Acta Universitatis Danubius
ŒCONOMICA

Key Pillars for FinTech and Cybersecurity

Mircea Constantin Șcheau[1], Călin Mihail Rangu[2], Florin Vasile Popescu[3], Daniel Mihai Leu[4]

Abstract: The technological advancements of the last couple of years combined with the unique situation created by the Covid-19 pandemic made the customer more open to the digitalization of several financial services and procedures in order to further reduce the need for face-to-face interaction. The financial technology companies found themselves in the position to leverage advancements in fields such as data analytics and artificial intelligence as well as the new financial paradigm brought by blockchain technology thus making technological innovation a top priority to meet these new customer needs. As the tendency of the financial sector as a whole to further embrace digitalization becomes more apparent, so does the protection of customer data become more complex as cyber-attack vectors increase in complexity aided by an ever-expanding attack surface. We argue that the rapid pace in which technological advancements are adopted in the financial services sector must be accompanied by responsible cyber security policies and regulations enforced from both the technological and human standpoints. We will provide an overview on the pace in which cybercrime in the financial sector grew in intensity as FinTech moved towards an end-to-end approach, the most common cyber threats which affect the financial sector as well as why cyber threat management should not be limited to a reactionary approach.

Keywords: distributed technology; financial and technology mixture; security; resilience

JEL Classification: G28; O21; O30; O44

[1] PhD, Constanta Maritime University & University of Craiova, Romania, Address: Constanta Maritime University Str. Alexandru Ioan Cuza 13, Craiova 200585 and University of Craiova, Str. Alexandru Ioan Cuza 13, Craiova 200585, Romania, E-mail: mircea.scheau@cmu-edu.eu, mircea.scheau@edu.ucv.ro.
[2] Associate Professor, PhD, Danubius University of Galati, Romania, Address: 3 Galati Blvd., 800654 Galati, Romania, Corresponding author: calinrangu@univ-danubius.ro; calin@rangu.ro.
[3] Associate Professor, PhD, Carol I National Defence University, Romania, Address: 68-72 Panduri Road, Bucharest 050662, E-mail: popescu.vflorin@unap.ro.
[4] Threat Researcher, Farscope Information Consulting, Romania, E-mail: daniel.leu2810@gmail.com.

1. Introduction

FinTech represents a financial and technological mix. It refers to the use of technology or the automation of financial services and processes. The English name is "Financial Technology" and refers to a vast and fast-growing industry that serves both consumers and businesses. From banking, insurance, and the internet to investment applications, to virtual currencies like Bitcoin… Fintech is applicable. Fintech companies integrate AI, blockchain, and financial science technologies in the financial sector to make them more secure, faster and more efficient. Fintech is one of the fastest growing technology fields, with innovative companies in almost all areas of finance, from payments and loans to scores or Forex credit transactions, stocks and so on.

As technological advancements brought forward by FinTech are rapidly changing the financial services landscape, the attack surfaces impacting this sector increases making room for cyber threat actors to fill in the gaps created by inadequate security measures and policies or lack, or not-updated regulations. The British-Dutch multinational consulting company KPMG International Limited released a report in August 2021, dubbed "Pulse of Fintech H1'21" which emphasized the strong position held by the global fintech market in the first half of 2021 (Pollari & Ruddenklau, 2021). The report characterized the market as diverse with deals being made across several FinTech subsectors such as regulatory technology, wealth management, blockchain and cybersecurity, recognizing the acceleration of the consumers digital behaviors brought by the Covid-19 global pandemic. It is worth mentioning that increased interest in the blockchain technology sector was observed among startups, and investors as well as government agencies and regulators. The same report states that in the first half of 2021, 2,456 deals were recorded in the global FinTech market with US $98 billion worth of investments.

Even though this registered momentum appears to hold despite the still uncertain nature of the global pandemic situation, there are several other factors which could affect the industry if left unchecked.

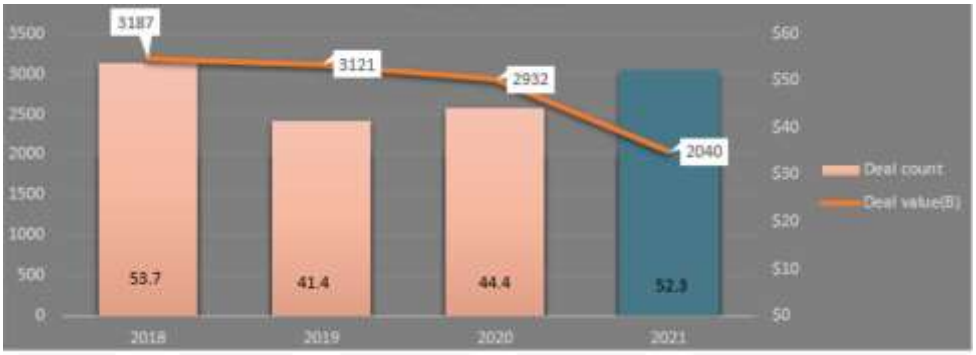

Figure 1. Global Venture Activity in Fintech (Pollari & Ruddenklau, 2021)

The classic methods through which financial institutions manage the risks generated by Fintech and those of cybercrime are mainly related to the field of risk management, especially operational ones. The new risk theory of the entire financial system, beyond operational risks, is designed on the risk-based approach model. The financial system, especially in the Fintech era, needs a re-establishment of regulations, because new technology companies, new start-ups can initially benefit from the flexibility of the principle-based approach even though this can create scalability limitations later. The previous rules-based approach may be more attractive to investors. For this reason, a rethinking of the balance between the two approaches, risk-based and rules-based can bring a new paradigm shift, especially since from the perspective of information systems security, a rules-based approach is the appropriate one to ensure effective control. The regulatory imbalance can create shadow banking companies that bring systemic risks through the digital transformation of business processes. An example is innovation in Peer-to-Peer (P2P) technology in which technical platforms act as agents between credit companies and borrowers, but without taking real responsibility. In turn, they generate significant risks, not being responsible for losses that may occur, including those that happen because of cybercrime incidents. "FinTech 3.0 thus needs a framework that is both balanced and dynamic, simultaneously benefiting private stakeholders (e.g. institutional or start-ups) and regulators.", According to Arner, Douglas W. & all (2015).

2. Research Method

According to Estelle M. Phillips and Derek S. Pugh (1994), there are various ways to be original in scientific research:

- to carry out empirical research (field, concrete) on topics that have not been addressed before to give a new interpretation to old ideas.
- bring new evidence for issues already known.

- to elaborate new syntheses.
- use the knowledge gained in studying socio-cultural realities in other countries.
- to experiment with research methods and techniques in different sociocultural contexts; to carry out interdisciplinary research.
- to look at sociocultural realities from a different theoretical perspective.
- present the professional knowledge gained in a way that has never been tried before.

In this study, the authors were able to give a new interpretation to some old ideas and to present the professional knowledge acquired in a way that has never been tried before. Thus, the relationship of *The New Paradigm of FinTech and CyberSecurity* was brought to light.

3. Analysis of FinTech Evolution

A protected and secure cyberspace is at the heart of the EU's digital single market, according to European Parliament studies (2021a). According to the European Commission's report (2019), the proper integration of new FinTech technologies through the introduction of innovative solutions and through unlocking its huge potential will give people confidence online. According to the same report, the 2019 Digital Economy and Society Index found that security concerns have limited, or prevented, 50% of EU internet users from doing business online. The 2020 Index (European Commission, 2021b) found that 39% of EU citizens who used the internet faced security issues.

The European Parliament's (2021b) study states that the number of Internet-connected (IoT) devices will reach 22.3 billion in 2024. A rapid increase in the use of digital solutions can be observed. Remote work, online shopping, social networking, and professional online applications saw a significant uptick during lockdown periods. These solutions can benefit the consumers and support the economy as well as the post-Covid recovery process (European Parliament, 2022). At the same time, we can also observe a significant increase in malicious cyber activities (European Commission, 2020). By 2030, 125 billion devices could be connected to the Internet, while 90% of individuals over the age of six will be online. "As cyberspace is interconnected by design, and digital and physical are increasingly intertwined, new dangers are emerging. (Lattice, 2019)".

Two main pillars can be identified - resilience and prevention (Scheffer & all, 2018). Considering that in her 2021 State of the Union address, European Commission President Ursula von der Leyen (2021) emphasized the need for an EU cyber defense policy (AM 1), MEPs insist that "it is essential to overcome fragmentation and the

current complexity of the EU's global cyber architecture and to develop a common vision for achieving online security and stability. " FinTech solutions, as the new digital ecosystems, create exactly this type of fragmentation that generates new and extensive IT security risks. The paper (Badea & all, 2021) showed that "New technologies (Artificial Intelligence, Big Data, blockchain, cloud-computing, robotics / chat-notes, use of APIs, open-source software) completely reshape the banking system, creating a new digital financial ecosystem, accelerating the fragmentation of the traditional value chain, implicitly causing new value chains. Regulations have prepared this process (e.g. PSD 2 in the banking field, or Insurance Distribution Directive IDD (The European Parliament and The Council, 2016) in insurance)".

The European Commission estimates (2021a) that, compared to 2015, in 2020 the economic losses caused by cybercrime upon the global economy were 5.5 trillion EURO. Also 2 out of 5 Europeans experience cyber security problems while one in eight businesses are affected by cyber-attacks. One of the three strategic approaches is to strengthen the security of interconnected equipment, and services as well as of the digital ecosystems created through FinTech.

EU businesses and organizations spend 41% less on cybersecurity than their US counterparts. The European Parliament (2021c) is working to strengthen cybersecurity to enable the EU to become a global cyber player through building common EU cyber defense capabilities to ensure a high level of collective cyber security in the EU through the implementation of the NIS directive. According to the preamble (Negreiro, 2021) „The coronavirus pandemic has triggered an unforeseen acceleration in the digital transformation of societies around the world. Yet, it has also exacerbated existing problems, such as the digital divide, and contributed to a global rise in cybersecurity incidents. During this unprecedented situation, there has been an increase in malicious cyber-activity across Member States, as revealed by a recent Europol report. Cybersecurity issues are becoming a day-to-day struggle for the EU."

4. FinTech Advancements: Big Data, Artificial Intelligence, Blockchain

According to OECD (2021), "Cyber security risks, risk of hacking and other operational risks witnessed across the board of digital financial products/services have direct implications on data privacy and confidentiality. While the deployment of AI does not open possibilities of new cyber breaches, it could exacerbate pre-existing ones by, inter alia, linking falsified data and cyber breaches, creating new attacks which can alter the functioning of the algorithm through the introduction of falsified data into models or the alteration of existing ones." The use of AI applications in the financial sector can create, or intensify, financial and non-

financial risks, including cyber risks, and must be analyzed from the perspective of financial consumer and investor protection (AI can raise issues related to data quality and data confidentiality, cybersecurity, fairness, the management and use of personal and identity data, risks of manipulation and social engineering, incorrect or discriminatory results for consumers). The lack of explicability of AI model processes could increase pro-cyclical and systemic risks in markets and could create possible incompatibilities with existing financial supervision and internal governance, possibly leading to a technologically neutral approach to policy making. While many of the potential risks associated with artificial intelligence in finance are not unique to this type of innovation, the use of these techniques could amplify these vulnerabilities, given the complexity of the techniques used, their dynamic adaptability and their level of autonomy.

According to Yano & all (2019), "Information technology such as AI, IoT, and Big Data is expected greatly to contribute to the realization of a new human-friendly ecosystem. However, it is a mistake to think that such an ecosystem will be built if technological innovation is realized. The modern economy faces major problems of data monopoly and data abuse. Society-5.0 is something that can be formed only after overcoming those problems. Collect data from every part of a society by the IoT, create bigdata, analyze it with AI, and feed results of data analysis back to the society. An ecosystem realizing this loop is the blueprint of Society 5.0 advocated by the Japanese government."

In general, we analyze new technologies in terms of cyber risks and opportunities for attackers, who are always one step ahead of defense and prevention systems. In some cases, the new technology can provide the necessary defenses through the concepts that it introduces. For example, blockchain, which by design contains several protection elements. According to Ng & Kwok (2017), there is high hope that Fintech, especially Blockchain as a solution for secure information technology and data security, will bring along the development of innovative financial products and services, as well as the potential to improve the efficiency of the financial services industry.

Big Data (BD) is the main concept of capturing and analyzing very large volumes of data, structured or unstructured, by applying advanced analytical methods. BD works closely with Artificial Intelligence algorithms as a data provider for identifying behavioral patterns based on which AI systems make predictive decisions. At the same time, Big Data can also be used to store the information provided by IoT (Internet-of-Things) which is another technology utilized in FinTech and could be the source of the development of advanced mobility systems. Big Data has three important characteristics, volume, velocity, and variety. Data science is actively involved in the development of data collection methods and algorithms. The use of BD can raise advanced ethical issues as the volume and speed of information

processing may escape human supervision, and thus reach a point where the decisions it makes may be biased consciously or unconsciously. As it was the case for the other technologies, BD also comes with the need to prevent new types of cybercrime that can play a role in corrupting the data based on which important decisions can be made. In the opposite sense, BD can be used to prevent cybercrime, especially in preventing fraud by detecting suspicious transactions. The combination of BD and AI can easily identify patterns of fraudsters, money launderers, transactions on behalf of individuals or institutions through credentials theft, and other reprehensible financial facts supported by information technology, including real-time risk management and predictive decisions.

The robotization of the industry supported by AI and BD technologies, to which we can add chat-bot algorithms, can ensure increasing customer satisfaction, the improvement of the consumer experience and automatic management of certain operations or transactions, but can also affect the decision-making process through technologically enabled social engineering.

According to Niveditha & all (2020), "Big Data platform, the specific methods will help malware researchers successful done the time-consuming process of systematically investigating malicious events. Security researchers want to create a use of Machine Learning (ML) algorithms with big data techniques to evaluate and track indefinite malware in a large scale. These techniques consist of dynamic and wide flux of malicious binaries which aid them to solve the emerging threat environment….ML algorithms may characterize a file's actions as either harmful or benevolent based on information gathered from the file utilizing static or dynamic analysis. Through implementing there are various ML algorithms, the classification model developed up through training with labeled data set which have easily identify new data."

According to Sentient Digital (2020), AI is a multi-faceted tool that can be used both to collect and organize data and to protect it against external forces. Due to the widespread adoption of AI in business operations in recent years, artificial intelligence and cybercrime protection and deterrence have developed an interdependent relationship in contemporary cyber security models. AI raises four main threats to an organization: large-scale automated attacks, hacking of surveillance systems, manipulation algorithms, deception of facial or voice recognition. Because AI also provides a growing source of confidence in cybersecurity tactics, knowing how this technology can be implemented in cybersecurity will be paramount in protecting your organization.

In response to the potential risks posed by Fintech innovations, several cybersecurity initiatives are considered essential to prevent and mitigate such emerging risks in a technology-based environment. A first perspective, according to Ng & Kwok (2017), refers to anti-fraud measures such as the need to develop tools, procedures, or

techniques to break one or more of the three factors in the "fraud triangle". By implementing internal controls, the "opportunity" factor can be eliminated. Although the basic elements of fraud remain the same, fraudsters use new tools and techniques - especially those driven by information technology - against Fintech (Deloitte, 2015).

In response to such threats, any deterrence and detection measures should be adjusted accordingly (Entrust, 2015).

Identity authentication is one of the main deterrents against hacking and anonymity issues in Fintech. Therefore, several RegTechs-type measures are proposed to regulate potential Fintech fraud.

Authentication mechanisms, such as digital certificates, mobile device certificates, and biometric identification, can provide a higher degree of security than traditional password authentication. (Rowntree, 2016).

On 21 April 2021, the European Commission (2021c) published a proposal for a regulation aimed at addressing the risks of AI and establishing harmonized rules on the use of AI in all business sectors. At the same time, it also proposes the establishment of a European Artificial Intelligence Committee. According to the OECD (2021), while the general scope of the proposal is wide, the strictest requirements apply to high-risk AI applications, which include creditworthiness assessment. The requirements for such a high-risk AI include the use of detailed and specific risk and quality management systems as well as conformity assessments; use high-quality, representative, error-free and complete data; keep records and logs and be transparent to users about the use and operation of artificial intelligence applications. The proposed rules also introduce a requirement for human supervision by properly trained individuals; the use of explicit human confirmation for decision-making; ensuring the accuracy, robustness, and security of the system; monitoring and notifying the regulatory authority of serious incidents, as well as recording in a public register.

5. Cyber Threats and Defense Strategy – Impact, Resilience and Collective Approach

A paper by Arner's, Douglas W. & all (2015) presents the current evolution of Fintech, called FinTech 3.5, the forerunners of which predate 2008. The current version is characterized by the democratization of digital financial services through new technologies, "the financial services industry since 2008 has been affected by a "perfect storm", financial, political and public in its source, allowing for a new generation of market participants to establish a new paradigm known today as FinTech. .... FinTech today comprises five major areas: (1) finance and investment,

(2) operations and risk management, (3) payments and infrastructure, (4) data security and monetization, and (5) customer interface".

As Fintech continues to expand its footprint in the financial services sector so does the threat landscape that affects it. One must consider the fact that financial technology companies find themselves in need of processing more and more data as their efficiency grows. In contrast with traditional banks which are being constantly monitored by national and international regulatory bodies through several checks and balances mechanisms and thus obligated to pay special attention to cyber security principles, financial technology companies, which are not required to follow such strict guidelines, generally do not impose such strict cyber security controls. This fact, combined with the continuous growth of the Fintech industry, makes financial technology companies appealing targets for cyber threat actors.

Like traditional financial institutions, most of the financial technology companies operate with considerable amounts of customer personally identifiable information (PII) as well as customer sensitive financial data. Based on this fact we can say that common threat vectors impacting the financial services sector must be made a priority when designing the cyber defense strategy of Fintech organizations.

A company's operational risk can be defined as the risk of loss caused by inadequate internal procedures, failures of different company systems or external events that can disrupt business continuity. Even though cyber risk represents a subset of a company's operational risk, according to a trend analysis conducted by Aldasoro & all (2020) in "Cyber risk in the financial sector" published in SUERF Policy Note, Issue No 206, which used Google Trends to compare global search interest on the two terms revealed an almost equal score in 2020. The search interest on "cyber risk" appeared to be consistent with the increase in the number and complexity of cyber threats impacting organizations worldwide. We conducted a similar experiment which revealed that in January 2022, "cyber risk" top class "operational risk" in global search interest.

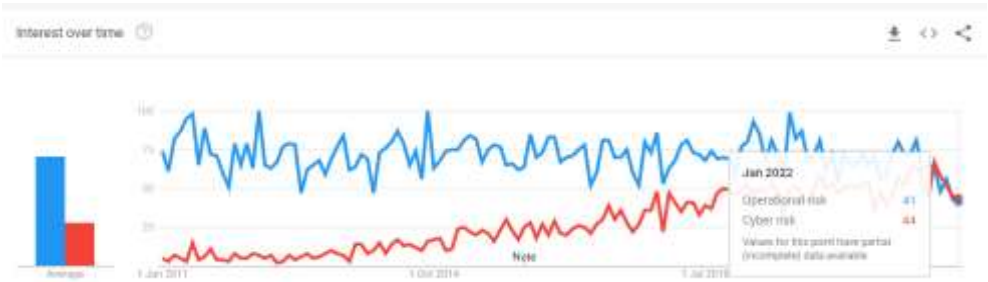

Figure 2. Number of Worldwide Searches for "Operational risk" and "Cyber risk" as per Google Trends Data. Data was Accessed on 24 January 2022

As general interest towards cyber risk increases so does the complexity of the cyber threats impacting the financial sector. The cause of a cyber-attack can vary and is directly linked with the type of threat actor responsible, ranging from unintentional incidents such as misconfigured systems and accidental data disclosure to malicious attacks executed by complex threat actors. Even though the threat actor ecosystem has been in a continuous shift in the last few years, impacted by the constant change in actor sophistication as well as the interference caused by law enforcement within actor underground communication channels, threat actors can still be classified in three important categories depending on their area of activity, motivation, and capabilities: hacktivists, financially motivated actors and nation state actors.

Even though the classifications did not suffer significant changes over the years, the techniques employed by the threat actors evolved. One attack vector that is of great concern to the financial services sector is ransomware, propagated by the ever so notorious ransomware gangs. These are highly organized financially motivated threat actors employing "double extortion" as a mode of operation; the threat actor not only prevents the victim from accessing his data by deploying locker software on their systems, but also downloads a copy of that data to put maximum pressure on the target.

Table 1. Correlations

	Hacktivists	Financially motivated threat actors	Nation State threat actors
Capabilities	Usually not very capable, they engage in offensive campaigns by using simple scripts and exploiting known vulnerabilities	Capabilities can vary for this category ranging from the utilization of simple scripts and known exploits to the execution of sophisticated campaigns.	Usually, capable individuals engaging in sophisticated campaigns that are sponsored by a state entity.
Motivation	Usually politically motivated with their campaigns tightly linked to social causes.	Financial gains	Usually aligned with the strategic interests of a nation state.

Source: Author's processing

Another type of threat that has the potential to greatly impact organizations operating in the financial sector is represented by the rise of information stealer malware.

Research in the cybercriminal underground revealed numerous instances of threat actors engaging in the development and distribution of different variants of information stealer malware. This type of software is commonly used to harvest information from the victim's browser such as credentials, autocomplete data, credit card information as well as cookie related data. Once the data is extracted from the victim, the actors either make use of it for financial gains in more complex operations or put it up for sale across different illicit forums and communication channels. Research revealed that in some situations, threat actors repurpose legitimate infrastructure such as the instant messaging service Telegram and use it to sell stolen authentication data of users of various financial services and financial technology companies, obtained from information stealer malware operations.

There is an interesting point of view made in an article titled "International Strategy to Better Protect the Global Financial System against Cyber Threats" released by the Carnegie Endowment for International Peace in November 2020 (Maurer & Nelson, 2019) which reinforced the idea that the tremendous increase in cyber-attacks is not just a problem for high income countries but a global one. The authors argue that the digitalization of the financial sector was, in some cases, happening at a greater pace in low to middle income countries, which makes the financial organizations that operate in said countries a target for threat actors. We concur to the point made by the article which states that while technical and financial resources are not lacking in the financial services sector, they should be leveraged by the organizations to devise a solid cyber defense strategy that incorporates national as well as international standards.

The "International Strategy to Better Protect the Global Financial System against Cyber Threats" (Maurer & Nelson, 2019) article introduces three core pillars as a baseline for a solid cyber defense strategy.

- Cyber Resilience which refers to the strengthening of collective cyber defense practices.

- International Norms which refer to the implementation and enforcement of international cyber security policies.

- Collective Response which refers to the collective effort in combating and disrupting threat actors and malicious activity mostly done through information sharing.

In addition to the aforementioned pillars, we propose a fourth pillar in the form of Cyber awareness which refers to an organization's level of understanding of the cyber threats it faces as well as the technology stack available to combat those threats.

As the type and severity of cyber threats an organization faces are strongly dependent on the country it is operating in, a strong public-private partnership is paramount in

the conception and implementation of a solid cyber defense strategy. In a November 2019 article written by Silvia Baur-Yazbeck, Judith Frickenstein and David Medine (2019) titled "Cyber Security in Financial Sector Development - Challenges and potential solutions for financial inclusion", the authors stated the importance of public-private partnerships in combating the effects of cyber-criminal activity and listed several examples of good practices which are worth mentioning such as the Israel's National Fintech-Cyber Innovation Lab, Luxembourg's Cyber Competence Center and Nigeria's Electronic Fraud Forum. All the aforementioned organizations act as cyber support centers for organizations, either through investment or through shared resources. We could argue that another good example, closer to home, that fits the criteria is the European Bucharest-based Cybersecurity Competence Centre which aims to bring together stakeholders from industry, academia and research organizations with the goal of creating a cybersecurity competence community.

Silvia Baur-Yazbeck, Judith Frickenstein and David Medine (2019) illustrate in their paper good examples of both Cyber Resilience and Collective Response pillars being considered by organizations operating in the private sector. The article lists several examples of private organizations that grouped together to increase their cyber resilience through threat intelligence sharing and capacity building programs such as the G4C German Competence Centre against Cyber Crime eV, the Cyber Security Operation Centre for Inclusive Finance, operating in Senegal and created by Suricate Solutions, the South African Banking Risk Information Centre (SABRIC), the Thailand Banking Sector CERT as well as the United States' Financial Services Information Sharing and Analysis Center (FS-ISAC).

6. Results and Recommendations

Today, FinTech companies have become even more established favorites as targets of cyber-attacks, which is why cybersecurity should be one of the most thought-out strategies for protecting against such cyber fraud related to technology and proactive activities. At the end of the day, it demands certain features on the market such as agility, flexibility, confidentiality, security, low prices in the fundamental pillars of IT: cloud, big data, and analytics. According to data provided by Finaria.it, "the global digital payments industry is expected to hit a $ 6.6trn value in 2021, a 40% increase in two years." According to the same sources, in 2021, 55% of payments were made without cash in the early financial inclusion of FinTech, changing the traditional financial category with something more up to date that generates greater protection for the user, as the risk of being victims. Cyber-attacks will increase as the visibility of your business increases. Within the FinTech industries, technologies are being implemented to provide more efficient financial services, but one of their main problems is exposure to various digital risks or phishing attacks, data theft or ransomware, for which cybersecurity experts recommend different strategic

solutions for prevention and protection of threats in digital financial companies, such as:

1. Establish beta strategies - At this stage, the security of both the network and the mobile application server deployed for the launch can be verified so that FinTech can reduce the security risks on its platform before it is used by end user.

2. Have identification and authentication systems - it may not be an idea at all to implement, but not all FinTech establish this system. The respective software implemented in the digital bank must require the identification and authentication of the user, i.e., to restrict access to the areas most likely to be attacked by cybercriminals, with certain personalization passwords per customer.

3. Data encryption - having a data encryption system is the best way to avoid leaking or cloning customer data, ensuring greater protection. Today, one of the most secure is the AES system.

4. Implementation of systems for blocking suspicious payments - restrictions will be applied on unsafe activities or payments of suspicious amounts.

5. Perimeter security - To have a more viable cybersecurity infrastructure within the FinTech mobile application, it is necessary to implement perfectly configured perimeter security systems and routers using https web URLs or create more secure networks. using VPN.

6. Set the ISO 27001 standard - this will allow you to obtain a Subjective Information Security Management System (ISMS), providing security guarantees to your customers.

7. Limit the storage of information - certain crucial information will be stipulated for transactions, keeping the most sensitive information to be cloned, archiving it in more secure systems. Following these recommendations, we know that one of the main challenges of FinTech is cybersecurity, and to the extent that certain sophisticated models are implemented, it will be possible to control and avoid the risks that could be generated, presenting a better service to its user. However, there will be more digital attacks with different destinations, so it is essential to have a comprehensive cyber security strategy, attack prevention and staff training, to mitigate them as much as possible, backing up the information on both servers, both from the company and from its own users

7. Conclusion

The relationship between FinTech and CyberSecurity is an extremely important issue for the financial sector, especially since, given the evolution of the market and recent events, more and more customers are migrating to digital channels, and transactions and payments are moving online. All regulations in accordance with ISO 270001, responsibilities in the field of information security must be assigned to a dedicated education system: cyber security, vulnerability management, information governance and the security of digital identities. From this reason we propose a dedicated pillar, complementary to the ones mentioned in our paper, Cyber awareness - which refers to an organization's level of understanding of the cyber threats it faces as well as the technology stack available to combat those threats.

This paper supports the conclusion of a new paradigm by combining FinTech approaches with cybersecurity methodologies and technologies. This junction determines the 360-degree use of innovative technologies, both for the development of new products and services, new digital ecosystems, and for preventing and combating cybercrime, together with continue awareness. This emerging fintech-cyber system will need to be surrounded by a layer of regulations that will allow it to thrive in a controlled and monitorable environment. Practice has shown that new technologies have created trust among people around the world, with cryptocurrencies exceeding $ 1,000 billion in value, although this value is not yet recognized as a financial asset. This confidence in technology is equivalent to the trust in the classic fiduciary system of the financial-banking field. This confidence can be shaken by the threats of cybercrime as well as using Fintech technologies which can generate risks and uncertainties. The conclusion of our study is that a combined effort, which has become urgent, is needed to recognize the new pillars of digital financial ecosystems which needs to be addressed from multiple angles such as regulatory, monitoring and implementation as well as through referring to the classical structures that will have to coexist and transform in an average period of time.

8. Acknowledgement

Author Contributions: Conceptualization, M.C.S., C.M.R. F.V.P. and D.M.L.; Methodology, M.C.S. and C.M.R.; Formal analysis, C.M.R, F.V.P. and D.M.L.; Investigation, C.M.R. and D.M.L.; Resources, C.M.R, F.V.P. and D.M.L.; Data curation and analysis, M.C.S. and C.M.R.; Writing—original draft preparation, C.M.R. F.V.P. and D.M.L.; Writing—review and editing, M.C.S., C.M.R. F.V.P. and D.M.L.; Visualization, M.C.S., C.M.R. F.V.P. and D.M.L.; Supervision, M.C.S. and C.M.R.; Project administration, M.C.S.; Funding acquisition, M.C.S.

All authors have read and agreed to the published version of the manuscript

Funding: This work was supported by a grant from the Romanian Ministry of Education and Research, CNCS-UEFISCDI, project code CNFIS-FDI-2021-0564, entitled "Development of institutional research capacity in UMC by improving R&D infrastructure and development of sustainability activities and intelligent experimental support".

Data Availability Statement: Data used in this analysis is not public, but available upon request.

Conflicts of Interest: The authors declare no conflict of interest

References

Arner, Douglas W.; Barberis, Janos Nathan & Buckley, Ross P. (2015). The Evolution of Fintech: A New Post-Crisis Aldasoro, I., Frost, J. Gambacorta, L., Leach, T. & Whyte, D. (2020). Cyber risk in the financial sector. *The European Money and Finance Forum (SUERF)*. *Policy Note*. Issue No 206. https://www.suerf.org/policynotes/18421/cyber-risk-in-the-financial-sector.

Arner, Douglas W.; Barberis, Janos Nathan & Buckley, Ross P. (2015). The Evolution of Fintech: A New Post-Crisis Paradigm?. University of Hong Kong Faculty of Law. *Research Paper* No. 2015/047, *UNSW Law Research Paper No. 2016-62*, SSRN: https://ssrn.com/abstract=2676553 or http://dx.doi.org/10.2139/ssrn.2676553.

Badea, L, Rangu, M. C. & Șcheau, M. C. (2021). Considerations on Digital Financial Ecosystem. Conference: *23rd RSEP International Economics, Finance & Business Conference. University of Washington Rome Center*. https://www.researchgate.net/publication/356832084_Considerations_on_Digital_Financial_Ecosystem_nov_2021.

Baur-Yazbeck, S.; Frickenstein. J. & Medine, D. (2019) Cyber Security in Financial Sector Development - Challenges and potential solutions for financial inclusion. *Consultative Group tiAssist the Poor (CGAP) & Gesellschaft fur Internationale Zusammenarbeit on behalf of Federal Ministry of Economic Cooperation and Development*. https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf.

Deloitte (2015). 2016 Hot topics for IT internal audit in financial services. *Web page*. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-audit-on-the-horizon.pdf.

Entrust (2015). 3 Ways Financial Institutions Can Improve Fraud Detection. *Web page*. https://www.entrust.com/blog/2015/09/3-ways-financial-institutions-can-improve-fraud-detection/.

Estelle, M. P & Derek, S. P (1994). How to Get a Phd: A Handbook for Students and Their Supervisors. Open University Press; 6th edition (1 Aug. 2015).

European Commission (2019). Digital Economy and Society Index (DESI). *Web page*. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2019.

European Commission (2020). New Europol report on latest developments of COVID-19 on the criminal landscape in the EU. *Web page*. https://digital-strategy.ec.europa.eu/en/news/new-europol-report-latest-developments-covid-19-criminal-landscape-eu.

European Commission (2021a). A cybersecure digital transformation in a complex threat environment — Brochure. *Web page*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/cybersecure-digital-transformation-complex-threat-environment-brochure.

European Commission (2021b). Digital Economy and Society Index (DESI). *Web page*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/desi.

European Commission (2021c). Proposal for a Regulation laying down harmonised rules on artificial intelligence, Laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. *Web page*. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF.

European Parlament. (2021a). *Web page*. https://www.europarl.europa.eu/news/en/headlines/priorities/digital.

European Parliament. (2021b). *Web page*. https://www.europarl.europa.eu/news/en/press-room/20210604IPR05531/parliament-calls-for-beefed-up-eu-security-against-cyber-threats.

European Parliament. (2021c). MEPs demand common EU cyber defensive capabilities. *Web page*. https://www.europarl.europa.eu/news/en/press-room/20210930IPR13930/meps-demand-common-eu-cyber-defensive-capabilitiesats, date: 20.12.2021.

European Parliament (2022). *Web page*. https://www.europarl.europa.eu/news/en/headlines/priorities/eu-response-to-coronavirus.

Lațici, T. (2019). *Cyber: How big is the threat?* European Parliamentary Research Service. *Web page*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf.

Maurer, T. & Nelson, A. (2019). International Strategy to Better Protect the Global Financial System against Cyber Threats. *Carnegie Endowment for International Peace*. Retrieved from https://carnegieendowment.org/files/Maurer_Nelson_FinCyber_final1.pdf.

Negreiro, M. (2021). *The NIS2 Directive, A high common level of cybersecurity in the EU*. European Parliamentary Research Service, *Web page*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

Ng, A.W. & Kwok, B. K. B. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator", *Journal of Financial Regulation and Compliance*, Vol. 25 No. 4, pp. 422-434. *Web page*. Retrieved from https://doi.org/10.1108/JFRC-01-2017-0013.

Niveditha, V. R., Ananthan, T. V., Amudha, S., Sam, D. & Srinidhi, S. (2020). Detect and Classify Zero Day Malware Efficiently In Big Data Platform. *International Journal of Advanced Science and Technology*. Vol. 29, No. 4s, (2020), pp. 1947-1954.

Organisation for Economic Co-operation and Development – OECD. (2021). *Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers*. *Web page*. Retrieved from https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf.

Pollari, I. & Ruddenklau, A. (2021). Pulse of Fintech, H1'21. *KPMG International. Web page*. Retrieved from https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/08/pulse-of-fintech-h1.pdf.

Rowntree, L. (2016). How Biometrics in Fintech Can Bring a Different Angle to Using Biometrics in Advertising. Exchange Wire. *Web page*. https://sdi.ai/blog/artificial-intelligence-and-cyber-crime/.

Scheffer, J.; Pupillo, L.; Griffith, M. K.; Blockmans, S. & Renda, A. (2018). Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force. *Centre for European Policy Studies (CEPS). Web page*. ; https://www.ceps.eu/wp-content/uploads/2018/11/CEPS_TFR%20on%20Cyber%20Defence_1.pdf.

Sentient Digital (2020). Artificial Intelligence and Cyber Crime: Facing New Threats. *Web page*. https://sdi.ai/blog/artificial-intelligence-and-cyber-crime.

Ursula, L. (2021). State of the European Union 2021. European Commission. *Web page*. https://multimedia.europarl.europa.eu/en/package/state-of-european-union-2021_20101.

Yano, M.; Dai, C.; Masuda, K. & Kishimoto, Y. (2019). Creation of a Blockchain and a New Ecosystem. Research Institute of Economy. *Trade and Industry RIETI Policy Discussion Paper Series* 19-P-029. Retrieved from https://www.rieti.go.jp/jp/publications/pdp/19p029.pdf.