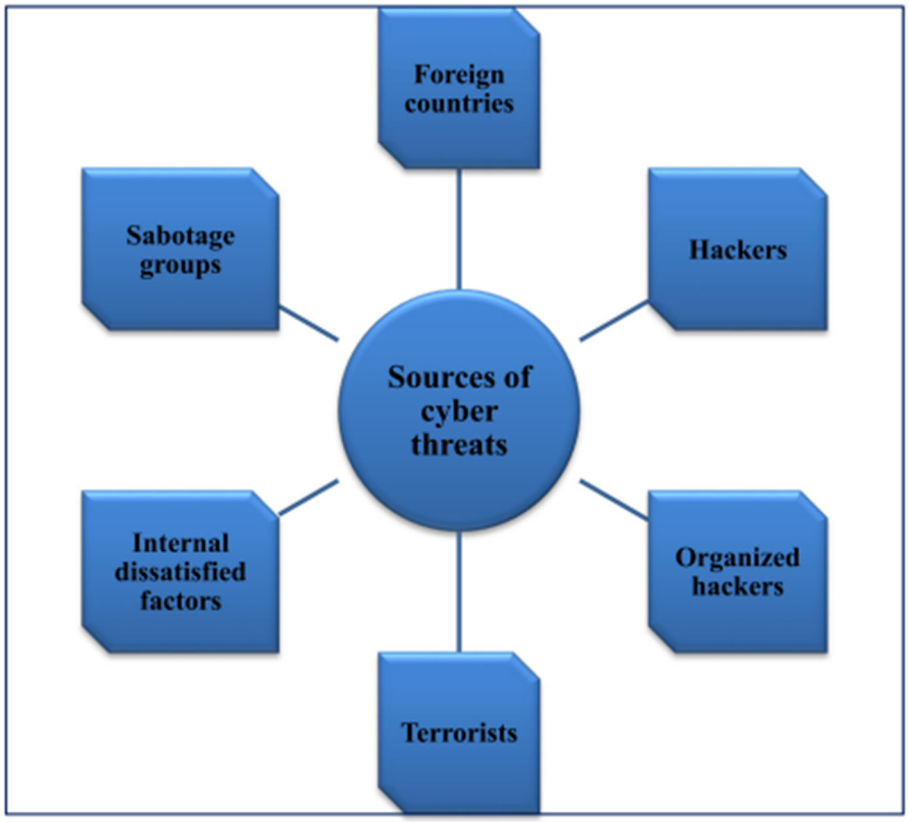

Figure 2. Sources of cyber threats. *Source: (Yuchong Li, et all, 2021)*

As can be seen in the figure above, the source of cyber-attacks is different, and very often being distributed randomly, it is very complicated to identify the person or persons who generated the respective cyber-attack.

Solutions

To address the challenges mentioned above, it is critical for fintech companies to implement appropriate cybersecurity measures (Creado & Ramteke, 2020). Companies need to develop a clearly defined cybersecurity plan that is in line with their business goals. This plan should include specific objectives, risk evaluations, strategies for handling incidents, and initiatives to raise employee awareness. It should also consider emerging risks and changing technologies to guarantee ongoing security measures.

Enterprises must give high priority to implementing robust access controls, as they play a crucial role in preventing unauthorized entry to sensitive data and systems. This involves the enforcement

 doi:10.20944/preprints202401.2194.v1

of strong authentication methods, like multifactor authentication, for verifying user identities, and the establishment of role-based access controls to ensure that employees have suitable access privileges according to their roles and duties.

Encryption serves as a crucial security measure for safeguarding data against unauthorized access. It is important for FinTech companies to apply encryption to protect data both during transmission and when stored on their systems. Utilizing secure encryption protocols like Transport Layer Security can help ensure the security of data in transit, while employing robust encryption algorithms is necessary for securing data at rest. ((Oraca) & (Craciun), n.d)

Regular security evaluations, like penetration testing and vulnerability scanning, are useful for uncovering potential weaknesses in systems. It is important that these assessments be carried out by experts to identify vulnerabilities, evaluate the efficacy of security measures, and promptly address any identified weaknesses.

A well-prepared and thoroughly practiced incident response plan is essential in minimizing harm and swiftly restoring services in the event of a cybersecurity incident. It is crucial for FinTech companies to create detailed response plans that define roles, escalation procedures, communication protocols, and recovery processes. Regular testing and simulation exercises are also necessary to verify the effectiveness of these plans.

It is essential to regularly apply security patches and updates to software, operating systems, and network infrastructure. This helps to address known vulnerabilities and protects against potential exploitation by cybercriminals.

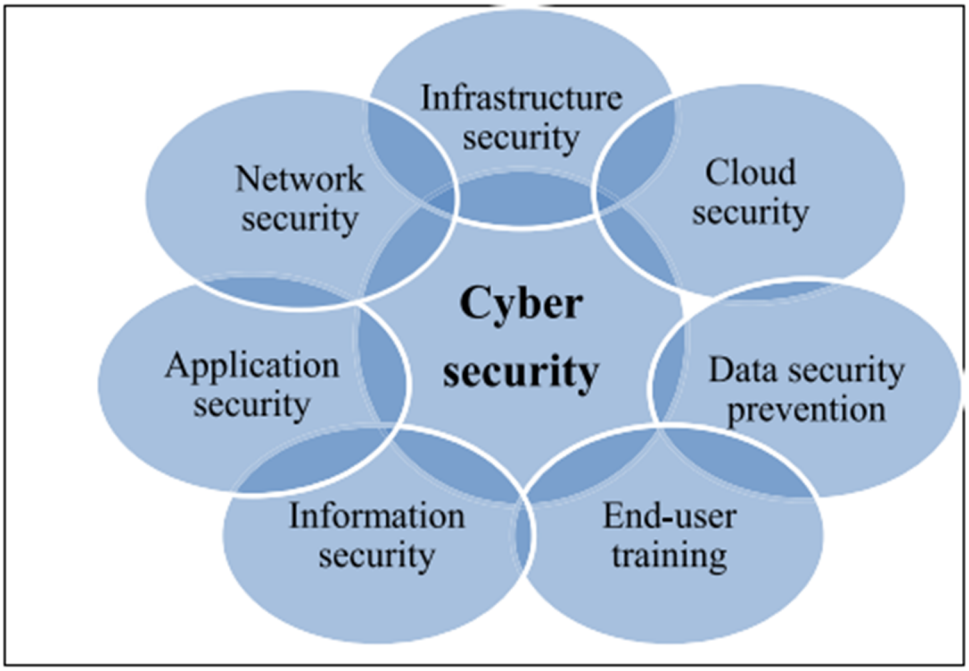

Figure 3. Security triangle (CIA). Source: (Yuchong Li, et all, 2021).

To ensure cyber security at the level of institutions involved in offering FinTech digital financial services, we appreciate that it is necessary that all those involved in the activity process and for a good protection and management of financial data flows, it is very important to know at the individual and institutional level what are the types of cyber. The figure above shows the different types of cyber security (Yuchong Li, et all, 2021).

Additionally, Fintech organizations should closely monitor and stay informed about the latest updates to data protection and privacy regulations, ensuring compliance with local and international laws such as the General Data Protection Regulation and the Payment Card Industry Data Security Standard.

Lastly, companies should develop a strong culture of security within their organizations. Fintech organizations should prioritize cybersecurity and data privacy from the top down, fostering a culture

 doi:10.20944/preprints202401.2194.v1

of security awareness and ensuring that all employees are trained on best practices for handling sensitive data and identifying potential threats.

2. Materials and Methods

To gather information on cybersecurity and data privacy in the fintech industry, a multi-step approach was followed ((Oraca) & (Craciun), n.d). This included conducting a thorough review of relevant literature, industry reports, and regulatory guidelines. The sources mentioned in the prompt were consulted to gain insights into the potential threats faced by fintech companies and the best practices for implementing cybersecurity measures. Results showed that cybersecurity risks were a major concern for financial regulators, with concerns ranging from operational risks to consumer protection. Fintech companies need to proactively address cybersecurity risks to protect sensitive financial data and maintain the trust of their customers. The findings revealed that cybersecurity and data privacy are crucial considerations for fintech companies

3. Results and Discussion

The results of the study highlighted may key points regarding cybersecurity and data privacy in the fintech industry. The study is a call to action for fintech companies to prioritize cybersecurity as a fundamental aspect of their business.

Fintech companies face a wide range of cyber threats, including phishing and social engineering attacks, malware and ransomware attacks, and network vulnerabilities. Phishing and social engineering attacks are often directed at unsuspecting employees who may inadvertently compromise sensitive information. Malware and ransomware attacks can cripple fintech operations, leading to financial losses and reputational damage. Additionally, network vulnerabilities pose a significant threat to the confidentiality and integrity of financial data. To mitigate these risks, it is essential for fintech companies to implement robust cybersecurity measures and adhere to data privacy regulations. The following data shows the data violation incidents in the US from 2015 to 2022.

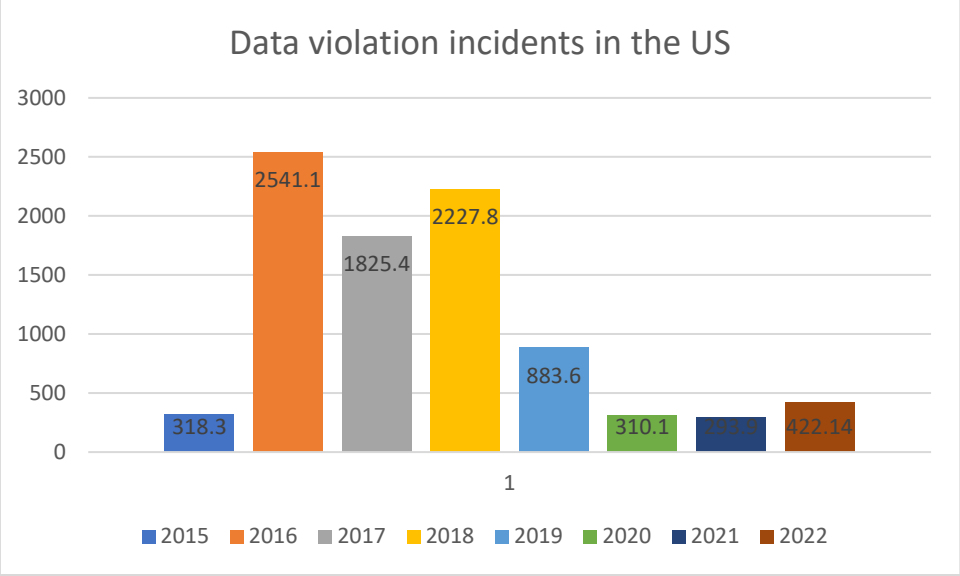

Figure 4. Data violation incidents in the US. *Source: own processing*.

One of the key best practices is to regularly conduct comprehensive security assessments and penetration testing to identify and address vulnerabilities in their systems. This proactive approach can help preempt potential cyber threats and safeguard sensitive financial information. Furthermore, fostering a culture of cybersecurity awareness and providing regular training to employees can significantly reduce the risk of falling victim to social engineering attacks. Strong authentication

 doi:10.20944/preprints202401.2194.v1

measures, encryption protocols, and secure access controls are imperative to protect financial data from unauthorized access. (Arner, D. W., et all, 2016).

Regulatory issues and lack of trust among customers further compound the challenges faced by fintech companies in ensuring cybersecurity and data privacy. Regulatory issues such as the General Data Protection Regulation and the Payment Card Industry Data Security Standard place additional compliance burdens on fintech companies. Non-compliance with these regulations can result in severe penalties and reputational damage. Moreover, the lack of trust among customers due to concerns about the security of their financial information underscores the urgency for fintech companies to invest in robust cybersecurity infrastructure and transparent data privacy practices.

Implementing best practices such as intrusion detection systems, threat intelligence feeds, and comprehensive cybersecurity programs can significantly enhance the cybersecurity posture of fintech companies. These measures not only protect sensitive financial data but also foster trust among customers, leading to increased adoption of fintech services. Intrusion detection systems and threat intelligence feeds can help detect and respond to potential cyber threats in real-time, minimizing the impact of attacks. Additionally, establishing strong partnerships with trusted cybersecurity providers can ensure continuous monitoring and prompt incident response, further strengthening the overall security of fintech systems. (IAPP, 2019)

Collaboration and information sharing within the industry are crucial for combating cyber threats and staying ahead of emerging risks. Creating platforms and networks for information sharing, such as cybersecurity forums and industry associations, can facilitate the exchange of best practices, threat intelligence, and cyber incident response strategies. (Gai et al., 2018) By pooling resources, knowledge, and expertise, fintech companies can collectively augment their cybersecurity capabilities and strengthen the overall resilience of the entire industry. In today's rapidly changing world, the significance of accurate weather forecasts cannot be overstated. Similarly, in the booming fintech world, the significance of cybersecurity and data privacy cannot be overstated. The following table shows the highest amount of victim losses in the United States in the year 2022. The data is considered in million US Dollars.

Table 1. Cybercrime and victim losses. Source: own processing.

Category	Loss in $ Million	
Investment	$	3,311.74
Business email Compromise	$	2,742.35
Tech Support	$	806.55
Personal Data breach	$	742.44
Confidence fraud	$	735.88
Real estate	$	396.93
Non-payment/ non-delivery	$	281.77
Credit card/ Check fraud	$	264.15
Government impersonation	$	240.55
Identity theft	$	189.21
Spoofing	$	107.93
Advanced fee	$	104.33

Industry-wide cybersecurity standards and regulations also need to be established to ensure consistent and robust cybersecurity practices among fintech companies. These standards should address key areas such as data encryption, access controls, authentication mechanisms, incident response protocols, and regular security audits. (Tyagi, 2022) Furthermore, the adoption of Explainable Artificial Intelligence techniques in credit card fraud detection can help address concerns surrounding the opacity of AI models. Additionally, fintech companies should prioritize cybersecurity as a fundamental aspect of their business. This includes allocating adequate resources, both in terms of budget and personnel, to develop and implement comprehensive cybersecurity programs.

 doi:10.20944/preprints202401.2194.v1

4. Challenges and Future Directions

To address the challenges mentioned above, it is critical for fintech companies to implement appropriate cybersecurity measures (Creado & Ramteke, 2020). Companies need to develop a clearly defined cybersecurity plan that is in line with their business goals. This plan should include specific objectives, risk evaluations, strategies for handling incidents, and initiatives to raise employee awareness. It should also consider emerging risks and changing technologies to guarantee ongoing security measures.

Enterprises must give high priority to implementing robust access controls, as they play a crucial role in preventing unauthorized entry to sensitive data and systems. This involves the enforcement of strong authentication methods, like multifactor authentication, for verifying user identities, and the establishment of role-based access controls to ensure that employees have suitable access privileges according to their roles and duties (RX Advanced Technologies LTD, 2024).

Encryption serves as a crucial security measure for safeguarding data against unauthorized access. It is important for FinTech companies to apply encryption to protect data both during transmission and when stored on their systems. Utilizing secure encryption protocols like Transport Layer Security can help ensure the security of data in transit, while employing robust encryption algorithms is necessary for securing data at rest (Oraca M.U., et al, 2023) and (Petrosyan A., 2023).

Regular security evaluations, like penetration testing and vulnerability scanning, are useful for uncovering potential weaknesses in systems. It is important that these assessments be carried out by experts to identify vulnerabilities, evaluate the efficacy of security measures, and promptly address any identified weaknesses.

A well-prepared and thoroughly practiced incident response plan is essential in minimizing harm and swiftly restoring services in the event of a cybersecurity incident. It is crucial for FinTech companies to create detailed response plans that define roles, escalation procedures, communication protocols, and recovery processes. Regular testing and simulation exercises are also necessary to verify the effectiveness of these plans.

It is essential to regularly apply security patches and updates to software, operating systems, and network infrastructure. This helps to address known vulnerabilities and protects against potential exploitation by cybercriminals.

Additionally, Fintech organizations should closely monitor and stay informed about the latest updates to data protection and privacy regulations, ensuring compliance with local and international laws such as the General Data Protection Regulation and the Payment Card Industry Data Security Standard.

Lastly, companies should develop a strong culture of security within their organizations. Fintech organizations should prioritize cybersecurity and data privacy from the top down, fostering a culture of security awareness and ensuring that all employees are trained on best practices for handling sensitive data and identifying potential threats.

5. Conclusions

As the fintech industry continues to grow and expand, ensuring cyber security and protecting data privacy will be crucial to maintaining customer trust. Fintech companies must prioritize the implementation of advanced cyber security measures, comprehensive data privacy policies, a strong security culture within their organization and stay abreast of regulatory changes. By following these best practices and cultivating a commitment to security throughout their operations, fintech organizations can build a solid foundation of trust with their customers while ensuring the security and privacy of their data. The booming fintech industry brings immense potential for innovation and growth, but it also comes with inherent cybersecurity risks. To fully unlock this potential and navigate the complexities of the digital landscape, fintech companies must prioritize cybersecurity and data privacy as fundamental aspects of their business operations and customer relationships.

Prioritizing cybersecurity and data privacy is critical to the success of fintech companies. Although the issue of cyber security is a priority for the fintech industry, data on incident statistics beyond 2020 is limited, which is why this is a limitation of our study.

However, we aim in our future research, through scientific databases, as well as through the authorities involved in the regulation and supervision of the fintech industry, to identify definite data on cyber-attacks and the financial impact on the fintech industry. It is critical for fintech companies to prioritize cybersecurity and data privacy to build customer trust and protect sensitive information.

Author Contributions: Conceptualization, R.K. and O.M..; methodology, R.K..; validation, R.K. and O.M..; formal analysis, R.K. and O.M..;.; investigation, R.K. and O.M..; resources, R.K. and O.M..; data curation, R.K. and O.M..; writing—original draft preparation, R.K..; writing—review and editing, R.K. and O.M..;.; visualization, R.K. and O.M..;.; supervision, R.K. and O.M..;.; project administration, R.K. and O.M..; funding acquisition, O.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used in the research article can be found in the URL https://www.statista.com/statistics/234987/victim-loss-cyber-crime-type/

Acknowledgments: many special thanks to the editorial team of the FinTech Journal and the valuable team of reviewers.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The Evolution of FinTech: A New Post-Crisis Paradigm? Georgetown Journal of International Law, 47(4), 1271-1320.
2. Apostu, S. A., Panait, M., Vasa, L., Mihaescu, C., & Dobrowolski, Z. (2022). NFTs and Cryptocurrencies—The Metamorphosis of the Economy under the Sign of Blockchain: A Time Series Approach. Mathematics, 10(17), 3218.
3. Becker, M., 2019, Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. Ethics Inf Technol 21, 307–317 (2019). https://doi.org/10.1007/s10676-019-09508-z
4. Brooks Charles J., Christopher Grow, Philip Craig, Donald Short, 2018, Cybersecurity Essentials, ISBN:9781119362395, John Wiley & Sons, Inc.
5. Creado, Y., & Ramteke, V. (2020, May 2). Active cyber defense strategies and techniques for banks and financial institutions. https://doi.org/10.1108/jfc-01-2020-0008
6. Cukier, K., & Zhu, H. (2018). Big Data, Big Risks: Toward Sustainable Cybersecurity in Financial Technology. Journal of Cybersecurity, 4(1), 1-17.
7. European Banking Authority. (2018). Guidelines on the Security Measures for Operational and Security Risks of Payment Services Under Directive (EU) 2015/2366 (PSD2). Retrieved from https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2263108/1f74ebf0-c7b2-4e89-ade0-16ebea24cc7d/EBA-GL-2018-07%20%28Guidelines%20on%20security%20measures%20for%20operational%20and%20security%20risks%20of%20payments%20services%20under%20PSD2%29.pdf
8. Financial Stability Oversight Council. (2020). Annual Report. Retrieved from https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1085
9. Gai, K., Qiu, M., & Sun, X. (2018, February 1). A survey on FinTech. Journal of Network and Computer Applications, 103, 262-273. https://doi.org/10.1016/j.jnca.2017.10.011
10. Gai, K., Qiu, M., & Sun, X. (2020). Blockchain Cybersecurity in Financial Technology Applications: A Case Study of Ant Financial. Journal of Information Security and Applications, 50, 102417.
11. International Association of Privacy Professionals (IAPP). (2019). The Growing Global Focus on Privacy: 2019 Privacy Governance Report. Retrieved from https://iapp.org/resources/article/the-growing-global-focus-on-privacy-2019-privacy-governance-report/
12. Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? IT Professional, 19(4), 68-72.
13. Manta, O., Folcut, O., & Militaru, L. (2023). ARTIFICIAL INTELLIGENCE, INTEGRITY, AND OPPORTUNITY IN INSURTECH. Journal of Information Systems & Operations Management, 17(1), 97-110.
14. Oraca, M U., & Craciun, L F. (n.d), 2023, The Rise of FinTech and the Need for Robust Cybersecurity Measures
15. Petrosyan A., 2023, Leading cyber-crime victim loss categories U.S. 2022, https://www.statista.com/statistics/234987/victim-loss-cyber-crime-type/
16. R K. (2023, October 11). Examining The Role of Fintech in Financial Inclusion and Its Impact on Financial Services to Underbanked Population in India. https://doi.org/10.36948/ijfmr.2023.v05i05.7473

17. RX Advanced Technologies LTD, 2024, ResilientX Security is the leading provider of cutting-edge cyber security solutions for Security testing, Posture Management, Security rating and Risk monitoring, https://resilientx.com/blog/ibm-cost-of-a-data-breach-report-2023-what-we-learn-from-it/
18. Smith, A. N., & Smith, B. L. (2018). FinTech: Addressing Cybersecurity Risks. Journal of Technology Research, 9, 1-16.
19. Suryono, R R., Budi, I., & Purwandari, B. (2020, December 21). Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review. Information, 11(12), 590-590. https://doi.org/10.3390/info11120590
20. Tong L, Yan W and Manta O (2022) Artificial Intelligence Influences Intelligent Automation in Tourism: A Mediating Role of Internet of Things and Environmental, Social, and Governance Investment. Front. Environ. Sci. 10:853302. doi: 10.3389/fenvs.2022.853302
21. Uddin, H., Ali, H., & Hassan, M K. (2020, August 18). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309. https://doi.org/10.1057/s41283-020-00063-2
22. Varshney, S., Munjal, D., Bhattacharya, O., Saboo, S., & Aggarwal, N. (2020, December 16). Big Data Privacy Breach Prevention Strategies. 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC). https://doi.org/10.1109/isssc50941.2020.9358878
23. World Economic Forum. (2019). Advancing Cyber Resilience: Principles and Tools for Boards. Retrieved from http://www3.weforum.org/docs/WEF_Advancing_Cyber_Resilience_Principles_and_Tools_for_Boards_2019.pdf
24. Yuchong Li, Qinghui Liu, 2021, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, Pages 8176-8186, ISSN 2352-4847. https://doi.org/10.1016/j.egyr.2021.08.126.