

Cybersecurity and the Development of the FinTech Sector in European Union Countries

Łukasz GIBOWSKI^{1*}, Krzysztof ŁUSIAKOWSKI²

¹ Kielce University of Technology, Faculty of Management and Computer Modelling, Poland; e-mail: lukaszgibowski1@wp.pl, ORCID iD: 0009-0007-9661-8268

² Kielce University of Technology, Faculty of Management and Computer Modelling, Poland; e-mail: klusiakowski@tu.kielce.pl, ORCID iD: 0009-0001-5770-2949

* corresponding author

Abstract

Research background: The dynamic growth of the FinTech sector in recent years has significantly influenced the transformation of financial systems in European Union (EU) countries. However, due to the digital nature of their operations and the processing of sensitive financial data, companies in the FinTech sector are particularly vulnerable to breaches of the integrity, confidentiality and availability of information.

Purpose: The main aim of the study is to assess the relationship between the level of cybersecurity and the degree of development of the FinTech sector in EU countries.

Methodology: Qualitative and quantitative methods were used to achieve the research objective. In particular, a review of the relevant literature and desk research were conducted. Spearman's rank correlation coefficient was used to determine the relationship between the level of cybersecurity and the degree of development of the FinTech sector in EU countries.

Findings: The analysis did not reveal a clear relationship between the level of cybersecurity and the degree of development of the FinTech sector in EU countries in 2020 and 2024. The observed variation between countries indicates that this relationship is complex and shaped by a range of co-occurring factors, which justifies the need for a multidimensional analysis.

Practical implications: The results point to the need to continuously take cybersecurity risks into account in management and supervisory processes within the FinTech sector. In the context of EU countries, this also suggests the necessity of accounting for variations in cybersecurity levels when shaping policy for the development of the FinTech sector.

Originality / value: This study provides an integrated approach to cybersecurity risks in the context of the FinTech sector's development. It combines theoretical analysis with an empirical assessment of the relationship between cybersecurity levels and advancement of financial technologies in EU countries.

Keywords: financial technologies; transformation of financial systems; risk; cybersecurity.

JEL classification: C89, G23, O32.

1. Introduction

The rapid growth of the FinTech sector in recent years has become one of the key drivers of the transformation of the global financial system. Innovative technologies have changed the way financial services are provided to both retail and institutional clients. However, as digitalisation progresses, the level of risk is increasing, particularly in the area of cybersecurity. Entities in the FinTech sector, which often handle sensitive customer data, are becoming particularly vulnerable to cyberattacks. In recent years,

there has been an increase in the number of incidents involving, among other things, hacking attacks and ransomware. This determines the level of user confidence in the digital financial services market.

Deloitte, a leading firm in the audit and advisory sector, has shared key findings from a survey conducted in 2024 in the form of interviews with FinTech leaders. The study focused on analysing the extent of collaboration between risk, compliance and innovation teams. The study revealed that gaps still exist in FinTech risk management. Only 34% of survey respondents stated that they had a dedicated risk committee at board level. In contrast, 75% of respondents declared that they had an audit committee. This may suggest that FinTech companies' approach to risk oversight is reactive. It is based mainly on audit results or incident analysis, rather than on proactive monitoring. This becomes particularly problematic in the context of emerging threats, such as sophisticated cyberattacks, complex financial crimes, risks arising from the actions of third parties, or risks generated by AI (Aron et al., 2026).

The main aim of the study is to assess the relationship between the level of cybersecurity and the degree of development of the FinTech sector in EU countries. The empirical section covers the years 2020 and 2024, and the data used in the analysis are sourced from Crunchbase.com, Eurostat and reports by the International Telecommunication Union (ITU). Achieving the research objective involved the following stages:

- a review of the literature on cybersecurity and the development of the FinTech sector,
- collection and verification of data on the level of cybersecurity and the development of the FinTech sector in EU countries for the years 2020 and 2024,
- analysis of the relationship between the level of cybersecurity and the degree of development of the FinTech sector using statistical methods,
- interpretation of the results obtained and assessment of the differences between EU countries in the area under study.

In order to achieve the aim of the study, the following research questions were formulated:

- Is there a correlation between the level of cybersecurity and the degree of development of the FinTech sector in EU countries?
- Do countries with a more developed FinTech sector exhibit higher levels of cybersecurity?

Based on the research questions posed, the following research hypotheses were formulated:

- Hypothesis 1: There is a statistically significant correlation between the level of cybersecurity and the degree of development of the FinTech sector in EU countries.
- Hypothesis 2: Countries with a higher level of development in the FinTech sector are characterised by a higher level of cybersecurity.

The originality of this study lies in its empirical analysis of the relationship between the level of cybersecurity and the degree of FinTech sector development in European Union countries. The existing literature has mainly focused on theoretical approaches and conceptual models describing cybersecurity and the development of the FinTech sector (Idayani et al., 2024; Greser, 2024; Kamuangu, 2024; Karangara & Manta, 2024), and only to a limited extent does it undertake empirical verification of these relationships. Existing quantitative studies, however, most often focus on the analysis of individual countries, such as Iraq (Al_Duhaidahawi et al., 2020), which limits the possibility of comparing results internationally and generalising them to a wider group of countries.

2. Literature review

Based on an analysis of the results of secondary research, theoretical, empirical and methodological research gaps have been identified. From a theoretical perspective, this stems from the predominance of conceptual approaches describing cybersecurity in the FinTech sector, whilst its links to the sector's level of development are given limited consideration. The empirical gap concerns the lack of quantitative research analysing the relationship between the level of cybersecurity and the degree of development of the FinTech sector in a comparative analysis across European Union countries. The methodological gap, in turn, concerns the limited use of classical quantitative methods to analyse the relationship between the phenomena under study.

Risk, as an inherent component of business operations, influences the decisions made by economic entities and the directions of their development. In a rapidly changing environment, companies must take its presence into account. As P. Buła (2015) points out, risk is present in all processes within a company and is linked to the performance of its specific functions. Consequently, it is necessary to continuously conduct an effective process aimed at mitigating identified risk categories. Crucially, the specific approach to risk management should be tailored to the company's profile. This is of particular importance in companies focused on innovative processes (Woźniak & Wereda, 2023). It is here that opportunities and threats converge, forming the very essence of risk (Damodaran, 2009). Examples of such entities include companies in the innovative financial technology (FinTech) sector, which, by offering financial services through innovative technologies, are exposed to specific types of risk. The literature distinguishes two main approaches to defining the term FinTech – the objective and the subjective. From a subjective perspective, it refers to the industry of technology companies (or their representatives) utilising information and communication technologies to provide financial services. Their activities result in the creation of new business models, processes, products and financial services (Folwarski, 2021; Jagodzińska-Komar, 2025). In the object-oriented approach, on the other hand, it refers to all technologies used in the process of providing financial services (Ha, Le & Nguyen, 2025; Pawłowska, 2023).

The risk specific to the FinTech sector can be defined as an uncertain event or condition which, if it occurs, poses a threat or presents an opportunity for a FinTech initiative (Alvarez-Dionisi, 2020). Table 1 presents the risk categories, ranked by significance, that determine the operations of entities in the FinTech sector.

Table 1. Risk category ranking for companies in the FinTech sector

Ranking position	Risk category	Characteristics
I	Reputational risk	One of the causes of this risk is a poorly managed customer service process. Such practices may directly or indirectly create a negative image of the service provider. Consequently, this affects how the provider is perceived by existing and potential customers. Importantly, the heavy penalties resulting from the materialisation of this risk are particularly severe for new entrants.
II	Cybersecurity risk	This stems from a lack of information integrity, availability and confidentiality. Cyber threats pave the way for numerous scams and crimes. The processing of sensitive financial data in the FinTech sector makes companies prime targets for cybercriminals. Incidents in this area include data breaches, hacking attacks and ransomware. Given the particularly vulnerable digital nature of the services provided by the FinTech sector, the level of risk must be constantly monitored and strictly controlled. A lack of effective oversight can undermine customer confidence in financial services, not to mention its direct impact on transaction security.

Ranking position	Risk category	Characteristics
III	Risk associated with financial crime, including AML/CFT risk	Fraud and financial crime currently represent one of the most significant threats to FinTech companies. Criminals, armed with the latest technology, are circulating illicit funds. Consequently, FinTech companies should implement appropriate procedures to mitigate these risks. Furthermore, if they provide financial services directly, they are obliged to protect customer accounts by using solutions such as biometric authentication, dynamic CVV codes and other innovations to maximise security.
IV	Compliance risk	Digital technologies continue to evolve within the FinTech sector, necessitating frequent regulatory changes. Operating across multiple jurisdictions also presents an additional burden. In this context, the priority should be to offer financial products in full compliance with local regulations. Supervision should focus on the ongoing monitoring of compliance, although the online activities of the FinTech sector still remain partly outside detailed regulation.
V	Operational risk	This risk arises from the malfunctioning of internal and supervisory processes, external disruptions, system failures and staff errors. It is the managers' responsibility to manage this category of risk on an ongoing and continuous basis.
VI	Market risk	FinTech companies operating in foreign markets are highly exposed to market risk. This risk stems from fluctuations in interest rates, exchange rates and other external factors that may affect their financial performance.
VII	Technological risk	Whilst the introduction of new technologies can, on the one hand, improve customer service and operational processes, on the other hand, the hasty implementation of innovative solutions without proper planning leads to incidents. Conversely, a failure to adopt innovations leads to the solutions currently in use becoming obsolete; therefore, changes should be implemented safely and in compliance with applicable regulations.
VIII	Financial risk	Financial risk depends on the size and scale of the business undertaken and the specific segment of the FinTech sector. It may include credit risk or liquidity risk. Failure to manage these risk categories may lead to bankruptcy and the cessation of business. It should be borne in mind that, in the case of digital loans, the number of defaults is higher than for traditional loans. To mitigate credit risk, lenders must ensure that the data used to assess borrowers' financial situations is up to date and reliable.
IX	Third-party risk	As FinTech companies join the digital ecosystem, they must rely on external suppliers and contractors, which creates additional risks. In this context, due diligence in verifying the parties involved in the provision of products and services is crucial. Disruptions in the operations of third parties could result in a threat to the data of FinTech customers.
X	Strategic risk	FinTech companies face numerous strategic challenges as they expand their operations. Diversifying their products and services is of paramount importance, particularly in the face of growing competition in the global market. In this context, building a distinctive brand has become a key factor for success.

Source: own compilation based on: Jain et al., 2023; Kwon et al., 2023; Thompsett, 2024.

The comprehensive list of risks in the sector in question, as set out in Table 1, highlights the need to implement an effective risk management system. The comprehensiveness of the risk management system determines the extent to which all risk categories are covered. However, business practice appears to differ in this respect. FinTech companies are not only exposed to specific risks themselves, but also create new opportunities and potential threats for the users of their services. According to B. Zhao (2025), by applying innovative technological solutions in finance, FinTech companies introduce new and unpredictable threats, including those related to increased exposure to cyber threats. Furthermore, these companies exert competitive pressure on traditional financial institutions.

The role of cybersecurity in the operations of FinTech entities cannot be overstated (Olaiya et al., 2024). According to M. Górka (2018), cybersecurity today poses a significant challenge in the context of cooperation among national institutions, private companies, and non-governmental organisations, as well as at the international level, involving collaboration between states and regional and global organisations. As noted R. Jain et al. (2023), the development of financial technologies has reduced physical crime, but at the same time increased cybercrime (Joel et al., 2025). One must agree with the argument put forward by M. O. Joel et al. (2025) that cybersecurity is currently a key issue for the FinTech sector. One must bear in mind the increasing reliance on digital financial services and the growing volume of sensitive data processed by FinTech platforms. With threats constantly evolving, preventive cybersecurity solutions are essential to protect financial data, defend against cyber threats and maintain the trust of customers and stakeholders within the digital financial ecosystem. The FinTech sector faces numerous cybersecurity challenges, including data breaches, ransomware attacks, social engineering, and emerging threats associated with new technologies such as quantum computing, AI and blockchain. Regulatory compliance is also a key factor, as FinTech companies are required to adhere to data protection regulations and cybersecurity regulations governing the services they provide. Achieving and maintaining compliance requires a comprehensive approach that takes into account the right to data privacy, the maintenance of security standards, and consumer protection.

According to data presented in the ENISA Threat Landscape 2025 report, which analyses the European cyber threat landscape for the period from July 2024 to June 2025, the breakdown of reported incidents reveals significant sectoral variation. In quantitative terms, the highest proportion of reports concerned the public administration sector (38.2%), which demonstrates its particular exposure to cyber threats. This was followed by the transport sector (7.5%), the digital infrastructure and services sector (4.8%), the financial sector (4.5%) and the manufacturing sector (2.9%). Within the financial sector, the dominant category of incidents was DDoS¹ attacks (83.5%), confirming their significance as a key factor in disrupting the operational continuity of financial institutions. This was followed by incidents classified as cybercrime (14.8%) and digital attacks against public institutions (1.7%) (ENISA, 2025). A different picture of the sectoral structure of incidents is presented in the 2024 Annual Report on the activities of CERT Polska: The Security Landscape of the Polish Internet. According to the data presented therein, in 2024 the largest share of the total number of incidents handled by CERT Polska, broken down by economic sector (in accordance with the internal classification of CSIRT NASK), was recorded in the financial markets infrastructure sector (42.6%). In turn, the banking sector accounted for 2.5% of all incidents recorded (NASK National Research Institute, 2025). The discrepancies identified between the reports stem from differing methodological assumptions, the scope of the analysis and the sectoral definitions adopted; however, they unequivocally confirm the significance of cyberattack threats in the broadly defined finance sector.

The growing use of digital technologies requires measures to strengthen cybersecurity in the financial markets. Both the European Union and individual Member States recognise this need and have been increasing investment in this area for several years. The Multiannual Financial Framework (2021-2027) allocates approximately €2.9 billion from EU funds for this purpose, which represents almost a twofold increase compared to the previous Framework (2014-2020) (Polish Economic Institute, 2025). In Poland, the Polish Financial Supervision Authority is carrying out a task as part of the project 'CSIRT KNF – establishment and development of a sectoral cybersecurity team for the banking sector and financial market infrastructure'. Under the project, over 13 million zlotys will be allocated to the development of

¹ An acronym for Distributed Denial of Service.

the CSIRT KNF sectoral cybersecurity team. The aim of the project is to enhance the digital security of financial institutions and to protect customers using banking services (KNF, 2025).

Cyber threats give rise to numerous categories of risk, affecting both individual institutions and the financial system as a whole. Countries with higher levels of cybersecurity can more effectively limit the scale and consequences of these threats, which should potentially strengthen the stability and resilience of the rapidly growing FinTech sector. Conversely, the rapid growth of the financial technology sector, coupled with insufficient security measures, may lead to the accumulation of risk and increased vulnerability to cyber incidents. It is therefore appropriate to empirically examine the relationship between the level of cybersecurity and the degree of development of the FinTech sector, thereby enabling the verification of potential correlations between these variables.

3. Methods

Both qualitative and quantitative methods were used in the research. In particular, desk research was conducted. The years 2020 and 2024 were selected for analysis because, from 2020 onwards, the ITU Cybersecurity Index (the measure of cybersecurity levels in a given EU country adopted for the analysis) is presented on a scale of 0 to 100. This ensures the comparability of the data. Furthermore, only two reports based on the specified research methodology have been published to date (in 2020 and 2024). Two quantitative indicators were adopted as measures of the development of the financial technology sector: (1) the number of FinTech companies per 500.000 inhabitants and (2) the percentage of online banking users reported by Eurostat.

To determine changes in the number of FinTech companies, data from the Crunchbase.com portal were used, which serves as a source of information on the financial technology industry utilised by both EU institutions and in academic research (Folwarski, 2019; Gibowski, 2025). Converting the number of FinTech companies per 500.000 inhabitants in individual EU countries is a standardisation procedure that enables the derivation of a comparable indicator of the sector's development intensity. This eliminates the impact of demographic differences between Member States and enhances the accuracy of the comparative analysis. The population figures for EU countries were obtained from Eurostat (as at 31 December of the relevant year). A comparison constructed in this way allows for a parallel assessment of the cybersecurity dimension and two aspects of the FinTech sector's development: supply (number of companies) and demand (the scale of internet banking usage by the public). The choice of these two indicators stems from the need to capture the two-sided nature of the FinTech sector's development, which depends, on the one hand, on the activity of entities offering financial technology services (the supply side) and, on the other, on the extent to which these services are adopted and used by users (the demand side). This approach helps to avoid a one-sided analysis and better reflects the actual level of development of the FinTech ecosystem in individual countries. In particular, there is no single, official composite measure covering the entire FinTech sector at an international level, which justifies the use of proxy variables. For this reason, the two simplified indicators mentioned above have been used. This provides a holistic, albeit simplified, view of the development of the FinTech sector. It should also be noted that limiting the analysis to just two variables describing the development of the FinTech sector constitutes a significant simplification of the research. The indicators adopted do not fully reflect the complexity of this sector; however, given the limited availability of comparable data for all EU countries, they represent the most consistent and measurable approximation of the phenomenon under study. Consequently, the results obtained should be interpreted with due regard to their limited scope of information. The relationships between

the variables under study were analysed using Spearman's rank correlation coefficient. The use of Spearman's rank correlation coefficient stems from the nature of the data, which do not meet the assumptions of a normal distribution and are ordered, justifying the use of non-parametric methods. This approach ensures that the statistical analysis is appropriate for the data structure and enhances the reliability of the results obtained. In addition, a general comparative analysis of countries was carried out by dividing them into groups based on their level of cybersecurity (using quartiles). The differences between the identified groups of countries in terms of the level of development of the FinTech sector were then assessed, which allowed for a more in-depth interpretation of the relationship between the level of cybersecurity and the development of the FinTech sector. The study did not employ regression models or panel models, primarily due to the nature and limitations of the available data. Firstly, the analysis covers only two time points (2020 and 2024), which significantly limits the possibility of using classical panel models to analyse changes over time. Panel models provide greater insights when used with longer time series, as they allow for the observation of persistent relationships and country-specific effects. In the present case, the number of time periods is too small to obtain stable and methodologically reliable parameter estimates.

4. Results and discussion

Table 2 compares EU countries in terms of their level of cybersecurity and the development of the FinTech sector in 2020 and 2024 respectively. Three indicators were taken into account: (1) the ITU Cybersecurity Index, (2) the number of FinTech companies per 500.000 inhabitants, and (3) the percentage of people using online banking.

A preliminary analysis suggests that the relationships between the level of cybersecurity and the development of the FinTech sector are complex and heterogeneous. Different models of development in the financial technology sector are observed across individual EU countries. In such circumstances, the use of simple regression models could lead to an oversimplification of the relationships under analysis and to a misinterpretation of the results. For this reason, it was decided to use Spearman's rank correlation coefficient, which is a non-parametric method for assessing the interdependence between variables. This method is more robust to the presence of outliers, non-normal distributions and non-linear relationships, making it more suitable for the specific nature of the data under analysis. An analysis of data for 2020 reveals variations in cybersecurity levels and in the development of the FinTech sector across individual EU countries. The values of the Spearman's rank correlation coefficient confirm a weak correlation. For the relationship between the Cybersecurity Index and the number of FinTech companies per 500.000 inhabitants, it stood at 0.17, whilst for the Cybersecurity Index and the percentage of users of online banking, it was 0.38. The results indicate that, although in the selected countries a higher level of cybersecurity coexists with a relatively greater scale of development in the innovative financial technology sector, no uniform or strong correlation between these phenomena can be established. For example, Estonia stands out for both the highest level of cybersecurity (99.48 points) and the highest number of FinTech companies per 500.000 inhabitants (3.130). It also recorded one of the highest percentages of online banking users (79.84%). In contrast, in Spain, despite a very high Cybersecurity Index (98.52 points), there was a relatively modest number of companies per 500.000 inhabitants (0.152) and a low percentage of online banking users. Cyprus (88.82 points) and Malta (83.65 points), on the other hand, were characterised by a high concentration of FinTech companies (2.349 and 1.748 per 500.000 inhabitants respectively), alongside a relatively average level of cybersecurity. Countries such as Romania and Bulgaria, on the other hand, are characterised by both

a low level of cybersecurity (76.29 and 67.38 points respectively), and a limited scale of FinTech sector development, measured by the number of FinTech companies per 500.000 inhabitants (0.061 and 0.161 respectively) and the percentage of online banking users (11.65% and 12.57%).

Table 2. Ranking of EU countries by level of cybersecurity and development of the FinTech sector in 2020 and 2024

Country	2020			2024		
	Cybersecurity Index (in points – scale from 0 to 100)	FinTech sector		Cybersecurity Index (in points – scale from 0 to 100)	FinTech sector	
		Entities: Number of FinTech companies per 500.000 inhabitants	Users: Percentage of people using the internet for online banking		Entities: Number of FinTech companies per 500.000 inhabitants	Users: Percentage of people using the internet for online banking
Austria	93.89	0.160	65.79	89.16	0.179	78.24
Belgium	96.25	0.149	75.30	96.81	0.178	83.34
Bulgaria	67.38	0.161	12.57	74.56	0.186	31.33
Croatia	92.53	0.071	50.15	87.75	0.093	61.52
Cyprus	88.82	2.349	52.12	98.02	2.773	80.54
Czechia	74.37	0.166	69.66	87.94	0.191	83.57
Denmark	92.60	0.364	94.32	100.00	0.476	97.76
Estonia	99.48	3.130	79.84	95.04	3.972	83.39
Finland	95.78	0.271	92.18	100.00	0.318	94.99
France	97.60	0.120	65.55 ²	98.98	0.155	71.88
Germany	97.41	0.126	64.91	93.84	0.166	66.92
Greece	93.98	0.052	36.55	97.11	0.067	54.15
Hungary	91.28	0.097	51.31	88.73	0.100	66.85
Ireland	85.86	0.606	68.99	90.90	0.710	86.71
Italy	96.13	0.070	39.45	100.00	0.094	55.01
Latvia	97.28	0.503	76.40	82.63	0.693	84.95
Lithuania	97.93	0.819	67.60	92.88	1.026	79.63
Luxembourg	97.41	2.300	70.63	98.72	2.411	76.06
Malta	83.65	1.748	60.32	92.96	1.810	73.90
Netherlands	97.05	0.338	89.41	99.22	0.401	96.35
Poland	93.86	0.088	49.49	93.54	0.105	56.75
Portugal	97.32	0.112	47.06	99.86	0.145	63.49
Romania	76.29	0.061	11.65	91.62	0.078	27.72
Slovakia	92.36	0.066	58.20	94.44	0.088	57.99
Slovenia	74.93	0.124	51.80	96.48	0.132	63.97
Spain	98.52	0.152	62.10	99.74	0.188	74.96
Sweden	93.89	0.407	84.69	99.31	0.462	83.07
Q1 (1st quartile)	88.82	0.097	50.15	90.90	0.105	61.52
Q2 (2nd quartile)	93.89	0.160	64.91	95.04	0.186	74.96
Q3 (3rd quartile)	97.32	0.503	75.30	99.22	0.693	83.39
V (coefficient of variation)	9%	150%	33%	6%	150%	24%
Min (value)	67.38	0.052	11.65	74.56	0.067	27.72
Max (value)	99.48	3.130	94.32	100.00	3.972	97.76
Min (Country)	Bulgaria	Greece	Romania	Bulgaria	Greece	Romania
Max (Country)	Estonia	Estonia	Denmark	Denmark, Finland, Italy	Estonia	Denmark

Source: authors' own elaboration based on data from Eurostat, Crunchbase.com and the ITU (2024).

² No data available for 2020. Data for 2019 (t-1) has been used.

Analysis of data for 2024 indicates further variation in cybersecurity levels and in the development of the FinTech sector across individual EU countries. The values of Spearman's rank correlation coefficient once again confirm the weak strength of the relationship. For the relationship between the Cybersecurity Index and the number of FinTech companies per 500.000 inhabitants, it stood at 0.05, whilst for the relationship between the Cybersecurity Index and the percentage of online banking users, it was 0.18.

In 2024, Estonia was once again the leader in terms of the number of FinTech companies per 500.000 inhabitants (3.972), although it had slipped to 14th place in the cybersecurity ranking (compared to its top ranking in 2020). Similarly, Cyprus (2.773 per 500.000 inhabitants) and Malta (1.810) stood out for their high concentration of FinTech companies, although their cybersecurity levels were also not among the highest in the EU. Romania and Bulgaria once again found themselves at the bottom of the ranking in terms of both cybersecurity levels and FinTech sector development. In the case of Italy, the cybersecurity level reached a maximum score of 100 points in 2024. Nevertheless, the number of FinTech companies per 500.000 inhabitants (0.094) and the percentage of online banking users (55.01%) remained relatively low compared to other EU countries (ranking 23rd and 24th respectively).

In terms of cybersecurity, the median value of the Cybersecurity Index stood at 93.89 points in 2020 and 95.04 points in 2024, indicating that a very high level of digital security has been maintained across the European Union. During the period analysed, the lowest index value was recorded in Bulgaria (67.38 points in 2020 and 74.56 points in 2024), whilst the highest values were achieved by Estonia in 2020 (99.48 points) and by Denmark, Finland and Italy in 2024 (100 points). The indicators of the FinTech sector's development were characterised by significantly greater variation. In the case of the number of FinTech companies per 500.000 inhabitants, the coefficient of variation remained at a very high level, standing at 150% in both 2020 and 2024, which indicates a strong concentration of this market segment in selected countries. The most dynamic changes, however, concerned the use of online banking. The median share of users utilising online banking rose from 64.91% in 2020 to 74.96% in 2024, with the minimum value increasing from 11.65% to 27.72%. This points to the ongoing digitalisation of financial services across the EU and the gradual reduction of digital exclusion in less developed Member States. At the same time, the decline in the coefficient of variation from 33% to 24% indicates a partial convergence in the level of adoption of online financial services between EU countries. The leaders in this regard remain the Nordic countries, primarily Denmark, Finland and the Netherlands, where the proportion of online banking users exceeded 94-97%, whilst the lowest figures were still observed in Romania and Bulgaria, despite a marked improvement compared to 2020. The comparative analysis indicates that the relationship between the level of cybersecurity and the development of the FinTech sector is complex and heterogeneous, and its interpretation should not be reduced to a linear relationship.

A preliminary analysis of the relationship between the level of cybersecurity and the development of the FinTech sector in European Union countries, carried out using Spearman's rank correlation coefficient, did not reveal a significant relationship for the entire sample under study. This result may indicate that the relationship between the analysed variables in 2020 and 2024 was not uniform across all EU countries. Consequently, an additional exploratory analysis was carried out, involving the division of countries into groups according to their level of cybersecurity using quartiles. The following classification was applied:

- Group I – countries with the highest cybersecurity index scores were classified in the group above the third quartile (Q3),
- Group II – countries with moderate index values were classified in the group between the first and third quartiles (Q1–Q3),

- Group III – countries with the lowest index values were classified in the group below the first quartile (Q1).

The aim of this approach was to examine whether correlations between the level of cybersecurity and the development of the FinTech sector exist within countries with similar levels of cybersecurity. For each of the identified groups, linear trend equations and the coefficient of determination R^2 were calculated. The analysis was conducted separately for two measures of the FinTech sector's development: (1) the number of FinTech companies per 500.000 inhabitants – the supply side, and (2) the percentage of people using online banking – the demand side (Table 3).

Table 3. The relationship between cybersecurity levels and the development of the FinTech sector across EU country groups

Year	Group of countries by cybersecurity level	FinTech sector development index	Linear trend equation	R^2 coefficient
2020	Group I	The supply side	$0.9067x - 87.852$	0.3333
2020	Group II		$0.0353x - 3.1263$	0.1967
2020	Group III		$0.0965x - 6.8574$	0.6270
2020	Group I	The demand side	$7.7242x - 691.23$	0.3823
2020	Group II		$3.3544x - 250.17$	0.1029
2020	Group III		$1.8374x - 97.978$	0.3184
2024	Group I	The supply side	$-0.2143x + 21.667$	0.2103
2024	Group II		$0.0971x - 8.2689$	0.0319
2024	Group III		$0.0026x + 0.0867$	0.0028
2024	Group I	The demand side	$-14.499x + 1526.8$	0.0815
2024	Group II		$2.8796x - 207.36$	0.1988
2024	Group III		$2.6403x - 156.49$	0.5698

Source: authors' own elaboration.

An analysis of the relationship between the level of cybersecurity and the development of the FinTech sector across groups of EU countries revealed varying results depending on the year, the group of countries, and the measure of FinTech sector development used. In 2020, a positive relationship was observed across all groups between the level of cybersecurity and the development of the FinTech sector, on both the supply and demand sides. The strongest relationship was recorded in the group of countries with the lowest level of cybersecurity (Group III) for the supply side of the FinTech sector ($R^2 = 0.6270$). However, despite the relatively high coefficient of determination, the relationship did not reach statistical significance at the 5% level. On the demand side, the correlations were weaker but still positive. In 2024, the correlations for the supply side weakened significantly. In Groups II and III, the R^2 values were very low (0.0319 and 0.0028), indicating a virtual absence of a linear relationship between the level of cybersecurity and the number of FinTech firms per 500.000 inhabitants. On the demand side, the strongest relationship was observed in Group III, representing countries with the lowest levels of cybersecurity ($R^2 = 0.5698$). However, despite the relatively moderate explanatory power, this relationship was not statistically significant at the 5% level. The results confirm that the relationship between the level of cybersecurity and the development of the FinTech sector is not uniform across all EU countries and varies depending on both the level of cybersecurity and the measure of FinTech sector development used. However, none of the estimated relationships were statistically significant at the 5% level, with only isolated cases approaching marginal significance. Given the small sample sizes within the individual groups and the use of quartile-based classification, the results may be sensitive to outliers and should not be interpreted in causal terms. The analysis is purely descriptive and serves to identify potential trends.

5. Conclusions

Cybersecurity risk is one of the determinants of the FinTech sector's stability. It stems from potential breaches of the integrity, availability and confidentiality of information. Furthermore, it can lead to financial fraud, extortion, ransomware attacks or data breaches. Due to their digital operating model and the processing of sensitive financial data, companies in the FinTech sector remain particularly vulnerable to cybercrime. The lack of effective monitoring and adequate supervisory mechanisms may result in a decline in customer trust and a reduction in the stability of the financial sector. For this reason, an attempt was made to empirically assess the relationship between the level of cybersecurity and the degree of development of the FinTech sector in EU countries.

The analysis indicates that Member States achieved a relatively high and, at the same time, similar level of cybersecurity, whilst the differences between EU countries continued to narrow. One can therefore speak of a progressive convergence in cybersecurity levels across EU Member States. At the same time, significantly greater variation was identified in the case of indicators describing the development of the FinTech sector, suggesting that the level of cybersecurity alone is not a sufficient factor to explain the scale of development of the financial technology sector in individual EU countries. This means that cybersecurity should be regarded as an essential condition for the stable functioning of the FinTech sector rather than as an independent factor determining its development, which also depends on regulatory, institutional, technological and market conditions. Taking these dimensions into account represents an important direction for further research by the authors. It is also important to highlight the limitations of this study, which relate primarily to the limited availability of up-to-date and fully comparable data on the actual scale of the FinTech sector in individual EU countries. Consequently, conclusions regarding the strength and direction of the relationship between the level of cybersecurity and the development of the FinTech sector should be interpreted with caution. The limited availability of data points to the need for further, in-depth research based on more precise and harmonised indicators, which will enable a more comprehensive assessment of the scale and dynamics of the FinTech sector's development in EU countries.

6. References

- Al_Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Sebai, M., & Harjan, S. A. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence from Iraqi banks. *International Journal of Research in Business and Social Science*, 9(6), 123–133. <https://doi.org/10.20525/ijrbs.v9i6.914>
- Alvarez-Dionisi, L. E. (2020). A Fintech Risk Assessment Model. *ISACA Journal*, 3, 1–6. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2020/volume-3/a-fintech-risk-assessment-model_joa_eng_0620.pdf
- Aron, Z., Cooper, L., Siciliano J., Wadhwani, R. & Futterman, J. (2026). *Accelerating with controls: How fintechs can balance innovation, risk, and compliance for growth*. Financial Services. <https://www.deloitte.com/us/en/insights/industry/financial-services/fintech-risk-and-innovation.html>
- Buła, P., 2015. *System zarządzania ryzykiem w przedsiębiorstwie jako element nadzoru korporacyjnego*, Wydawnictwo Uniwersytetu Jagiellońskiego.
- Crunchbase. (n.d.). *Companies* [Zestaw danych]. <https://www.crunchbase.com/discover/organization/companies>
- Damodaran, A. (2009). *Ryzyko strategiczne: podstawy zarządzania ryzykiem*, tłum. A. Maciejewski, Wydawnictwa Akademickie i Profesjonalne: Akademia Leona Koźmińskiego.

- ENISA. (2025). *ENISA Threat Landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
- Eurostat. (n.d.). *Database* [Zestaw danych]. <https://ec.europa.eu/eurostat/data/database>
- Folwarski, M. (2019). *Sektor FinTech na europejskim rynku usług bankowych Wyzwania konkurencyjne i regulacyjne*. Wydawnictwo poltext.
- Folwarski, M. (2021). *Innowacje cyfrowe w bankowości a wyłączenie cyfrowe i finansowe społeczeństwa*. Wydawnictwo Uniwersytetu Jagiellońskiego.
- Gibowski, Ł. (2025). Assessment of the conditions for the development of the Financial Technology (FinTech) sector in selected countries in 2021. *e-mentor*, 2(109), 59–67. <https://www.doi.org/10.15219/em109.1702>
- Górka, M. (2018). Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa. In T. Dębowski (Ed.), *Cyberbezpieczeństwo wyzwaniem XXI wieku* (pp. 31–50). Wydawnictwo Naukowe ArchaeGraph.
- Greser, J. (2025). Cyberbezpieczeństwo w sektorze bankowym – zarys zagadnienia. In K. Szpyt (Ed.), *FinTech Nowe technologie w sektorze bankowym* (pp. 269–281). Wydawnictwo C.H. BECK.
- Ha, D., Le, P., & Nguyen, D. K. (2025). Financial inclusion and fintech: a state-of-the-art systematic literature review. *Financial Innovation*, 11(69), 1–42. <https://doi.org/10.1186/s40854-024-00741-0>
- Idayani, R. W., Nadlifatin, R., Subriadi, A. P., & Gumasing, M. J. J. (2024). A comprehensive review on how cyber risk will affect the use of fintech. *Procedia Computer Science*, 234, 1356–1363. <https://doi.org/10.1016/j.procs.2024.01.1356>
- ITU. (2020). *Global Cybersecurity Index 2024 4th Edition*. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>
- ITU. (2024). *Global Cybersecurity Index 2024 5th Edition*. <https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx>
- Jain, R., Kumar, S., Sood, K., Grima, S., & Rupeika-Apoga, R. (2023). A Systematic Literature Review of the Risk Landscape in Fintech. *Risks*, 11(36), 1–15. <https://doi.org/10.3390/risks11020036>
- Jagodzińska-Komar, E. (2025). Rozwój usług płatniczych w świetle koncepcji otwartych finansów. *Studia i Prace Kolegium Zarządzania i Finansów*, 206, 41–53. <https://doi.org/10.33119/SIP.2025.206.2>
- Joel, M. O., Chibunna, U. B., & Daraojimba, A. I. (2025). Cybersecurity Challenges in Fintech: A Comprehensive Overview and Risk Analysis. *International Journal of Academic Management Science Research (IJAMSR)*, 9(3), 9–18.
- Jović, Ž., & Nikolić, I. (2022). The Darker Side of Fintech: the Emergence of New Risks. *Zagreb International Review of Economics & Business*, 25, Special Conference Issue, 45–63. <https://doi.org/10.2478/zireb-2022-0024>
- Kamuangu, P. (2024). A Review on Cybersecurity in Fintech: Threats, Solutions, and Future Trends. *Journal of Economics, Finance and Accounting Studies*, 6(1), 47–53. <https://doi.org/10.32996/jefas.2024.6.1.5>
- Karangara, R., & Manta, O. (2024). Cybersecurity & Data Privacy in Fintech. *Preprints*. <https://doi.org/10.20944/preprints202401.2194.v2>
- KNF (2025). *Wzmocnienie cyberbezpieczeństwa polskiego sektora finansowego*. https://www.knf.gov.pl/dla_rynk%C5%9CIRT_KNF/Wzmocnienie_cyberbezpieczenstwa_polskiego_sektora_fi_nansowego
- Kwon, Y., Owens, J., & Lee, D.J. (2023). Managing Fintech Risks: Policy and Regulatory Implications. *ADB Briefs*, 245, 1–12. <http://dx.doi.org/10.22617/BRF230170-2>
- Olaiya, O. P., Adesoga, T. O., Ojo, A., Olagunju, D. O., Ajayi, O., & Adebayo, Y. O. (2024). Cybersecurity strategies in fintech: safeguarding financial data and assets. *GSC Advanced Research and Reviews*, 20(01), 50–56. <https://doi.org/10.30574/gscarr.2024.20.1.0241>

- Państwowy Instytut Badawczy NASK. (2025). *Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*. https://cert.pl/uploads/docs/Raport_CP_2024.pdf
- Polski Instytut Ekonomiczny (2025). *Europa potrzebuje większych inwestycji w cyberbezpieczeństwo*. https://pie.net.pl/wp-content/uploads/2025/03/2025_03_26_Europa-potrzebuje-wiekszych-inwestycji-w-cyberbezpieczenstwo.pdf
- Pawłowska, M. (2023). The Impact of Fintech Enterprises on the Level of Competition in the Financial Sector. Increase or Decrease in Competition? *Journal of Finance and Financial Law*, 2, 27–56. <https://doi.org/10.18778/2391-6478.S2.2023.02>
- Thompsett, L. (2024.07). *Top 10: FinTech Risks*. FinTech MAGAZINE. <https://fintechmagazine.com/articles/top-10-fintech-risks>
- Woźniak, J., & Wereda, W. (2023). Wprowadzenie. In W. Woźniak & W. Wereda (Ed.), *Mapa ryzyka w zarządzaniu organizacją*, CeDeWu.
- Zhao, B. (2025). FinTech and Risk Management: Exploring Opportunities, Challenges, and Regulatory Responses, *SHS Web Conf.*, 225, 02024 (2025) ICFMDE 2025, 1–9. <https://doi.org/10.1051/shsconf/202522502024>