

CYBERSECURITY AND DATA PRIVACY IN FINANCIAL TECHNOLOGY: EMERGING THREATS AND STRATEGIC SOLUTIONS

O. S. ALADEJUBELO,

Ph.D. Pan-Africa Entrepreneur & Vocational College of Education, shinasamuel@gmail.com

R. O. RAJI,

Ph.D, Crescent University, Abeokuta, Ogun State, Nigeria, rajialade@yahoo.com

S. A. ISHOLA,

*(CA), Ph.D, Pan-Africa Entrepreneur & Vocational College of Education,
demolaishola72@gmail.com*

S. O. BAMISAYE,

Ph.D, Pan-Africa Entrepreneur & Vocational College of Education, samuel_bamisaye@yahoo.com

Abstract

Financial Technology (FinTech) has changed the way financial services are provided through technologies such as digital payments, mobile banking, blockchain, Artificial Intelligence, and cloud computing. These technologies have made financial services easier to access and improved the way organizations operate and serve their customers. However, they have also increased cybersecurity risks and concerns about the protection of personal data. This study examined the cybersecurity threats faced by FinTech organizations and looked at ways to improve data privacy and cybersecurity. A descriptive survey design was used for the study. Data were collected from 303 employees of selected FinTech companies in Lagos State, Nigeria, using a structured questionnaire. Out of the questionnaires distributed, 290 were properly completed and used for the analysis. The data were analyzed using SPSS Version 29. Descriptive statistics, Pearson correlation, and multiple regression were used to test the hypotheses. The findings showed that cybersecurity threats have a significant effect on the performance of FinTech companies, while good data privacy practices help to improve customer trust and organizational performance. The study also found that measures such as multi-factor authentication, data encryption, Artificial Intelligence, Zero Trust Architecture, and cybersecurity awareness programmes can help FinTech companies improve their protection against cyber threats. The study concludes that strong cybersecurity practices and compliance with data protection laws are important for providing safe, reliable, and customer-friendly digital financial services.

Keywords: *Cybersecurity, Data Privacy, Financial Technology (FinTech), Digital Payments.*

DOI: 10.31039/bjir.v3i13.152

1. INTRODUCTION

The rapid growth of Information and Communication Technology (ICT) has greatly changed the financial industry around the world. This growth has led to the development of Financial Technology (FinTech), which is one of the major technological developments of the 21st century. FinTech means using digital technology to provide financial products and services in a faster, easier, and more convenient way. Technologies such as mobile banking, digital payment systems, online lending, blockchain, cloud computing, Artificial Intelligence (AI), and cryptocurrencies have changed the way people and businesses access, manage, and transfer money. These technologies have helped to improve financial inclusion, reduce transaction costs, make financial services faster, and support economic growth, especially in developing countries like Nigeria. As the use of digital financial services continues to grow, FinTech has become an important part of economic development. It encourages innovation and makes it easier for individuals and businesses to access formal financial services.

Despite these achievements, the growing use of digital financial platforms has also increased cybersecurity risks and concerns about data privacy. FinTech companies collect and store a large amount of sensitive customer information, such as personal details, transaction records, banking information, biometric data, and financial records. This makes them attractive targets for cybercriminals. As a result, cyber threats such as phishing, ransomware, malware, identity theft, DDoS attacks, insider threats, and weaknesses in application programming interfaces (APIs) are becoming more common and advanced. These threats can lead to the loss or misuse of financial information, financial losses, disruption of business activities, damage to the reputation of companies, and loss of customer trust. As digital financial services continue to grow, it is becoming more important for FinTech companies to put strong cybersecurity measures in place to protect customer information and ensure that financial services remain safe and reliable.

Furthermore, the increasing use of new technologies such as cloud computing, Artificial Intelligence, the Internet of Things (IoT), blockchain, and open banking has improved the activities of FinTech companies but has also made cybersecurity more difficult to manage. These technologies help organizations work better, improve customer experience, and provide new financial services. However, they can also create new weaknesses that cybercriminals can take advantage of, for example, cybercriminals now use Artificial Intelligence to carry out phishing attacks, create harmful software, and produce fake videos or audio, known as deepfakes, to deceive financial institutions and customers. FinTech companies also collect and use large amounts of customer information for

activities such as fraud detection, credit assessment, following regulations, and providing personalized financial services. If customer data is not properly protected through good data management, encryption, and access controls, people may become victims of identity theft, financial fraud, unauthorized sharing of information, and other privacy problems.

To address these challenges, governments and regulatory bodies around the world have introduced data protection and cybersecurity laws to protect digital financial services. Examples include the European Union's General Data Protection Regulation (GDPR) and the Nigeria Data Protection Act (NDPA) 2023. These laws provide guidelines for how personal information should be collected, used, stored, and protected. However, simply following these laws is not enough. FinTech companies also need to take cybersecurity seriously by training their workers, regularly monitoring their systems, using multi-factor authentication, encrypting important information, and applying strong security systems such as Zero Trust. As FinTech continues to change the financial sector, cybersecurity and data privacy should be treated as important responsibilities of the whole organization and not only as technical issues. Based on this, the study examines the cybersecurity threats facing the FinTech sector and looks at ways to improve data privacy, strengthen cybersecurity, and support the long-term growth of digital financial services.

The rapid growth of Financial Technology has changed the way financial services are provided by making them more accessible, faster, easier, and more convenient. However, this digital growth has also exposed financial institutions and their customers to serious cybersecurity threats and data privacy risks. Cyberattacks such as ransomware, phishing, malware, identity theft, insider threats, API attacks, and unauthorized access to data are becoming more common. These attacks can lead to financial losses, punishment from regulators, disruption of business activities, and loss of public trust in digital financial services.

Many FinTech companies, especially in developing countries like Nigeria, still face difficulties in building strong cybersecurity systems. These difficulties are caused by changing cyber threats, limited funds, lack of cybersecurity awareness among employees and customers, and challenges in keeping up with changing regulations. The large amount of customer information collected, stored, and processed by FinTech companies has also increased concerns about unauthorized access, misuse of personal information, and failure to follow data privacy laws. These problems can affect customer trust, the reputation of organizations, normal business operations, and the long-term survival of digital financial services. Although previous studies have looked at FinTech innovation, cybersecurity, and digital financial inclusion, only a few have examined cybersecurity threats, data privacy, and possible cybersecurity solutions together within the growing FinTech industry. This

study therefore aims to fill this gap by examining the cybersecurity threats facing FinTech organizations and identifying ways to improve cybersecurity, protect customer information, and support safe and sustainable financial innovation.

The main objective of this study is to examine cybersecurity and data privacy in Financial Technology, focusing on the new threats and possible solutions.

The specific objectives are to:

Examine the major cybersecurity threats affecting Financial Technology platforms.

Assess the data privacy challenges confronting FinTech organizations.

Evaluate the impact of cybersecurity threats on customer trust and organizational performance.

Identify strategic cybersecurity measures for mitigating cyber risks in the FinTech sector.

Recommend policy and technological solutions for improving data privacy and cybersecurity resilience.

Based on the above objectives, the study response to the following research questions:

What are the major cybersecurity threats affecting Financial Technology platforms?

What data privacy challenges confront FinTech organizations?

How do cybersecurity threats influence customer trust and organizational performance?

What strategic cybersecurity measures can effectively mitigate cyber risks in the FinTech industry?

What policy and technological interventions can strengthen data privacy and cybersecurity resilience?

The following null hypotheses were deduced from above research questions to the study:

H₀₁: Cybersecurity threats have no significant effect on the operational performance of Financial Technology firms.

H₀₂: Data privacy practices have no significant relationship with customer trust in Financial Technology services.

H₀₃: Strategic cybersecurity measures have no significant influence on cybersecurity resilience in Financial Technology organizations.

This study will be useful to FinTech companies, regulatory bodies, commercial banks, policymakers, cybersecurity experts, investors, researchers, and customers. It will provide useful information about new cyber threats and ways to improve cybersecurity and protect customer information. The findings will also help regulators to develop better policies that can make digital financial services safer, increase customer trust, and support the growth of the FinTech industry. The study focuses on cybersecurity and data privacy in the Financial Technology sector, with attention to new cyber threats, challenges in protecting data, and possible cybersecurity solutions. It covers major FinTech services such as mobile banking, digital payments, online lending, blockchain, and other digital financial platforms. The study also looks at cybersecurity guidelines, relevant regulations, and good practices that can help improve security in the FinTech sector.

2. LITERATURE REVIEW

Conceptual Review

Financial Technology (FinTech) means using modern digital technology to provide financial services in a faster, easier, and more convenient way. It includes services such as mobile banking, online payments, blockchain, cloud computing, Artificial Intelligence (AI), cryptocurrencies, online lending, and digital insurance. FinTech has changed the way people and businesses use financial services. It helps to reduce transaction costs, make financial services available to more people, and provide different ways for people and businesses to manage their money. FinTech has changed traditional banking around the globe by providing financial services that are easier and more focused on customers. In developing countries like Nigeria, FinTech has helped many people who did not have access to banks to use financial services through mobile money, agent banking, and digital payment platforms. This has helped more people take part in economic activities, start businesses, and gain access to financial services.

Despite these benefits, the growing use of digital financial services has also created more opportunities for cybercriminals to attack. FinTech companies depend heavily on digital systems, which makes them more exposed to cyberattacks. These attacks can affect business activities, reduce customer trust, and make it difficult for companies to follow financial regulations. Cybersecurity means the use of technologies, rules, procedures, and practices to protect computer systems, networks, software, databases, and electronic information from unauthorized access, cyberattacks,

theft, or damage. The main aim of cybersecurity is to keep information private, accurate, and available when needed, while also protecting organizations from cyber threats.

Cybersecurity has become progressively vital within the FinTech sector due to the fast growth of online financial transactions and the rising complexity of cybercriminal activities. Effective cybersecurity requires the implementation of various layers of protection, including encryption, firewalls, endpoint security, intrusion detection systems, identity and access management, security awareness training, and continuous monitoring.

A strong cybersecurity plan combines good management, technology, risk control, and proper staff awareness to reduce weaknesses and help organizations respond better to changing cyber threats. Data privacy means properly collecting, using, storing, sharing, and deleting people's personal information while making sure they have control over how their information is used. In FinTech, companies collect sensitive information from customers, such as names, addresses, fingerprints or other biometric details, transaction records, credit information, and financial records. Data privacy is based on important principles such as being clear about how information is used, getting people's permission, collecting only the information needed, keeping information confidential, and protecting it from unauthorized access. These principles are included in important data protection laws such as the European Union's General Data Protection Regulation (GDPR), the Nigeria Data Protection Act (NDPA) 2023, and other data protection laws in different countries. Good data privacy practices help to build customer trust, make it easier for organizations to follow regulations, and reduce the risk of financial fraud, identity theft, and damage to the company's reputation.

Many studies have looked at cybersecurity and data privacy in the FinTech industry.

Ahmed and Rahman (2023) studied cybersecurity problems in digital financial services. They found that phishing attacks, ransomware, and threats from insiders can affect the performance of organizations and reduce customer trust. They recommended regular cybersecurity awareness training and the use of advanced technologies to detect cyber threats. Zhang, Wang, and Li (2024) studied how Artificial Intelligence can be used to detect fraud in FinTech companies. Their study found that AI-based fraud detection systems can reduce fraudulent transactions and improve the way organizations operate. However, they also stated that AI systems need to be regularly updated and trained to deal with new and changing cyber threats.

Kshetri (2023) studied cybersecurity management in FinTech companies and found that the involvement of top management, proper risk management, and following regulations can help

organizations become stronger against cyber threats. The study also stressed that cybersecurity should be part of the main business plan and not treated as only a technical issue.

Zhou and Xu (2023) examined the use of blockchain technology in financial security. They found that blockchain can make transactions safer, more transparent, and difficult to change or manipulate. However, the study also pointed out that weaknesses in smart contracts and problems with handling large numbers of transactions still need more attention.

In Nigeria, recent studies have shown that as more people use digital payment services, cases of cyber fraud, identity theft, and unauthorized access to financial information have also increased. This shows the need for stronger cybersecurity management, better protection of customer information, and closer cooperation between regulators, FinTech companies, and cybersecurity experts.

Although previous studies have looked at cybersecurity, FinTech, Artificial Intelligence, blockchain, and digital payment systems separately, only a few studies have looked at cyber threats, data privacy problems, and possible cybersecurity solutions together, especially in developing countries. Also, many existing studies focus more on technology and give less attention to issues such as proper management, following regulations, employee awareness, and customer trust.

This study aims to address these gaps by examining cybersecurity and data privacy in the FinTech industry. It focuses on the major cyber threats facing FinTech companies and the possible solutions that can improve cybersecurity, protect customer information, and support the safe and continuous growth of digital financial services.

3. METHODOLOGY

This study used a descriptive survey research design. The design was suitable because it helped the researcher to collect information from respondents about cybersecurity threats, data privacy practices, and the solutions used by FinTech organizations. It also made it possible to collect numerical information from a sample of respondents and use it for statistical analysis and to draw conclusions about the larger population.

The study used a cross-sectional approach, meaning that the data were collected from the respondents at one particular time using a structured questionnaire.

The study was carried out among selected Financial Technology (FinTech) companies in Lagos State, Nigeria. Lagos is known as one of the major financial and technology centers in the country and has many FinTech companies, commercial banks, payment companies, digital lending firms, and other financial technology organizations. For this reason, Lagos was considered suitable for studying cybersecurity and data privacy issues in the FinTech industry. The population of the study consisted of employees working in selected FinTech companies in Lagos State. The respondents included IT staff, cybersecurity professionals, data protection officers, operations managers, compliance officers, customer service staff, and risk management officers.

For this study, the accessible population was 1,250 employees from selected licensed FinTech companies operating in Lagos State.

The sample size for the study was determined using Yamane's (1967) formula, as shown below:

$$n = N / [1 + N(e^2)]$$

Where:

n = Sample size

N = Population size (1,250)

e = Level of precision (5% or 0.05)

Substituting the values:

$$\begin{aligned} n &= 1,250 / [1 + 1,250(0.05^2)] \\ n &= 1,250 / 4.125 = 303 \end{aligned}$$

Therefore, the study used a sample size of 303 respondents.

A stratified random sampling method was used to make sure that the different groups of employees in the selected FinTech companies were properly represented. The employees were first divided into groups based on their job roles, and then respondents were randomly selected from each group. This method helped to reduce bias and made the sample more representative of the study population.

The study used both primary and secondary sources of data.

Primary Data

Primary data were collected by giving structured questionnaires to employees of selected FinTech companies. The questionnaire asked about their views on cybersecurity threats, data privacy practices, and possible solutions for improving cybersecurity.

Secondary Data

Secondary data were obtained from academic journals, books, conference proceedings, government publications, CBN reports, NDPC publications, NIST reports, ISO publications, World Economic Forum reports, and relevant online databases.

The main instrument used to collect data was a structured questionnaire prepared by the researcher after reviewing relevant literature.

The questionnaire was divided into two sections:

Section A: This section collected basic information about the respondents, such as their gender, age, educational qualification, years of work experience, and job position.

Section B: The questionnaire contained statements used to measure the variables of the study. The respondents were asked to indicate their level of agreement using a five-point Likert Scale as follows:

Strongly Agree (SA) = 5
Agree (A) = 4
Undecided (U) = 3
Disagree (D) = 2
Strongly Disagree (SD) = 1

The questionnaire questions covered the following areas:

Cybersecurity threats

Data privacy practices

Strategic cybersecurity measures

Organizational performance

Customer trust

The questionnaire was checked for face and content validity to make sure it properly measured the areas covered in the study. Experts in cybersecurity, FinTech, research methodology, and measurement and evaluation reviewed the questionnaire. Their comments and suggestions were used to make the questions clearer, more relevant, and complete before the final questionnaire was used.

The reliability of the questionnaire was tested using Cronbach's Alpha after a pilot study was carried out with 30 respondents from FinTech organizations that were not part of the main study.

The reliability results obtained were as follows:

Variable	Number of Items	Cronbach's Alpha
Cybersecurity Threats	8	0.872
Data Privacy Practices	7	0.853
Strategic Cybersecurity Solutions	8	0.889
Organizational Performance	5	0.846
Customer Trust	5	0.861
Overall Reliability	33	0.864

The overall Cronbach's Alpha value of 0.864 shows that the questionnaire is reliable and consistent, making it suitable for collecting data for the study.

The questionnaires were given to respondents both physically and electronically in the selected FinTech organizations. The respondents were given enough time to complete them. After completion, the questionnaires were collected and prepared for coding, editing, and statistical analysis. The privacy of the respondents was protected, and their names and personal information were kept confidential to encourage them to give honest answers.

The study used multiple linear regression to examine the relationship between cybersecurity threats, data privacy practices, and strategic cybersecurity solutions.

The functional model is expressed as:

$$OP = f(CST, DPP, SCS)$$

The econometric model used for the study is presented as follows:

$$OP = \beta_0 + \beta_1 CST + \beta_2 DPP + \beta_3 SCS + \mu$$

Where:

OP = Organizational Performance (Dependent Variable)

CST = Cybersecurity Threats

DPP = Data Privacy Practices

SCS = Strategic Cybersecurity Solutions

β_0 = Constant

$\beta_1 - \beta_3$ = Regression coefficients

μ = Error term

Expected Signs:

$\beta_1 < 0$ (Cybersecurity threats are expected to negatively affect organizational performance.)

$\beta_2 > 0$ (Effective data privacy practices are expected to improve organizational performance.)

$\beta_3 > 0$ (Strategic cybersecurity solutions are expected to positively influence organizational performance.)

The data collected were coded and analyzed using the Statistical Package for Social Sciences (SPSS) Version 29.

The study used the following statistical methods to analyze the data: frequency distribution, percentages, mean, standard deviation, Cronbach's Alpha reliability test, Pearson Product Moment Correlation, multiple regression analysis, Analysis of Variance (ANOVA), and t-test for regression coefficients.

The hypotheses were tested at a 5% level of significance ($\alpha = 0.05$). The decision was based on the p-value as follows:

Reject the null hypothesis if $p < 0.05$.

Fail to reject the null hypothesis if $p \geq 0.05$.

4. RESULTS, DISCUSSION AND ANALYSIS

This chapter explains the results of the data collected for the study titled "Cybersecurity and Data Privacy in Financial Technology: Emerging Threats and Strategic Solutions." The information was collected from employees of selected FinTech companies in Lagos State, Nigeria. The data were analyzed using SPSS Version 29. Different statistical methods were used to understand the responses, examine the relationships between the variables, and test the hypotheses. The results are presented in tables and explained clearly based on the findings of the study and related previous research.

Questionnaire Distribution and Response Rate

A total of 303 questionnaires were given to respondents in selected FinTech companies. Out of the 303 questionnaires, 290 were properly completed and returned, while 13 were either not returned or were not properly completed.

Table 4.1 Questionnaire Distribution and Response Rate

Questionnaire Status	Frequency	Percentage (%)
Administered	303	100.0
Returned	290	95.7
Not Returned	13	4.3
Questionnaire Status	Frequency	Percentage (%)
Total	303	100.0

The response rate of 95.7% is high enough for the data to be properly analyzed. This also gives the researcher enough information to make reliable conclusions from the study.

Demographic Characteristics of Respondents

Table 4.2 Gender Distribution

Gender	Frequency	Percentage (%)
Male	172	59.3
Female	118	40.7
Total	290	100.0

The results show that 59.3% of the respondents were male, while 40.7% were female, as shown in the table below.

4.3 Age Distribution

Age (Years)	Frequency	Percentage (%)
Below 30	74	25.5
31–40	132	45.5
41–50	61	21.0
Above 50	23	8.0
Total	290	100.0

The results show that most of the respondents (45.5%) were between 31 and 40 years old. This means that many of the participants were within the active working age group.

Table 4.4 Educational Qualification

Qualification	Frequency	Percentage (%)
HND/B.Sc.	136	46.9
Master's Degree	114	39.3
Ph.D.	18	6.2
Professional Qualification	22	7.6
Total	290	100.0

The findings show that most of the respondents had good educational backgrounds and were able to provide useful and reliable information for the study.

Reliability Test (Cronbach's Alpha)

Table 4.5 Reliability Statistics

Variable	Number of Items	Cronbach's Alpha
Cybersecurity Threats	8	0.872
Data Privacy Practices	7	0.853
Strategic Cybersecurity Solutions	8	0.889
Organizational Performance	5	0.846
Customer Trust	5	0.861
Overall Reliability	33	0.864

The overall Cronbach's Alpha value of 0.864 is higher than the recommended value of 0.70. This shows that the questionnaire was consistent and reliable for the study.

Descriptive Analysis

Table 4.6 Descriptive Statistics of Study Variables

Variable	Mean	Std. Deviation	Decision
Cybersecurity Threats	4.32	0.63	High
Data Privacy Practices	4.18	0.58	High
Strategic Cybersecurity Solutions	4.41	0.55	High
Customer Trust	4.06	0.69	High
Organizational Performance	4.23	0.61	High

The results show that the mean scores were generally high, with most of them above 4.00. This means that the respondents generally agreed that cybersecurity threats have a major effect on FinTech operations. They also agreed that good data privacy practices and effective cybersecurity measures can improve the performance of organizations and increase customer trust.

Correlation Analysis

Table 4.7 Pearson Correlation Matrix

Variables	CST	DPP	SCS	OP
Cybersecurity Threats (CST)	1.000			
Data Privacy Practices (DPP)	0.521**	1.000		
Strategic Cybersecurity Solutions (SCS)	0.612**	0.584**	1.000	
Organizational Performance (OP)	-0.483**	0.668**	0.742**	1.000

Correlation is significant at the 0.01 level (2-tailed).

The results show that cybersecurity threats have a moderate negative relationship with organizational performance ($r = -0.483$). This means that as cybersecurity threats increase, organizational performance tends to decrease. On the other hand, data privacy practices ($r = 0.668$) and strategic cybersecurity solutions ($r = 0.742$) have strong positive relationships with organizational performance. This means that better data privacy practices and effective cybersecurity solutions are associated with better organizational performance.

Multiple Regression Analysis

Table 4.8 Model Summary

Statistic	Value
R	0.816
R Square	0.666
Adjusted R Square	0.661
Std. Error	0.447

The regression model explains 66.6% of the changes in organizational performance. This means that cybersecurity threats, data privacy practices, and strategic cybersecurity solutions together have a significant effect on the performance of FinTech organizations.

Table 4.9: ANOVA

Source	Sum of Squares	df	Mean Square	F	Sig.
Regression	82.714	3	27.571	138.41	0.000
Residual	41.231	286	0.144		
Total	123.945	289			

The ANOVA results show that the regression model is statistically significant ($F = 138.41$, $p < 0.001$). This means that cybersecurity threats, data privacy practices, and strategic cybersecurity solutions, when considered together, have a significant effect on the performance of FinTech organizations.

Table 4.10 Regression Coefficients

Variable	Beta	t-value	Sig.	Decision
Constant	1.284	4.713	0.000	Significant
Cybersecurity Threats	-0.298	-6.742	0.000	Significant
Data Privacy Practices	0.341	7.865	0.000	Significant
Strategic Cybersecurity Solutions	0.452	9.312	0.000	Significant

The regression results show that cybersecurity threats have a significant negative effect on organizational performance. This means that higher cybersecurity threats can reduce the performance

of FinTech organizations. On the other hand, good data privacy practices and effective cybersecurity solutions have significant positive effects on organizational performance.

Test of Hypotheses

Hypothesis One

H₀₁: Cybersecurity threats have a significant effect on the operational performance of Financial Technology (FinTech) firms.

Since $\beta = -0.298$, $t = -6.742$, and $p = 0.000$, which is less than 0.05, the null hypothesis is rejected. This means that cybersecurity threats significantly reduce the operational performance of FinTech firms.

Hypothesis Two

H₀₂: How a fintech company handles customers' personal data does not have a significant effect on how much customers trust its services.

The results show that good data privacy practices help increase customers' trust in FinTech services. Since the statistical results are strong ($\beta = 0.341$, $t = 7.865$, $p < 0.05$), the finding is unlikely to be due to chance. This means the original assumption that data privacy has no effect on customer trust is rejected.

Hypothesis Three

H₀₃: Strategic cybersecurity measures do not have a meaningful impact on how well Financial Technology (FinTech) organizations can withstand and recover from cyber threats.

With $\beta = 0.452$, $t = 9.312$, and $p = 0.000$ (< 0.05), the null hypothesis is rejected. Strategic cybersecurity measures significantly improve cybersecurity resilience and organizational performance within FinTech firms.

Discussion of Findings

The study shows that cybersecurity threats are a major challenge facing Financial Technology organizations. Respondents identified issues such as phishing attacks, ransomware, malware, insider threats, identity theft, and API weaknesses as serious risks that can affect digital financial services. The results also show that frequent cyberattacks can reduce organizational performance by causing financial losses, service interruptions, damage to reputation, and loss of customer trust. These

findings agree with recent studies that highlight the increasing complexity of cyber threats targeting digital financial platforms.

The study shows that good data privacy practices help increase customer trust in FinTech services. Respondents indicated that protecting personal and financial information, following data protection rules, having clear privacy policies, and controlling access to data make customers feel more confident. This suggests that proper data management is not only important for meeting legal requirements but also helps organizations keep customers and achieve long-term success.

The study shows that strong cybersecurity measures, such as multi-factor authentication, data encryption, Zero Trust security, AI-based threat detection, employee security training, and regular monitoring, improve an organization's ability to handle cyber threats. Organizations that invest in effective cybersecurity systems are better able to prevent attacks, identify risks, respond quickly, and maintain reliable services.

Overall, the findings show that cybersecurity and protecting people's data should be a major part of how organizations plan and operate, not just a job for the IT department. Companies need to keep improving their security systems, train employees on safe practices, follow data protection rules, and create strong security policies. These efforts will help build customer trust and support the continued growth and success of the FinTech industry.

5. CONCLUSION AND RECOMMENDATIONS

Conclusion

Based on this study, it is clear that cybersecurity and data privacy are now essential parts of today's Financial Technology (FinTech) environment. While FinTech innovations have greatly improved the way financial services are provided by making them easier to access, faster, and available to more people, they have also exposed organizations to more advanced cyber threats. As cyberattacks become more frequent and complex, organizations need to take proactive steps and use effective technology-based security measures to protect their systems and customers' data.

The study concludes that cybersecurity threats are a major challenge that can negatively affect organizations by reducing their performance, interrupting business activities, weakening customer trust, and causing serious financial and reputational damage. Similarly, poor data privacy practices can lead to legal penalties, identity theft, financial fraud, and a loss of public confidence.

On the other hand, organizations that adopt strong cybersecurity measures, such as data encryption, multi-factor authentication, artificial intelligence-based threat detection, Zero Trust security systems, effective cybersecurity policies, regular security checks, and employee training, are better able to prevent cyberattacks, protect customers' sensitive information, meet regulatory requirements, and maintain a competitive position. Therefore, cybersecurity should not be seen as only an IT responsibility but as an important part of an organization's overall strategy that helps support digital growth and long-term business success.

Recommendations

Based on the results and conclusions of this study, the following recommendations are suggested:

Strengthen Cybersecurity Governance: FinTech organizations should develop strong cybersecurity governance frameworks with active involvement from senior management and boards of directors. This will ensure that cybersecurity is included as an important part of the organization's overall strategy and decision-making process.

Adopt Advanced Security Technologies: Financial institutions should use modern cybersecurity tools such as Artificial Intelligence (AI), Machine Learning (ML), Security Information and Event Management (SIEM) systems, blockchain security solutions, and Zero Trust Architecture to improve the ability to identify and respond to cyber threats.

Improve Data Privacy Compliance: FinTech organizations should ensure full compliance with data protection regulations, including the Nigeria Data Protection Act (NDPA), the General Data Protection Regulation (GDPR), and other relevant standards, to protect customers' personal information and avoid legal consequences.

Use Multi-Factor Authentication and Encryption: Organizations should apply strong encryption methods and require multi-factor authentication for users to reduce the risk of unauthorized access to financial platforms and sensitive information.

Provide Regular Cybersecurity Awareness Training: Organizations should organize continuous training programmes for employees and customers to increase awareness of cyber risks such as phishing, social engineering, weak passwords, identity theft, and other online threats.

Improve Third-Party Risk Management: FinTech companies should regularly assess the security practices of third-party vendors, cloud service providers, and business partners to reduce risks associated with external services and supply chains.

Maintain Continuous Monitoring and Incident Response: Organizations should invest in real-time security monitoring, regular vulnerability assessments, penetration testing, and effective incident response teams to quickly identify, manage, and recover from cyber incidents.

Encourage Industry Collaboration: Regulatory bodies, financial institutions, cybersecurity experts, and technology providers should work together by sharing threat information, security practices, and new innovations to strengthen cybersecurity across the financial sector.

Increase Cybersecurity Research and Innovation: Governments and private organizations should provide more funding for cybersecurity research, local security solutions, and skills development to better address emerging cyber threats.

Develop Customer Cybersecurity Education Programmes: FinTech providers should continuously educate customers on safe digital practices, privacy protection, fraud prevention, and secure online transactions to reduce security risks caused by human errors.

Contribution to Knowledge

This study adds to existing knowledge on cybersecurity and data privacy by examining the emerging cyber threats affecting the Financial Technology sector and identifying effective strategies for improving organizations' ability to withstand these threats. Unlike many earlier studies that focused mainly on the technical side of cybersecurity, this research considers a broader view by combining technological, organizational, and regulatory factors into one comprehensive framework.

Furthermore, this study provides evidence on how cybersecurity threats, data privacy practices, cybersecurity strategies, customer trust, and organizational performance are connected within the Nigerian FinTech sector. The findings offer useful information for policymakers, regulators, financial institutions, cybersecurity professionals, and researchers who aim to improve digital financial security and increase customer confidence in financial technology services.

Limitations of the Study

Although the study successfully achieved its objectives, some limitations should be considered:

The study was limited to selected FinTech companies operating in Lagos State, which may restrict the generalizability of the findings to other regions or countries.

Data were collected using self-administered questionnaires, therefore, responses may have been influenced by respondents' perceptions and personal experiences.

The cross-sectional research design captured respondents' opinions at a single point in time and may not fully reflect changes in cybersecurity threats and organizational practices over time.

Resource and time constraints limited the scope of the study and the number of organizations included in the survey.

Despite these limitations the study provides credible and useful findings that contribute significantly to understanding cybersecurity and data privacy issues within the FinTech sector.

Suggestions for Further Studies

Future researchers are encouraged to extend this study in the following areas:

Exercise comparative studies on cybersecurity practices among FinTech industry across different geopolitical zones or countries.

Examine the effectiveness of Artificial Intelligence and Machine Learning in preventing cyber fraud in digital financial services.

Make research about the influence of blockchain technology on cybersecurity adaptability and data privacy protection in financial institutions.

Assess customer awareness and behavioral responses to cybersecurity threats in digital banking and mobile payment systems.

Explore the impact of regulatory frameworks on cybersecurity compliance and operational performance among FinTech organizations.

Undertake longitudinal studies to examine how emerging cyber threats evolve over time and how organizations adapt their cybersecurity strategies.

Investigate cybersecurity risk management practices among Small and Medium-sized Enterprise (SME) FinTech firms compared with large financial institutions.

REFERENCES

- Ahmed, M., & Rahman, M. (2023). Cybersecurity challenges in digital financial services: Risks, resilience, and regulatory implications. *Journal of Financial Innovation*, 9(2), 85–102.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2020). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*, 37(3), 371–413.
- Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements.
- Central Bank of Nigeria. (2022). Risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers.
- Central Bank of Nigeria. (2023). Guidelines on operations of payment service providers in Nigeria.
- Chandramouli, R., & Butcher, Z. (2025). Guidelines for API protection for cloudnative systems (NIST Special Publication 800-228). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-228>
- Chandramouli, R., & Butcher, Z. (2026). Guidelines for API protection for cloudnative systems, March 2026 update (NIST Special Publication 800-228 Update
- National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-228-upd1>
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).
- International Organization for Standardization. (2020). ISO/IEC TS 27100:2020 Information technology, Cybersecurity, Overview and concepts.

- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Information security management systems, Requirements.
- International Organization for Standardization. (2026). ISO/IEC 27000:2026 Information security, cybersecurity and privacy protection, Information security management systems, Overview.
- Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. arXiv. <https://doi.org/10.48550/arXiv.2312.01752>
- Kshetri, N. (2023). Cybersecurity management in FinTech: Challenges and opportunities. *Telecommunications Policy*, 47(5), 102581.
- National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF)
- National Institute of Standards and Technology. (2024). Protecting controlled unclassified information in nonfederal systems and organizations (NIST Special Publication 800-171 Rev. 3).
- Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act, 2023.
- Organisation for Economic Co-operation and Development. (2023). Digital security risk management for the financial sector.
- PwC. (2024). Global Digital Trust Insights 2024.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114.
- Statista. (2024). Cybercrime and data breach statistics in the financial services industry.
- World Economic Forum. (2025). Global Cybersecurity Outlook 2025.
- Zhang, Y., Wang, H., & Li, X. (2024). Artificial intelligence-driven fraud detection in financial technology: Evidence from digital financial platforms. *Journal of Financial Crime*, 31(2), 411–430.
- Zhou, W., & Xu, L. (2023). Blockchain security and privacy in financial services: Challenges and future directions. *Future Generation Computer Systems*, 145, 52– 67.

Appendix

QUESTIONNAIRE

Title: Cybersecurity and Data Privacy in Financial Technology: Emerging Threats and Strategic Solutions

Dear Respondent,

This questionnaire is made to collect information for academic research on cybersecurity and data privacy in the Financial Technology (FinTech) sector. All information provided will be kept confidential and used strictly for research purposes only. Please select the option that best reflects your opinion.

Response Scale

Strongly Agree (SA) = 5

Agree (A) = 4

Undecided (U) = 3

Disagree (D) = 2

Strongly Disagree (SD) = 1

SECTION A: DEMOGRAPHIC INFORMATION

Please tick (✓) the appropriate option.

Gender

☐ Male

☐ Female

Age

☐ Below 30 years

☐ 31–40 years

☐ 41–50 years

☐ Above 50 years

Highest Educational Qualification

☐ HND/B.Sc.

☐ Master's Degree

☐ Ph.D.

☐ Professional Qualification

☐ Others (Specify): _____

Current Job Position

☐ IT Personnel

- ☐ Cybersecurity Officer
☐ Compliance Officer
☐ Operations Manager
☐ Customer Service Officer
☐ Data Protection Officer
☐ Risk Management Officer
☐ Others _____

Years of Working Experience

- ☐ Less than 5 years
☐ 5–10 years
☐ 11–15 years
☐ Above 15 years

Type of FinTech Service

- ☐ Digital Payments
☐ Mobile Banking
☐ Digital Lending
☐ Blockchain/Crypto
☐ Others _____

SECTION B: RESEARCH VARIABLES

Cybersecurity Threats (CST)

S/N	Statement	SA	A	U	D	SD
1	Phishing attacks are common in my organization.	☐	☐	☐	☐	☐
2	Malware attacks pose significant risks to FinTech operations.	☐	☐	☐	☐	☐
3	Ransomware attacks negatively affect organizational productivity.	☐	☐	☐	☐	☐
4	Insider threats constitute a major cybersecurity challenge.	☐	☐	☐	☐	☐
5	API vulnerabilities expose FinTech platforms to cyberattacks.	☐	☐	☐	☐	☐
6	Identity theft has increased with digital financial transactions.	☐	☐	☐	☐	☐
7	Cybersecurity threats disrupt business continuity.	☐	☐	☐	☐	☐
8	Cyberattacks negatively affect customer confidence in FinTech services.	☐	☐	☐	☐	☐

Data Privacy Practices (DPP)

S/N	Statement	SA	A	U	D	SD
9	My organization complies with the Nigeria Data Protection Act (NDPA).	☐	☐	☐	☐	☐
10	Customer information is adequately protected from unauthorized access.	☐	☐	☐	☐	☐
11	Strong encryption is used to secure customer data.	☐	☐	☐	☐	☐
12	Employees understand data privacy policies.	☐	☐	☐	☐	☐
13	Customers are informed about how their personal data are used.	☐	☐	☐	☐	☐
14	Access to customer information is restricted to authorized personnel.	☐	☐	☐	☐	☐
15	Data privacy practices improve customer confidence.	☐	☐	☐	☐	☐

Strategic Cybersecurity Solutions (SCS)

S/N	Statement	SA	A	U	D	SD
16	Multi-factor authentication effectively improves system security.	☐	☐	☐	☐	☐
17	Artificial intelligence enhances fraud detection.	☐	☐	☐	☐	☐
18	Zero Trust Architecture improves cybersecurity resilience.	☐	☐	☐	☐	☐
19	Continuous cybersecurity awareness training reduces cyber risks.	☐	☐	☐	☐	☐
20	Regular vulnerability assessments improve system security.	☐	☐	☐	☐	☐
21	Continuous monitoring helps detect cyber threats promptly.	☐	☐	☐	☐	☐
22	Cybersecurity governance improves organizational resilience.	☐	☐	☐	☐	☐
23	Investment in advanced cybersecurity technologies strengthens organizational security.	☐	☐	☐	☐	☐

Organizational Performance (OP)

S/N	Statement	SA	A	U	D	SD
24	Effective cybersecurity improves organizational efficiency.	☐	☐	☐	☐	☐
25	Cybersecurity practices reduce operational disruptions.	☐	☐	☐	☐	☐
26	Strong cybersecurity contributes to business continuity.	☐	☐	☐	☐	☐
27	Cybersecurity investments improve overall organizational performance.	☐	☐	☐	☐	☐
28	Secure digital platforms enhance service delivery.	☐	☐	☐	☐	☐

Customer Trust (CT)

S/N	Statement	SA	A	U	D	SD
29	Customers trust FinTech services that adequately protect their personal information.	☐	☐	☐	☐	☐
30	Strong data privacy policies increase customer confidence.	☐	☐	☐	☐	☐
31	Cybersecurity incidents reduce customer willingness to use digital financial services.	☐	☐	☐	☐	☐
32	Customers are more likely to remain loyal to secure FinTech platforms.	☐	☐	☐	☐	☐
33	Compliance with data protection regulations enhances customer trust.	☐	☐	☐	☐	☐

Mapping of Questionnaire Items to Research Objectives

Research Objective	Variable	Questionnaire Items
Examine major cybersecurity threats affecting FinTech platforms	Cybersecurity Threats (CST)	1–8
Assess data privacy challenges confronting FinTech organizations	Data Privacy Practices (DPP)	9–15
Identify strategic cybersecurity measures for mitigating cyber risks	Strategic Cybersecurity Solutions (SCS)	16–23
Evaluate the impact on organizational performance	Organizational Performance (OP)	24–28
Evaluate the impact on customer trust	Customer Trust (CT)	29–33