THE 18TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

The Rise of FinTech and the Need for Robust Cybersecurity Measures

Mirela-Alexandra Ungureanu (Oraca)[1], Luminita-MariaFilip (Craciun)[2]

Abstract: The increasing use of financial technology (FinTech) has transformed the financial sector and has provided consumers new and innovative products and services, whilst enhancing competition in the industry and accelerating the race to digitization. However, the rapid growth of FinTech is also exposing individuals and businesses alike to ever-increasing cyber security risks and challenges. Cyberattacks on financial and banking institutions, as well as targeting of vulnerabilities in financial apps and products by threat actors are becoming more frequent, sophisticated, and costly, with potentially devastating consequences for the integrity, stability, and trust in the financial system. The purpose of this work is to review the current state of business, the cyber security-related risks and challenges associated with this sector, the relevant regulations, and the best practices in the Fintech industry. The study's findings are reflected in the presentation of several strong and proactive cybersecurity measures aimed at reducing risks and guaranteeing the confidentiality and integrity of financial transactions.

Keywords: risks; technology; financial; vulnerabilities; confidentiality

JEL Classification: G28; O21; O30; O44

1. Introduction

According to a Market Data Forecast report, the global fintech market is expected to show a stable upward trajectory, reaching a market value of approximately $324 billion by 2026. This growth is projected to occur at a compound annual growth rate (CAGR) of around 25.18% over the forecast period 2022 - 2027.

The emergence of FinTech has revolutionized the financial landscape and brought numerous benefits to both financial service providers and consumers. Novel solutions have introduced greater convenience, accessibility, and cost-efficiency, enabling users to conduct financial transactions anytime and anywhere through digital platforms, mobile applications, and online interfaces. Moreover, FinTech has democratized financial services by expanding access to underserved populations and by promoting financial inclusion.

The adoption of FinTech can support financial development by advancing key policy objectives such as financial stability, integrity, inclusion, efficiency, innovation, and competition. Furthermore, it can establish the necessary groundwork for the digital economy to thrive. Fintech-driven business models

[1] Student, Danubius University of Galati, Romania, Faculty of Economic Sciences and Business Administration, Address: 3 Galati Blvd., 800654 Galati, Romania, alexandra@ungureanu.net.
[2] Senior Lecturer, PhD, Danubius University of Galati, Romania, Faculty of Economic Sciences and Business Administration Address: 3 Galati Blvd., 800654 Galati, Romania, mariacraciun@univ-danubius.ro.

and products have the capacity to bolster economies, making them more resilient and fostering a faster recovery from the impacts of the pandemic (Feyen, Natarajan, & Saal, 2023).

However, the unique nature of FinTech introduces specific cybersecurity challenges as platforms handle sensitive financial information, such as personal and financial data, payment details, and transaction records, making them attractive targets for cybercriminals. The interconnectedness of financial systems, the reliance on third-party vendors, and the use of emerging technologies like cloud computing and mobile applications further amplify the cybersecurity risks faced by companies in the industry.

This research paper aims to explore the rise of FinTech and shed light on the crucial need for robust cybersecurity measures in this rapidly evolving domain. Its primary objectives include:

- Examining the growing importance of cyber security for the FinTech sector, given the escalating risks and vulnerabilities.
- Assessing the potential impact of cyber security breaches on FinTech companies, their customers, and the overall financial ecosystem.
- Identifying the legal and regulatory frameworks that govern cyber security in FinTech and analysing their effectiveness in addressing emerging challenges.
- Analysing strategies and best practices for robust cyber security measures in FinTech, including technological solutions, risk management approaches, and collaboration among stakeholders.

In conclusion, this paper tries to shed light on the critical relationship between FinTech and cyber security in this digital age.

2. Background and Terminology

In order to lay the groundwork for the following chapters, this section outlines the key terms, namely FinTech and Cyber Security.

2.1. FinTech (Financial Technology)

Financial technology, commonly known as FinTech, refers to financial services or products that are offered using technology. It encompasses a wide range of digital solutions that aim to improve and streamline various financial activities, including payments, banking, lending, investment, and insurance (Gomber, Koch, & Siering, 2018). FinTech has gained significant traction in recent years, disrupting traditional financial systems and transforming the way individuals and businesses access and manage their finances.

Companies within the FinTech industry offer automated solutions for various financial tasks such as insurance, investments, trading, risk management, banking services, and more by using specialized software and algorithms to assist individuals, businesses, and organizations in effectively managing their finances through computer or smartphone applications. Additionally, fintech platforms provide valuable insights into financial matters.

One could argue that the current surge in fintech is primarily fuelled by two essential factors: i) the widespread availability of mobile devices, internet connectivity, and communication networks, which has created a state of constant connectivity, allowing continuous access to financial services, and ii) the decreasing costs of computing power and data storage, that have made advanced technologies, such as

cloud computing, more affordable and accessible. These two factors combined enable the development of innovative business models for delivering financial technology solutions (Feyen, Natarajan, & Saal, 2023).

2.2. Cyber Security

The term "cyber security" refers to a set of measures, processes, and technologies designed to protect digital systems, networks, and data from unauthorized access, manipulation, disruption, and destruction (NIST, 2023). This is to be achieved by implementing various security controls, such as access controls, encryption, firewalls, intrusion detection systems, and incident response mechanisms (to name a few), to safeguard against cyber threats.

Given the increasing reliance on digital systems and the Internet, cyber security has become a critical concern for individuals, organizations, and governments around the globe. Cyber threats can take various forms, including hacking, malware, phishing, ransomware, data breaches, and distributed denial-of-service (DDoS) attacks, and can lead to financial losses, reputational damage, privacy breaches, and even compromise national security.

According to a recent report by Cybersecurity Ventures (Morgan, 2022), the projected global annual cost of cybercrime is expected to exceed $8 trillion in 2023. However, it is important to note that this staggering amount may be an underestimate, indicating the potentially even larger impact of cybercrime.

IBM's report on the Cost of a data breach for 2022 reveals that the average cost of a data breach reached a record high, standing at USD 4.35 million. This amount reflects a 2.6% rise compared to the previous year, where the average cost of a breach amounted to USD 4.24 million. Financial organizations incurred the second highest costs, after the healthcare sector — averaging USD 5.97 million (IBM Security, 2022).

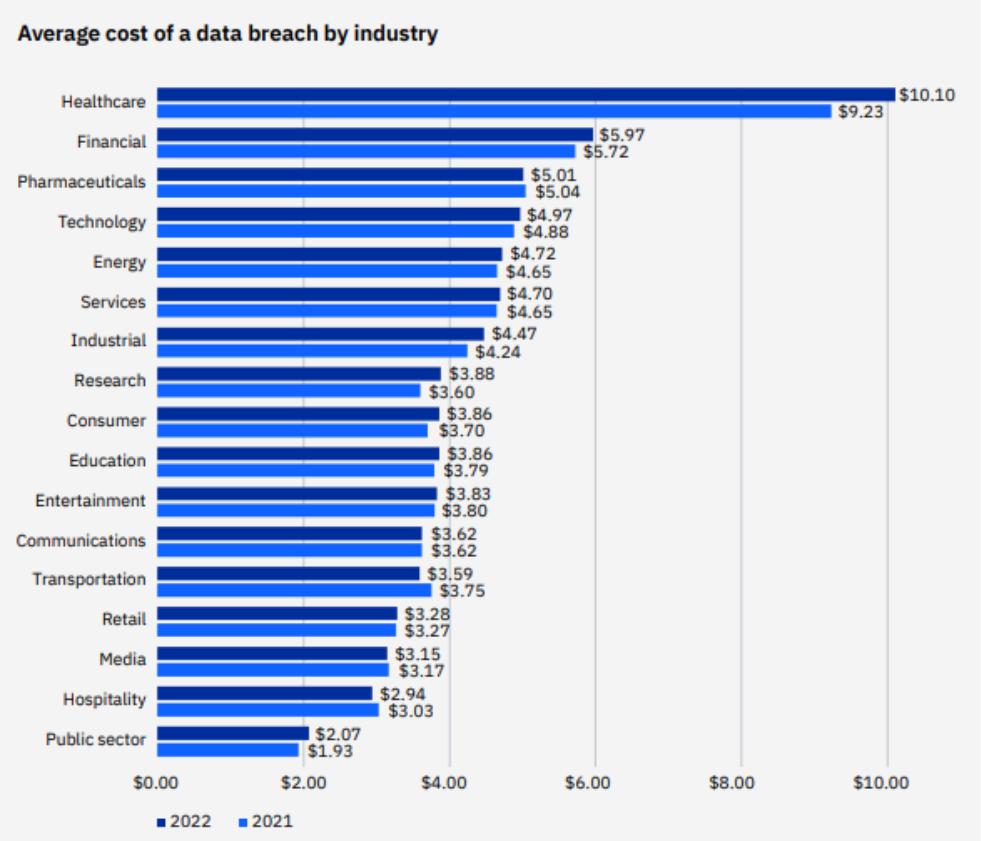

Figure 1. Average cost of a data breach, IBM Security, 2022

In fact, the need to safeguard digitally reliant businesses, Internet of Things (IoT) devices, and individuals from cyber threats has become crucial and this trend is expected to drive global expenditures on cybersecurity products and services to new hights - a cumulative total of $1.75 trillion over the five-year span from 2021 to 2025.

3. Cybersecurity in FinTech

Within the realm of financial technology, cyber security plays a critical role in safeguarding the integrity, confidentiality, and availability of data and systems. It encompasses the practices, technologies, and measures designed to protect FinTech platforms, networks, and applications from unauthorized access, data breaches, cyber threats, and other malicious activities.

In this context, the focus is on addressing the specific risks and challenges associated with the digital transformation of financial services as well as the protection of sensitive financial information, transactional data, personal data, and intellectual property, while ensuring the secure functioning of financial systems and infrastructure.

Cybersecurity in FinTech goes beyond protecting the interests of individual companies. It plays a vital role in safeguarding the financial system as a whole. A cybersecurity breach on a FinTech platform can have far-reaching consequences, including financial losses, reputational damage, erosion of consumer trust, and potential systemic risks. Therefore, ensuring robust cybersecurity measures is not only a business imperative but also a critical component of maintaining the stability, resilience, and trustworthiness of the FinTech industry (Traynor, 2018).

For the FinTech industry, effective cyber security involves a multi-layered approach and encompasses various aspects, including network security, data protection, access controls, encryption, authentication mechanisms, and robust incident response plans. Additionally, compliance with legal and regulatory requirements, such as data protection laws and industry standards, is crucial to ensure the confidentiality, integrity, and availability of financial data within the FinTech ecosystem (Mani, 2019).

4. Common Cyber Threats for the FinTech Industry

As the financial technology (FinTech) sector continues to expand, it becomes more and more attractive to malicious actors and faces a wide range of cyber security threats and risks. Understanding these threats is essential for implementing the most effective measures.

Phishing and social engineering attacks are some of the most common causes of a breach due to the human factor and according to IBM's report on the Cost of a data breach for 2022, also extremely costly, whit an average impact of USD 4.91 million for phishing and USD 4.10 million for social engineering (IBM Security, 2022). In this case, attackers attempt trick users to obtain confidential information, such as credentials or banking data, usually through email messages. Engaging with any of the compromised links or attachments in phishing emails can trigger the installation of malicious software on the targeted computer system or redirect to a fake webpage designed to gather login credentials.

Another important threat faced by FinTech companies is represented by malware and ransomware attacks. Malware refers to malicious software designed to disrupt or gain unauthorized access to computer systems. Malware attacks can compromise user data, disrupt services, or enable unauthorized access to financial systems. However, in most cases, attackers use malware to infect systems and gain unauthorized access to data, then deploy ransomware that encrypts the company's data. To release it without making it public or in some cases not to entirely wipe the company's database, the threat actors demand a ransom.

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 malware, 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 in to ransom demands even if official recommendations go against such practices.

For 2022, the average cost of a ransomware attack (not including the ransom itself), amounted to USD 4.54 million, whilst the average cost of a destructive or wiper attack was USD 5.12 million.

Infrastructure attacks focus on critical systems like power grids, water supply networks, transportation infrastructure, and financial services aiming to disrupt essential services and inflict extensive damage on a large scale.

Distributed Denial of Service (DDoS) Attacks aim to overwhelm 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.

Critical infrastructure remains highly vulnerable due to heavy reliance on state and local agencies, as well as third- and fourth-party vendors, who may lack sufficient cyber security controls. This is especially true in sectors such as finance, utilities, and government services, where outdated and

unpatched code, as well as legacy systems, are commonly employed (Brumfield, 2023). The average cost of a data breach for critical infrastructure was USD 4.82 million in 2022.

Nowadays, attackers have a broader attack surface due to increased interconnectivity and fragmentation of services, which introduce additional points of entry in every product chain and user interface (Feyen, Natarajan, & Saal, 2023). The initial target might be FinTech companies' IT infrastructure, including servers, networks, and databases, to gain access to sensitive information or disrupt operations or third parties that provide digital services, such as cloud computing.

Since FinTech companies develop and use complex applications and platforms that may have security vulnerabilities, attackers might find and exploit these to gain unauthorized access to data or perform fraudulent transactions. The risk arises from the increasingly condensed timeframes for exploiting vulnerabilities post-disclosure. This exploitation can initiate in less than 24 hours and swiftly escalate to its peak level.

According to Akamai research (Winterfeld, 2023), the financial services industry has seen the highest growth in web application and API attacks. the number of web application and API attacks detected over the past year has experienced a significant surge, increasing by 3.5 times compared to the previous year. This surge represents the highest growth rate among all industry verticals.

5. Impact of Security Breaches in the FinTech Industry

In the rapidly evolving realm of financial technology (FinTech), cybersecurity is a crucial factor in upholding trust and confidence among users, customers, and stakeholders. Security breaches in the FinTech industry can have serious consequences for all parties involved. These consequences can include but are not limited to financial losses, loss of user trust, reputational damage, disruption of operations and services, impact on regulation and compliance (Feyen, Natarajan & Saal, 2023).

As presented in the previous chapters, cyber-attacks can lead to significant financial losses for companies and users through fund theft or financial fraud. For companies, this can translate into compromised assets, loss of revenue, legal liabilities, and increased operational costs. Users may suffer financial losses through stolen funds or fraudulent transactions, potentially impacting their personal finances and trust in the FinTech ecosystem.

Security breaches shake the confidence of users both in FinTech companies and the overall financial system. Users may feel betrayed and concerned about the safety of their personal and financial information. This loss of trust can lead to a decline in user adoption and engagement with FinTech services, determining users to be hesitant to share sensitive data, conduct transactions, or even discontinue their usage altogether (Elliott & Jenkinson, 2020). Rebuilding user trust requires transparent communication, robust security measures, and proactive efforts to address vulnerabilities.

Furthermore, a significant security breach tarnishes the reputation of a FinTech company, causing long-term consequences. News of the breach, negative publicity, and the perception of inadequate security measures can damage the company's brand image. This can lead to a loss of credibility among customers, partners, and investors. Reputational damage can hamper business growth, hinder partnerships, and impede the company's ability to attract new customers and secure investments.

Another thing to keep in mind is that FinTech companies operate within a highly regulated environment, necessitating adherence to stringent data protection and cybersecurity standards. Since a security breach exposes the company to potential legal and financial ramifications, regulatory bodies may impose fines,

penalties, or sanctions for failing to protect financial and personal data adequately. Non-compliance with regulations can result in legal disputes, damage the company's reputation, and impede future growth. Companies must prioritize cybersecurity to ensure compliance, mitigate risks, and avoid severe consequences (Marlow, 2023).

Cyber-attacks can disrupt the normal operations and services of FinTech companies, leading to service outages, system failures, or compromised functionality. These disruptions adversely impact users who rely on FinTech services for financial transactions, investments, or other critical operations. Service unavailability or delays can damage customer relationships, create dissatisfaction, and potentially drive users to seek alternative providers. The financial implications include loss of revenue, operational inefficiencies, and increased recovery costs to restore services and regain user trust (Adrian & Ferreira, 2023).

6. Cyber security Frameworks and Standards Applicable in FinTech

In recognition of the critical role cyber security plays, various legal and regulatory frameworks have been established to ensure the protection of sensitive financial data, promote secure practices, and mitigate cyber risks.

Compliance with cyber security regulations and industry standards is crucial for companies operating in the FinTech industry especially since failure to meet regulatory requirements might expose FinTech platforms to significant risks and can result in legal consequences, financial penalties, and reputational damage.

Some of the widely recognized cybersecurity frameworks and standards applicable to the FinTech industry will briefly be described in this chapter.

The GDPR, implemented in the European Union (EU), sets rigorous standards for the protection of EU citizens personal data even if the organization is outside the EU. This means that FinTech companies that handle the personal information of EU residents are required to comply with the GDPR's provisions and implement appropriate security measures, obtain consent for data processing, and notify individuals in case of data breaches (European Parliament and the Council of the European Union, 2016).

Another widely adopted framework for managing and reducing cybersecurity risks is the one developed by the National Institute of Standards and Technology. It provides a set of guidelines, standards, and best practices that help organizations identify, protect, detect, respond to, and recover from cyber threats. FinTech companies can use the NIST Framework as a foundation to develop their cybersecurity programs (National Institute of Standards and Technology, 2018).

The International Organization for Standardization (ISO) has developed the ISO 27001 and ISO 27002 standards, which focus on information security management systems (ISMS) and provide comprehensive guidance for implementing and maintaining effective cybersecurity controls. ISO 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS, while ISO 27002 provides a code of practice for information security controls. Compliance with these standards demonstrates a commitment to maintaining a high level of information security in FinTech operations.

Another comprehensive framework, specifically designed for organizations that handle payment card data, is the Payment Card Industry Data Security Standard (PCI DSS). Even though its main focus is on protecting cardholder data, PCI DSS also encompasses broader security controls and practices. To

ensure secure handling of sensitive financial information companies that process, store, or transmit payment card data must comply with the PCI DSS requirements (PCI Security Standards Council, 2022).

The Center for Internet Security (CIS) Controls has also listed a prioritized set of cybersecurity actions that organizations can take to enhance their security posture. These controls, derived from real-world threats, are continuously updated to address emerging risks and can help FinTech companies establish a strong baseline for their cybersecurity practices.

A framework that provides governance and management practices for IT processes and offers a holistic approach to aligning IT with business objectives, including cybersecurity is Control Objectives for Information and Related Technologies (COBIT), created by ISACA (Information Systems Audit and Control Association). It can be leveraged to establish effective controls, risk management processes, and governance structures to address cybersecurity risks (Simplilearn, 2023).

The Cloud Security Alliance (CSA) CCM is a framework that provides a set of security controls and best practices for secure cloud computing. As many FinTech companies rely on cloud-based services, adherence to the CCM can help ensure the security of cloud environments, data protection, and compliance with relevant regulations.

The Open Web Application Security Project (OWASP) is an open community dedicated to improving the security of software applications. The OWASP Top Ten Project highlights the ten most critical security risks facing web applications. FinTech companies that develop and use web-based applications can refer to OWASP resources to mitigate these risks and ensure secure application development.

It's important to note that the list above is not exhaustive, and there are other cybersecurity frameworks and standards applicable to the FinTech industry. However, all the listed frameworks and standards offer valuable guidance and industry-accepted practices for establishing effective cybersecurity controls in the FinTech sector. FinTech companies should assess their specific needs, regulatory requirements, and risk profiles to determine which frameworks are most relevant to their operations. Implementing these frameworks can assist in building a robust cybersecurity foundation and demonstrating a commitment to safeguarding customer data and financial transactions.

By adopting well established frameworks and standards, FinTech organizations can align their cybersecurity efforts with industry best practices, enhance their security posture, and demonstrate their commitment to safeguarding sensitive financial data and systems. Some of the benefits include enhanced risk management, improved compliance, increased customer trust and streamlined security operations.

7. Strategies for robust Cybersecurity in FinTech

Given the rapidly evolving nature of financial technology (FinTech), the significance of robust cybersecurity measures cannot be emphasized enough. To mitigate the ever-increasing risks in this industry, it is vital for companies to enhance their security measures in order to safeguard customer data and cultivate trust among users. This section presents essential cybersecurity best practices for FinTech.

First and foremost, companies should establish a well-defined cybersecurity strategy that aligns with their business objectives. This strategy should encompass clear goals, risk assessments, incident response plans, and employee awareness programs. It should also take into account emerging threats and evolving technologies to ensure continuous protection.

Additionally, enterprises should prioritize the implementation of strong access controls as they are critical in preventing unauthorized access to sensitive data and systems. This implies enforcing strong

authentication mechanisms, such as multifactor authentication, to verify user identities and implementing role-based access controls to ensure that employees have only the appropriate access privileges based on their roles and responsibilities.

Encryption is a fundamental security measure that protects data from unauthorized access and FinTech companies should encrypt data both during transmission and while stored on their systems. Secure encryption protocols, such as Transport Layer Security (TLS), should be utilized to secure data in transit, while strong encryption algorithms should be employed for data at rest.

Additionally, regular security assessments, such as penetration testing and vulnerability scanning, help identify potential weaknesses in systems. However, these assessments should be performed by qualified professionals to identify vulnerabilities, assess the effectiveness of security controls, and address any weaknesses promptly.

One of the most important protection measures in the event of a cybersecurity incident is a well-prepared and practiced incident response plan and it is crucial for minimizing damage and restoring services promptly. FinTech companies should develop detailed response plans that outline the roles and responsibilities, escalation procedures, communication protocols, and recovery processes but also conduct regular testing and simulation exercises to help ensure the effectiveness of these plans.

Applying security patches and updates to their software, operating systems, and network infrastructure is also crucial as regular systems and applications updates help address known/discovered vulnerabilities and protects against exploits that cybercriminals may target.

It is a known fact that human error is the most common cause of data breaches (Verizon, 2022) and one of the ways to mitigate this risk is through cyber security awareness training. Companies should provide regular cybersecurity awareness training to their employees, educating them on the latest threats, social engineering techniques, and safe practices, emphasizing the importance of strong passwords, showcasing techniques to identify phishing attempts, and encouraging them to report any suspicious activities. Cybersecurity should be ingrained in the culture of FinTech companies by promoting a security-first mindset among employees and regularly communicating updates and best practices to the entire organization. By fostering this kind of culture of security, companies will be able to create a collective responsibility that help maintain robust cybersecurity measures.

Another thing to keep in mind is that FinTech companies often rely on third-party vendors for various services, which makes it crucial to ensure that these vendors maintain robust cybersecurity practices. Conducting due diligence when selecting partners, including strict cybersecurity requirements in vendor contracts, and regularly assessing their security measures can greatly help minimize potential risks.

Lastly, continuous monitoring of FinTech systems and networks allows for the timely detection and response to cybersecurity threats. Thus, implementing security information and event management (SIEM) solutions, intrusion detection systems, and threat intelligence feeds will help companies identify and mitigate potential attacks in real-time.

Implementing these best practices can significantly enhance the cybersecurity posture of FinTech companies, protecting sensitive financial data, and fostering trust among customers (Brumfield, 2023).

The call to action for FinTech companies is clear: prioritize cybersecurity as a fundamental aspect of the business. This requires allocating adequate resources, both in terms of budget and personnel, to develop and implement comprehensive cybersecurity programs. It involves establishing a strong cybersecurity culture within the organization, fostering awareness among employees, and promoting a security-first mindset.

Additionally, collaboration and information sharing within the industry are crucial. Companies should actively engage in partnerships and information-sharing initiatives to collectively combat cyber threats and stay ahead of emerging risks. By pooling resources, knowledge, and expertise, FinTech companies can collectively augment their cybersecurity capabilities and strengthen the overall resilience of the entire industry.

Furthermore, continuous monitoring, threat intelligence analysis, and regular security assessments are essential to identify vulnerabilities and address them promptly. Companies should embrace emerging technologies and trends in cybersecurity, such as artificial intelligence, blockchain, and secure authentication mechanisms, to stay one step ahead of sophisticated cyber adversaries.

By heeding this call to action and prioritizing cybersecurity, FinTech companies can safeguard their own operations, protect their customers' sensitive information, and maintain the trust and confidence that underpin the success of the FinTech industry. The potential benefits of FinTech can be fully realized when cybersecurity becomes an integral part of the innovation and growth journey.

In conclusion, the rise of the FinTech industry brings immense potential, but it also comes with inherent cybersecurity risks. The future success of the sector relies on a proactive and holistic approach to cybersecurity. By taking decisive action now, companies can strengthen their defenses, mitigate risks, and contribute to a secure and resilient digital financial ecosystem.

References

Adrian, T. & Ferreira, C. (2023, March 2). *Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards*. Retrieved May 15. from imf.org: https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards.

Brumfield, C. (February 21, 2023). *Cyber arms race, economic headwinds among top macro cybersecurity risks for 2023*. Retrieved May 15. From csoonline.com: https://www.csoonline.com/article/3688729/cyber-arms-race-economic-headwinds-among-top-macro-cybersecurity-risks-for2023.html?utm_date=20230302212830&utm_campaign=CSO%20US%20Update&utm_content=Title%3A%20Cyber%20arms%20race%2C%20economic%20headwinds%20am.

Elliott, J. & Jenkinson, N. (2020, December 7). *Cyber Risk is the New Threat to Financial Stability*. Retrieved May 15. from imf.org: https://www.imf.org/en/Blogs/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability

European Parliament and the Council of the European Union. (2016, April 27). *GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Gene.* Retrieved May 15, 2023, from eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Feyen, E.; Natarajan, H. & Saal, M. (2023). *Fintech and the future of Science: market and policy implications.* Washington: World Bank Publications.

(2022). *Global Fintech Market Research Report - Segmentation By Technology (API; AI; Blockchain; Distributed Computing), Service (Payment; Fund Transfer; Personal Finance; Loans; Insurance; Wealth Management), Application (Banking; Insurance; Securities; & Others.* Market Data Forecast. Retrieved May 15, 2023, from https://www.marketdataforecast.com/market-reports/fintech-market

Gomber, P.; Koch, J.-A. & Siering, M. (2018). Digital Finance and FinTech: Current Research and Future Research Directions. *Journal of Business Economics*, 537-580.

IBM Security. (2022). *Cost of a Data Breach Report 2022.* Armonk: IBM Corporation. Retrieved May 15, 2023, from https://www.ibm.com/downloads/cas/3R8N1DZJ

Mani, V. (2019, February 8). Cybersecurity and Fintech at a Crossroads. *ISACA Journal, 1*. Retrieved May 15, 2023, from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/cybersecurity-and-fintech-at-a-crossroads

Marlow, D. (2023, January 2). *An overview of Cybersecurity Issues faced by the Fintech Industry*. Retrieved May 15, 2023, from securityboulevard.com: https://securityboulevard.com/2023/01/an-overview-of-cybersecurity-issues-faced-by-the-fintech-industry/

Morgan, S. (2022, December 10). *Top 10 Cybersecurity Predictions And Statistics For 2023.* Northport, New York. Retrieved May 15, 2023, from https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

National Institute of Standards and Technology. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2023). *NIST Glossary of Key Information Security Terms.* Retrieved May 15, 2023, from csrc.nist.gov: https://csrc.nist.gov/glossary/term/cybersecurity

PCI Security Standards Council, . (2022, March). *Payment Card Industry Data Security Standard. Requirements and Testing Procedures*. Version 4.0.

Simplilearn. (2023, February 21). *What is COBIT? Understanding the COBIT Framework [Updated]*. Retrieved from simplilearn.com: https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article

The CSA Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing. (n.d.). Retrieved May 15, 2023, from cloudsecurityalliance.org: https://cloudsecurityalliance.org/research/cloud-controls-matrix/.

Traynor, P. (September, 2018). *Digital Finance and Data Security. How Private and Secure Is Data Used in Digital Finance?* Center for Financial Inclusion. Retrieved May 15, 2023, from https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2018/09/CFI43-CFI_Online_Security-Final-2018.09.12.pdf.

Verizon (2022). *2022 DBIR: Financial and Insurance (NAICS 52).* Retrieved from verizon.com: https://www.verizon.com/business/resources/reports/dbir/

Winterfeld, S. (2023, February 1). *7 Key Takeaways for Financial Services from Recent Research*. Retrieved May 15, 2023, from akamai.com: https://www.akamai.com/blog/security/7-key-takeaways-for-financial-services-from-recent-research