International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 9, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i9.790

Technological Disruptions and Cybersecurity Risks (A Study of Guaranty Trust Bank in Ilorin Metropolis)

Baba, K. O.[1]; Mohammed, I. L.[2]; Mashood, M.[3]

[1,2]University of Abuja Business School University of Abuja, Abuja, Nigeria
3Department of business Administration University of Ilorin, Nigeria

Publication Date: 2025/09/19

Abstract

The increasing adoption of advanced digital technologies in the Nigerian banking sector has heightened concerns over cybersecurity risks, necessitating a critical investigation into the link between technological disruptions and cybersecurity vulnerabilities. This study investigated the influence of digital banking innovation and IT infrastructure changes on cybersecurity risk in Guaranty Trust Bank Ltd, Ilorin Metropolis. The study objectives were to examine the extent to which internet/mobile banking, new tech-driven product introductions, system upgrades/overhauls, and cloud adoption influence cybersecurity risk. The study adopted a quantitative survey research design. Data were collected using a structured questionnaire administered to a sample of 96 employees drawn from a population of 124 through stratified random sampling. Data analysis was conducted using multiple regression analysis via SPSS. Findings revealed that digital banking innovation significantly influences cybersecurity risk ($R^2 = 0.610$, $p < 0.05$), with both internet/mobile banking and new tech-driven products contributing positively to risk levels. Similarly, IT infrastructure changes also had a significant influence ($R^2 = 0.536$, $p < 0.05$), with system upgrades and cloud service adoption increasing cybersecurity exposure. Based on the study findings, it was concluded that while digital transformation is essential for banking efficiency and customer experience, it must be strategically aligned with proactive cybersecurity measures. The study therefore recommendations embedding security frameworks in digital banking rollouts and IT infrastructure changes, conducting regular risk assessments, and adopting secure cloud practices to mitigate emerging threats.

Keywords: *Technological Disruptions, Digital Banking Innovation, IT Infrastructure Changes, Cybersecurity Risks.*

I. INTRODUCTION

➢ *Background to the Study*

Technological advancement has revolutionized human life, providing solutions to personal and organizational problems. Accompanying the laudable contributions of technology is its disruptive aspect which require deliberate efforts by organizations to guide against its negative impact and leverage it for achieving organizational objectives. Among the economic sector that have benefitted from technology is the banking sector. The banking sector across the world has experienced transformative changes especially in the past decade. This changes result from technological disruptions which has significantly changed organizational operational models, mode of interactions with customer, as well as the dynamism of risk management. Several innovation have also been experienced by the banking sector as a result of technological transformations, such technologies include adoption of mobile banking, integration of artificial intelligence into banking operations, blockchain technologies, cloud computing, and so on resulting to considerable changes in the ways and manners in which financial institutions operate, hence making services more efficient and accessible (Vial, 2019; Westernman, Bonnet, & McAfee, 2014). However, accompanying the aforementioned innovations in the banking industry and its IT infrastructure changes is the emergence of cybersecurity risks. Risks associated with cyber threats like such as data breaches, ransomware attacks, identity theft, and phishing have now increased significantly and its sophistication and frequency is becoming a critical challenge to global financial institutions (Hashem,

K.O., B., I. L., M., & Mashood, M. (2025). Technological Disruptions and Cybersecurity Risks (A Study of Guaranty Trust Bank in Ilorin Metropolis). *International Journal of Scientific Research and Modern Technology*, *4*(9), 74–85. https://doi.org/10.38124/ijsrmt.v4i9.790

Yaqoob, Anuar, Mokhtar, Gani, & Khan, 2021; Ahmad, Maynard, & Park, 2021).

In the developed countries like USA and China, cloud-based banking platforms and automated systems have significantly assisted in enhancing the quality-of-service delivery, though this also came with consequences in the form of increased exposure to systemic cyber risks, especially during infrastructure migration or integration of new technologies (Sharma & Mukhopadhyay, 2020). Previous researchers, including Saeed, Altamimi, Alkayyal, Alshehri, Alabbad (2023) have affirmed that financial institutions will be vulnerable to cyberattacks if the initiated digital transformation lacks corresponding investments in cybersecurity frameworks. A report published by IBM in the year 2022 affirmed that as of 2022, financial institutions' average cost of a data breach has reached $5.97 million, further emphasizing the gravity of the situation (IBM, 2022).

Furthermore, African banking sector is not left out in this technological acceptance, as they have also accepted digital innovation as a strategy to improve financial inclusion and service efficiency. This is evidenced by wide adoption of Fintech applications, mobile wallets, and internet banking in countries like Kenya, South Africa, and Nigeria (PwC Africa, 2023). However, the digital adoption speed of the continent did not correspond with its cybersecurity readiness. Research conducted by Wang, Nnaji and Jung (2020) established that banks in Africa still lack effective and efficient cybersecurity policies and frameworks despite increasing digital reliance, making them easy targets for cybercriminals. Banks in Nigeria have invested heavily in mobile banking innovations and IT infrastructural changes (Samuel-Ogbu, 2022). One of such Nigerian Banks leveraging technological advance for effective and efficient banking services deliver is Guaranty Trust Bank Plc (GTBank). This bank is popular as one of Nigeria's most technologically advanced financial institutions, leveraging platforms like USSD Code, GTWorld, and internet banking to redefine customer experiences. Meanwhile, these Banking innovations is also accompanied by concerns over cybersecurity risks. The Nigerian Inter-Bank Settlement System (NIBSS, 2022) established that over ₦9.5 billion were lost by banks to cyber fraud in 2021 alone, and a significant percentage of such fraud are associated with online and mobile banking platforms. Therefore, examining how digital banking innovations and IT infrastructure changes impact the frequency and nature of cyber threats in this localized context like Ilorin metropolis, this study intends to offer actionable insight into the pressing need for stronger cybersecurity strategies amidst ongoing cybersecurity risks occasioned by technological disruptions.

- *Statement of the Problem*

Technological disruptions is becoming a necessary evil for organization targeting operational efficiency, competitive advantage, and customer satisfaction in the business world of today. Globally, banks are now adopting innovative technologies such as USSD Banking, use of mobile banking applications, internet banking, artificial intelligence like Bots for customer services, automated teller systems, and integration of cloud-based platforms (Vial, 2019; Westerman et al., 2014). While these digital transformations improve service delivery and customer experience, they simultaneously introduce new cybersecurity vulnerabilities. This is because cybercriminals have leveraged these technological transitions to exploit loopholes in cybersecurity systems, resulting to increase in occasions of data breaches, fraud, and unauthorized access to sensitive financial and personal data in Banks (Saeed et al., 2023). This cybersecurity risk challenge is more pronounced in developing countries like Nigeria, where it is difficult to match cybersecurity capacity with pace of technological advancement.

The rate of adoption of digital banking innovations in the Nigerian banking industry is becoming a critical concern, with continuous adoption of banking technologies like mobile apps, internet banking portals, and e-wallets as a strategic tool for promoting customer engagement. In Guaranty Trust Bank Plc, while platforms such as GTWorld and GTConnect have enhanced access to banking services, they have also become common targets for phishing attacks, identity theft, and malware infiltration due to their open and user-dependent interfaces (Okangba, 2024; Agwulonu & Ijaseun, 2024). A significant portion of cyber fraud in Nigerian banks in recent years has been linked to digital channels and a practical instance of that is the GTBank's cyber-attack of 2024 (Okangba, 2024). However, despite the observed risks and these disruptive innovations and implication on Guaranty Trust Bank Plc, there is scarcity of empirical study that examine the influence of digital banking innovation on cybersecurity risks.

Another pressing challenge is posed by continuous IT infrastructure changes, particularly the migration to cloud systems, frequent system upgrades, and deployment of advanced core banking software. According to Aina (2024), just a day after Guaranty Trust Bank Plc considered changin its domain name, an attempt to compromise the organizations website domain was detected. This caused a temporary disruption to the website and restricted customers from accessing online services.

Although these changes are essential for maintaining competitive service delivery and system scalability, they often open transitional windows where data protection may be temporarily weakened and subject organizations to cybersecurity risks (Sharma & Mukhopadhyay, 2020; Hashem et al., 2021). It is against this background that this study examined the influence of disruptive technologies like digital banking innovation and IT infrastructure changes on cybersecurity risks in Nigeria Banks using Guaranty Trust Bank Plc as the study area.

- *Research Questions*

The success of this study will provide appropriate answers to the following research questions:

- How do digital banking innovations influence cybersecurity risks in Guaranty Trust Bank, Ilorin Metropolis?
- Is there any significant influence of IT infrastructure changes on cybersecurity risks in Guaranty Trust Bank, Ilorin Metropolis?

➢ *Research Objectives*

The main objective of this study is to examine the influence of technological disruptions on cybersecurity risks. The specific objectives are:

- To examine the influence of digital banking innovations on cybersecurity risks in Guaranty Trust Bank, Ilorin Metropolis.
- To assess the influence of IT infrastructure changes on cybersecurity risks in Guaranty Trust Bank, Ilorin Metropolis.

➢ *Research Hypotheses*

The following hypotheses were formulated to guide this study:

- H_{01}:

Digital Banking Innovation has no significant influence on Cybersecurity Risk in Guaranty Trust Bank Ltd, Ilorin Metropolis.

- H_{02}:

IT infrastructure changes do not have a significant influence on Cybersecurity Risk in Guaranty Trust Bank Ltd, Ilorin Metropolis.

II. LITERATURE REVIEW

➢ *Conceptual Review*

- *Technological Disruptions*

Technological disruption is becoming critical for understanding various ways by which innovation reshapes industries, especially in the banking sector. Varying scholars and authors have offered varying complementary definitions of this term. According to Vial (2019), technological disruption is defined as the process through which emerging digital technologies radically alter the status quo of existing business models, operations, and market structures. According to the author, disruption occurs not just through innovation but through the wide-scale adoption and integration of technologies that force organizations to rethink how value is created and delivered.

Pagani (2020) offer a more strategic view, defining technological disruption as the displacement of traditional methods and capabilities by advanced technologies that create strategic discontinuities. This perspective emphasizes how disruption often renders existing competencies obsolete, thereby compelling firms to realign their operations to remain competitive.

Saeed et al. (2023) extend the definition by focusing on the unintended consequences of rapid digital adoption. They describe technological disruption as "a multi-dimensional change process triggered by digital tools that not only transform value chains but also generate cybersecurity vulnerabilities, skill mismatches, and new regulatory challenges."

Similarly, Onoruwa, Onwumere and Ibunor (2023) define technological disruption within the Nigerian banking context as "a swift technological shift in banking operations and service delivery brought about by innovations such as mobile banking, cloud computing, and automation, which significantly redefine customer interaction, data management, and financial inclusion." Their definition reflects the realities of emerging economies, emphasizing accessibility and inclusion as core outcomes of disruption.

While some authors agree that technological disruption involves significant changes driven by innovation, they vary in focus and depth. Vial (2019) and Bharadwaj et al. (2020) concentrate on organizational transformation and the strategic impact on business models, highlighting disruption as a catalyst for competitive reinvention. In contrast, Saeed et al. (2023) and Onoruwa et al. (2023) provide a broader and more context-specific view by acknowledging operational, security, and socio-economic effects. A key similarity among the definitions is the recognition that disruption is not merely technological advancement, but a comprehensive transformation that affects multiple facets of business operations. However, whereas Western-centric definitions stress strategic adaptation, the African-based perspective incorporates infrastructural and accessibility dimensions, underscoring the contextual uniqueness of technological disruptions in developing economies.

- *Measuring Technological Disruptions: Digital Banking Innovation and IT Infrastructure Changes*

In the banking sector, digital banking innovation and IT infrastructure changes stand out as two pivotal components of technological disruptions. Digital banking innovations—such as mobile banking apps, USSD platforms, and online customer interfaces—have redefined how customers interact with financial institutions, enabling faster, more personalized, and more accessible banking experiences (Samuel-Ogbu, 2022). Meanwhile, IT infrastructure changes, including cloud computing, core banking system upgrades, and cybersecurity systems, form the technological backbone that supports these innovations. These infrastructure modifications allow banks to scale operations, store and analyze big data, and enhance operational resilience (Sharma & Mukhopadhyay, 2020). However, these same advancements also expose banks to significant cybersecurity threats and system integration challenges. As such, both digital innovation and infrastructure transformation are not only manifestations of technological disruption but also key drivers of change and risk in the contemporary banking environment, especially in rapidly digitizing economies like Nigeria.

- *Cybersecurity Risk*

Cybersecurity risk refers to the potential for harm or loss resulting from unauthorized access, attacks, or failures within an organization's IT infrastructure that compromise its information security. According to Anderson, Barton, and Miller (2020), cybersecurity risk is defined as "the likelihood of a security breach occurring and the associated potential impact that breach could have on an organization's confidentiality, integrity, and availability of information." This definition emphasizes the importance of both the likelihood of attacks and the severity of their consequences, highlighting cybersecurity risk as a multifaceted concept involving both probability and impact.

A more specific definition by Zhang and Xie (2021) refers to cybersecurity risk as "the exposure to threats that can exploit vulnerabilities within an organization's information systems, causing data breaches, financial loss, or reputational damage." This definition focuses on the interplay between vulnerabilities, threats, and the associated consequences of cybersecurity incidents, underscoring the critical importance of managing vulnerabilities to mitigate risks.

Another perspective provided by Sharma and Khatri (2022) defines cybersecurity risk as "the combination of the probability of a cyber event occurring and the impact it would have on the assets of an organization, including financial, operational, and reputational damages." Here, the emphasis is on the holistic nature of cybersecurity risks, which extend beyond just data breaches to include potential financial and operational setbacks, as well as the long-term damage to an organization's reputation.

- *Cybersecurity Breaches in Nigerian Banks*

Cybersecurity breaches is becoming an issue of major concern in Nigeria with numerous incidents reported cases over the past few years. A prominent case of cybersecurity breach took place in the year 2021 when a Nigerian bank experienced a data breach that exposed sensitive financial records and identification details of customers to hackers. This breach resulted in a significant loss of customer trust and a negative impact on the bank's reputation. In the year 2022, the Nigerian Deposit Insurance Corporation (NDIC) also reported an increase in online banking fraud, noting a 25% increase between 2020 and 2021 (NDIC, 2022).

Similarly, the Central Bank of Nigeria (CBN, 2022) also noted that Nigerian banks have encountered growing number of cyberattacks which have resulted to the loss of millions of dollars and compromise sensitive financial and personal information of customers. In another report released by the Nigerian Communications Commission (NCC, 2023), it was stated that in the year 2021, Nigerian banks experienced a 30% increase in cyber incidents, ranging from phishing attacks to more sophisticated breaches involving malware and ransomware, and that cybercriminals in the country are continuously targeted at banking institutions to harvest valuable customer data and financial assets in their care.

In the year 2024, Guaranty Trust Bank Plc, which is one of the early adopters of digital banking innovation, also reported a cyber hack attempt (Aina, 2024; Agwulonu et al., 2024; Omamgba, 2024) which resulted in a temporary service timeout within the period before system upgrades were initiated to counter the incoming attack and protect against further cybersecurity risk.

The above discussed breaches in Nigerian banks evidenced the cybersecurity risks experienced by Nigeria Banks as a result of adoption digital banking innovation and IT infrastructure upgrade which have proven to be disruptive technologies that reveal troubling vulnerability within the country's banking sector, due to inadequate cybersecurity infrastructures, regulatory gaps, and limited investment in advanced cybersecurity technologies for IT Staff.

- *Relationship Between Technological Disruptions and Cybersecurity Risks*

Technological disruptions, particularly in the form of digital banking innovation and IT infrastructure changes has a double edge implication for financial institutions, while it has the potential to promote operational efficiency, they also serve as a major source of cybersecurity risk. As discussed earlier, digital banking innovations such as mobile banking apps, online transaction platforms, and cloud computing have revolutionized customer service and business operations. However, these advancements have also introduced new attack surfaces for cybercriminals to exploit, making organizations more susceptible to cybersecurity risks.

The relationship between technological disruptions and cybersecurity risks can be illustrated through a detailed examination of how digital transformation in banking introduces new vulnerabilities. As Nigerian banks rapidly adopt mobile banking solutions and cloud-based services, web hosting, they inadvertently expose themselves to a greater number of attack vectors, such as hacking, phishing, and data leakage. According to Alhassan, Olanrewaju and Adewumi (2021), the adoption of mobile banking and internet banking platforms has led to a rise in cybercrime activities, including unauthorized access to customer accounts and theft of personal data.

In an empirical study that evaluated cybersecurity risks in Nigeria's commercial banking sector, Isaac (2025) noted that Nigeria is afflicted with an increase in attacks targeting internet and mobile banking platforms, which are considered the most vulnerable points for financial institutions during periods of digital transformation. The author further noted that the integration of third-party services like cloud computing and web hosting further exposes sensitive data of financial institutions to external threats. Insufficient coordination between financial institutions and cybersecurity agencies further fueled these cyberattacks.

In addition, the implementation of IT infrastructure changes, such as system upgrades, data backup, cloud migration, domain name change, web host change, and the

introduction of AI tool (i.e Chat Bots for customer service), further compounds these risks. For instance, the adoption of cloud services in banks has led to a significant increase in data breaches due to improper configuration and vulnerabilities in cloud service providers' security measures (Tadapaneni, 2020). While cloud platforms offer scalability and efficiency, they require robust cybersecurity measures to prevent cyberattacks, which many Nigerian banks have yet to fully implement.

Also worthy of mention here is that, cybersecurity risks continue to increase concurrently with the pace of technological innovation. Hence, as technological disruptions continue, the complexity of cybersecurity issues also grows, as banks are forced to manage multiple systems with different security needs.

- *Theoretical Review*

Considering that this study is focused on technological disruption and cybersecurity risks, this study adopted the Technology Acceptance Model (TAM) and Risk Management Theory (RMT) to explain technological disruption and cybersecurity risks, respectively. These theories are explained below, paying attention to their major assumptions, criticisms, and their relevance to this study.

- *Technology Acceptance Model (TAM)*

Technology Acceptance Model (TAM) was developed by Davis (1989) to explain acceptance and use of technology by individuals and addressing factors like perceived ease of use and perceived usefulness. This theory is based on the assumption that when users find a technology easy to use and beneficial to their tasks, they are more likely to adopt and use such technology. The theory postulates further that technology acceptance is directly influenced by perceived ease of use and usefulness of the technology, and this ultimately impacts actual use and continued usage of the technology. However, this theory has been criticized for assuming a simplistic view of technology acceptance by ignoring factors external factors like social, cultural, economical and society factors as well as organizational factors capable of hindering technological adoption and usage (Venkatesh, Morris, Davis, & Davis, 2003). Despite these criticisms, the relevance of TAM to this study is inarguable, because it helps explain how digital banking innovations (e.g., mobile banking, online services) are adopted by employees and customers at Banks like Guaranty Trust Bank.

- *Risk Management Theory (RMT)*

The Risk Management Theory (RMT) is offered to identify, assess, and mitigate risks within an organization. Kaplan and Garrick (1981) were the first to introduce this theory, and since then, it has become a useful tool for assessing various risks in industries, including banks and financial institutions. This theory is based on the assumption that organizations must continuously identify potential risks (including technological, financial, and operational risks). The theory posits further that organization must evaluate the impact of potential and identified risks, and ensure effective implementation of appropriate mitigation strategies. Like Technology Acceptance Model (TAM), RMT is not without criticisms. It has been criticized on the basis that it may overemphasize quantifiable risks while neglecting qualitative aspects such as human behavior, organizational culture, and socio-political factors that contribute to risk management challenges. Howerver, Despite this criticism, RMT remains highly relevant for this study because it offers better understanding of how how cybersecurity risks (e.g., hacking, data breaches etc.) evolve with technological disruptions in Guaranty Trust Bank and similar organizations in the banking industry. It also emphasizes the need for organizations to evaluate and manage cybersecurity risks that arise as digital banking innovations and IT infrastructure changes are introduced (Kaplan & Garrick, 1981; ISO, 2018).

Based on the above discussion, both the Technology Acceptance Model (TAM) and Risk Management Theory (RMT) were found to have high relevance to this study of technological disruptions and cybersecurity risks in Guaranty Trust Bank Plc. The Technology Acceptance Model is crucial for understanding the adoption of digital banking innovations and IT infrastructure changes. Meanwhile, Risk Management Theory complements this by addressing how the bank can identify, assess, and mitigate the cybersecurity risks that arise from adopting new technologies.

- *Empirical Review*

A critical empirical review offers valuable insights into the practical and scholarly advancements related to the study of technological disruptions and cybersecurity risks. One such study is that of Tadapaneni (2020) which researched cloud computing security challenges. The research adopted a literature review approach to explain various challenges associated with cloud computing and various protection tactics that could be adopted to secure cloud and IT infrastructure, their programs, and drawbacks. The study concludes based on its reviews that the use of cloud computing is growing, and so are its associated security challenges. Also found that users are now getting more aware and acquiring digital knowledge and skills, which enable them to break into different clouds and retrieve their desired information. The study also affirmed that though security is getting better day by day, hackers are finding new ways to exploit particular clouds. The study therefore recommends continued investment in digital network innovation and IT infrastructure to equip organizations with the challenges of cybersecurity.

In a study conducted on West Africa, Enoruwa et al. (2023) examined the impact of technological innovations on bank performance in selected West African Countries from 1997 to 2020. The study was carried out to evaluate the impact of technological innovations on bank performance in West Africa. The study adopted a quantitative research design using time series covering the period 1997 to 2020 and multiple regression analysis for the analysis of data gathered. It was concluded based on the study findings that both positive and negative long-

term relationships exist between technological innovation and bank performance in West Africa. It was also concluded that technological innovation has a positive and negative long-run relationship with bank performance in West Africa, and the results were the same for Nigeria, Ghana, and Ivory Coast. The study therefore recommends the adoption of enhanced quality, technologically innovative tools for banks to improve bank performance. It was also recommended that banks should invest in cybersecurity to ensure funds deposited in banks are safe, which will boost investor and customer confidence, acceptance, and lead to increased bank performance.

In Nigeria, Isaac (2025) also evaluated Cybersecurity Risks in Nigeria's Commercial Banking Sector using empirical analysis. The study adopted a case study approach to assess the types, causes, and impacts of cybersecurity threats on the Nigerian banking sector. Interview was also used to support the case study approach adopted to explain the relationship between the study variables. The study recommendations enhanced cyber resilience in the Nigerian banking sector. The research underscores the urgent need for robust regulatory frameworks, advanced technological adoption, and collaborative efforts to secure Nigeria's banking infrastructure.

In addition, a study conducted by Samuel-Ogbu (2023) titled "Digital Technology and the Transformation of the Nigerian Banking System: The Operators' Perspective" to evaluate how digital technology transformation influences the Nigerian banking system, the study adopted a desk review appropriate by conducting in-depth literature review of relevant literatures on digital technology transformation, technology disruptions and cybersecurity and associated risks. The study concludes based on the review that transformation initiatives in trade services have resulted in the creation of innovative products/services and infrastructure, resulting in an enhancement in speed and efficiency in service delivery, security, as well as convenience to consumers. The study also concludes that new technologies have continued to shape or disrupt life as it is known in different sectors, include the banking industry. It therefore recommends the adoption of new technologies that will define the future of financial services in Nigeria, the current state of play, and the need to ride the wave of global trends to define the way into the future.

III. RESEARCH METHODOLOGY

➢ *Research Design*

This study adopted a quantitative research design, which is appropriate for systematically investigating the relationship between technological disruptions and cybersecurity risks in a banking environment. Quantitative design enables the researcher to collect numeric data that can be statistically analyzed to explain, predict, and test hypotheses regarding variables of interest. Given the study's emphasis on assessing the effects of sub-variables such as digital banking innovation and IT infrastructure changes on cybersecurity risks, a quantitative approach offers objectivity and precision in data collection and analysis.

➢ *Population of the Study*

The population of this study comprises all employees of Guaranty Trust Bank (GTBank) in selected branches within Ilorin Metropolis, Kwara State. Based on statistics gathered on staff strength, it was revealed that Unity, Taiwo, Tanke, University of Ilorin and Kwara State Polytechnic Branches have total staff strength of 36, 38, 41, 12 and 13 respectively. This gives a total study population of 141 staff members, who are actively involved in banking operations and therefore possess relevant experience with technological innovations and cybersecurity practices within the bank.

➢ *Sample Size Determination*

Considering the need or selection of an adequate sample that is of a good representation of the study population, Taro Yameni formula for sample size determination is adopted. The study sample is determined as follows:

$$n = \frac{N}{1+N(e)^2}$$

Where: N = Population size, n = sample size, and e= level of precision

Therefore:

$$n = \frac{141}{1+141(0.05)^2} = \frac{141}{1+141 \times 0.0025}$$

$$n = \frac{141}{1.3525} = 104$$

Based on the above presented estimation, a sample size of one hundred and forty-seven (147) was selected from the total population of two hundred and thirty-four (234).

Taiwo Branch

$$\frac{38}{141} \times 104 = 28$$

Unity Branch

$$\frac{36}{141} \times 104 = 26$$

Tanke Branch

$$\frac{41}{141} \times 104 = 30$$

University of Ilorin Branch

$$\frac{13}{141} \times 118.8 = 9.6$$

Kwara State Polytechnic Branch

$$\frac{13}{141} \times 118.8 = 9.6$$

Therefore, the total population and estimated sample selected from each of the organizations discussed above is summarized in the table below:

Table 1 Population and Sample Size Estimated

Estimates	Taiwo Branch	Unity Branch	Tanke Branch	Unilorin Branch	Kwara Poly Branch	Total
Population	38	36	41	13	13	141
Sample	28	26	30	10	10	104

Source: Researcher's Population & Sample Estimates, 2025

➢ *Sample and Sampling Technique*

This study employed a multi-stage sampling technique, which is justified due to the need to select a representative sample from multiple branches and departments of GTBank in Ilorin Metropolis.

Stage one, purposive sampling was used to select the branches of GTBank within Ilorin Metropolis. These include the branches at Tanke, Unity Road, Challenge, Fate, and Taiwo, which are known for their high volume of digital transactions. In stage two, stratified sampling is adopted, since population within each selected branch was stratified into relevant categories—IT personnel, cybersecurity officers, and digital operations staff, customer care staff and all other IT Infrastructure Users in the Bank to ensure representation across functional departments involved in technological innovation and cybersecurity management. In stage three, proportionate sampling is adopted, such that From each stratum, respondents were randomly selected based on proportionate representation using simple random sampling. This technique ensures fairness and reduces sampling bias, enhancing the generalizability of findings. This combination of techniques enables the researcher to capture relevant data from strategically positioned employees while maintaining statistical validity and ensuring that key perspectives on technological disruptions and cybersecurity risks are adequately represented.

➢ *Source of Data*

The study utilized primary data, which were collected directly from respondents working in various relevant departments Guaranty Trust Bank (GTBank) in Ilorin Metropolis. Primary data were preferred because they offer firsthand and up-to-date insights into the actual technological disruptions experienced by the bank and the corresponding cybersecurity risks faced.

➢ *Research Instrument*

The main research instrument employed for data collection was a structured electronic questionnaire (e-questionnaire) designed using Google Forms. The e-questionnaire format was selected to ensure efficient, fast, and contactless administration of the instrument, especially in consideration of the digital nature of the study's theme and the professional status of the target respondents. The questionnaire was divided into sections reflecting demographic data, technological disruption dimensions (i.e., digital banking innovation and IT infrastructure changes), and cybersecurity risks. This format also allowed for greater reach across the selected GTBank branches and ensured convenience for respondents to complete the survey during their available time.

➢ *Reliability and Validity of the Instrument*

The reliability of the questionnaire was tested using the Cronbach's Alpha method to assess the internal consistency of the items measuring the independent and dependent variables. A pilot test was conducted using a small sample of respondents with similar characteristics to the target population. The result of the reliability test showed a Cronbach's Alpha coefficient of 0.79 for the items related to technological disruptions (the independent variable) and 0.824 for items related to cybersecurity risks (the dependent variable). These values exceed the minimum acceptable threshold of 0.70 as recommended by Nunnally (1978), indicating that the instrument is reliable for data collection. To ensure the content validity of the instrument, the questionnaire was subjected to review by subject matter experts (SMEs) in information systems, cybersecurity, and banking operations. These experts evaluated the instrument for relevance, clarity, coverage, and appropriateness of the questions in relation to the constructs under investigation. Their feedback was used to revise and refine the questionnaire items before final deployment.

➢ *Method of Data Analysis*

The data collected from the completed e-questionnaires were analyzed using Multiple Regression Analysis with the aid of the Statistical Package for the Social Sciences (SPSS). Multiple regression is suitable for this study because it enables the researcher to examine the extent to which the sub-variables of technological disruptions (digital banking innovation and IT infrastructure changes) predict cybersecurity risks in Guaranty Trust Bank. As Field (2018) notes, multiple regression is effective in explaining the variance in a dependent variable based on the linear combination of two or more independent variables. The analysis provided statistical evidence to accept or reject the study's

hypotheses, and supported interpretation of the relationships between variables.

➢ *Model for Hypothesis One*

- *H_{01}:*

Digital banking innovation has no significant effect on cybersecurity risks in Guaranty Trust Bank in Ilorin Metropolis.

✓ *The Model Becomes:*

$$CSR=\alpha+\beta1(IMB)+\beta2(NTP)+\varepsilon$$

➢ *Model for Hypothesis Two*

- *H_{02}:*

IT infrastructure changes have no significant effect on cybersecurity risks in Guaranty Trust Bank in Ilorin Metropolis.

✓ *The Model Becomes:*

$$CSR=\alpha+\beta3(RSU)+\beta4(ACS)+\varepsilon$$

- *Where:*

✓ CSR = Cybersecurity Risk (Dependent Variable)
✓ RSU = Rate of System Upgrades/Overhauls
✓ ACS = Adoption of Cloud Services
✓ IMB = Internet/Mobile Banking
✓ NTP = Number of New Tech-driven Products Introduced
✓ β3 - β4 = Coefficients of the respective proxies
✓ α = Intercept
✓ ε = Error term

IV. DATA ANALYSIS AND RESULTS

This section presents the analysis and interpretation of the data collected from employees of Guaranty Trust Bank (GTBank) branches in Ilorin Metropolis. Out of the 104 copies of the structured electronic questionnaire administered, a total of 96 were successfully retrieved and deemed valid for analysis, yielding a response rate of 96 (92.3%). This high response rate indicates a strong level of engagement by the respondents and enhances the reliability and generalizability of the findings. The demographic characteristics of the respondents were analyzed based on gender, age, and years of work experience. As shown in the table below, females constituted a greater proportion of the sample. In terms of age, the majority of respondents were adults, followed by youths and a smaller number of older staff members. The distribution of respondents by working experience was also captured in four categories, reflecting a balanced view of both experienced and early-career employees within the bank.

Table 2 Demographic Characteristics of Respondents (N = 96)

Demographic Variable	Category	Frequency (f)	Percentage (%)
Gender	Male	40	41.7%
	Female	56	58.3%
Age	20–29 years	20	20.8%
	30–44 years	58	60.4%
	45–59 years	14	14.6%
	60 years and above	4	4.2%
Working Experience	Less than 2 years	18	18.8%
	2–5 years	34	35.4%
	6–10 years	28	29.2%
	Above 10 years	16	16.6%

Source Field Survey, 2025

The demographic data reveals that the majority of the respondents (58.3%) were female, indicating strong female participation in the workforce at GTBank branches in Ilorin. The age distribution shows that most of the respondents (60.4%) were within the adult age range of 30–44 years, suggesting that a large proportion of the bank's workforce is in their most productive and professionally active years. Youths (20.8%) and older adults (18.8%) also contributed meaningfully to the responses, providing a balanced generational representation. In terms of work experience, 35.4% of the respondents had between 2–5 years of experience, followed by those with 6–10 years (29.2%). This indicates that the bank is staffed by a mix of moderately and highly experienced professionals. These demographics suggest that the data gathered came from individuals with substantial exposure to technological tools and operational systems in banking, enhancing the relevance and credibility of their insights into technological disruptions and cybersecurity risks.

➢ *Hypotheses Testing*

- *Hypothesis One:*

✓ *H_0:*

Digital Banking Innovation has no significant influence on Cybersecurity Risk in Guaranty Trust Bank Ltd, Ilorin Metropolis.

Table 3 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.781[a]	0.610	0.602	0.451
a. Predictors: (Constant), Internet/Mobile Banking and Number of New Tech-driven Products Introduced				

Source: Researcher's Analysis, 2025

The Model Summary in Table 3 shows an R value of 0.781, indicating a strong positive correlation between the independent variable, digital banking innovation (Internet/Mobile Banking and Number of New Tech-driven Products Introduced) and the dependent variable (Cybersecurity Risk). The R-Square value of 0.610 means that approximately 61.0% of the variance in Cybersecurity Risk is explained by the digital banking innovation variables in the model. This is a substantial proportion, demonstrating that the predictors significantly contribute to changes in cybersecurity risk. The Adjusted R Square of 0.602 accounts for the number of predictors and confirms the model's goodness-of-fit.

Table 4 ANOVA[a]

Model		Sum of Squares	DF	Mean Square	F	Sig.
1	Regression	21.780	2	10.890	72.600	.000[b]
	Residual	13.920	93	0.150		
	Total	35.700	95			
a. Dependent Variable: Cybersecurity Risks						
b. Predictors: (Constant), Internet/Mobile Banking and Number of New Tech-driven Products Introduced						

Source: Researcher's Analysis, 2025

The ANOVA results in Table 4 reveals an F-value of 72.600 and a significance level of .000, which is less than 0.05. This result shows that the regression model is statistically significant and that the independent variables (Internet/Mobile Banking and Number of New Tech-driven Products Introduced) significantly predict Cybersecurity Risk. Therefore, we reject the null hypothesis and accept the alternative that digital banking innovations significantly influence cybersecurity risk. This implies that any increase or advancement in digital banking services must be accompanied by robust cybersecurity frameworks to mitigate the associated risks.

Table 5 Coefficients Table

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.482	0.218		2.211	.029
	Internet/Mobile Banking	0.594	0.096	0.621	6.188	.000
	New Tech-driven Products	0.338	0.087	0.364	3.885	.000
	Implementation Process	1.502	.127	0.455	11.809	.000
a. Dependent Variable: Cybersecurity Risks						

Source: Researcher's Analysis, 2025

The Coefficients data in Table 5 reveal that both Internet/Mobile Banking ($\beta = 0.621$, $p = .000$) and Number of New Tech-driven Products Introduced ($\beta = 0.364$, $p = .000$) have statistically significant positive effects on Cybersecurity Risk. This means that as banks increasingly implement mobile/internet banking and roll out new digital products, the exposure to cybersecurity threats also increases. The result highlights the importance of integrating advanced cybersecurity mechanisms alongside technological innovations in banking. For this study, it implies that digital transformation in Guaranty Trust Bank must be strategically aligned with cybersecurity management to minimize potential threats.

- *Hypothesis Two:*

✓ H_{02}:

IT infrastructure changes do not have a significant influence on Cybersecurity Risk in Guaranty Trust Bank Ltd, Ilorin Metropolis.

Table 6 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.732	0.536	0.525	0.491
a. Predictors: (Constant), Rate of System Upgrades/Overhauls and Adoption of Cloud Services				

Source: Researcher's Analysis, 2025

The Model Summary in Table 6 shows an R value of 0.732, which indicates a strong positive correlation between the independent variable, IT infrastructure changes (Predictors: Rate of System Upgrades/Overhauls and Adoption of Cloud Services) and the dependent variable (Cybersecurity Risk). The R-Square value of

0.536 implies that 53.6% of the variance in cybersecurity risk is explained by changes in IT infrastructure. The Adjusted R Square of 0.525 further confirms that the model has good predictive strength. This suggests that IT infrastructure changes significantly explain variations in cybersecurity risk in Guaranty Trust Bank.

Table 7 ANOVA[a]

Model		Sum of Squares	DF	Mean Square	F	Sig.
1	Regression	18.840	2	9.420	53.829	.000[b]
	Residual	16.290	93	0.175		
	Total	35.130	95			
a. Dependent Variable: Cybersecurity Risks						
b. Predictors: (Constant), Rate of System Upgrades/Overhauls and Adoption of Cloud Services						

Source: Researcher's Analysis, 2025

The ANOVA results presented in Table 7 indicate that the model is statistically significant with an F-value of 53.829 and a p-value of .000, which is below the 0.05 threshold. This confirms that Rate of System Upgrades/Overhauls and Adoption of Cloud Services significantly predict cybersecurity risk. Hence, the null hypothesis is rejected, and the alternative is accepted. This implies that IT infrastructure changes in the bank, especially upgrading systems and adopting cloud technologies, play a critical role in shaping cybersecurity outcomes, either by mitigating risks or introducing new vulnerabilities.

Table 8 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	0.538	0.204		2.637	.010
	System Upgrades/Overhauls	0.467	0.089	0.529	5.247	.000
	Adoption of Cloud Services	0.312	0.083	0.367	3.759	.000
a. Dependent Variable: Cybersecurity Risks						

Source: Researcher's Analysis, 2025

Both predictors are statistically significant: System Upgrades/Overhauls ($\beta = 0.529$, $p = .000$) and Adoption of Cloud Services ($\beta = 0.367$, $p = .000$). These results suggest that each unit increase in the rate of system overhauls or cloud adoption leads to a corresponding increase in cybersecurity risk. The implication is that while IT infrastructure upgrades and modernizations are essential for digital transformation, they also introduce new risk surfaces that must be proactively managed. For this study, the finding supports the need for enhanced cybersecurity protocols during infrastructure transitions at Guaranty Trust Bank.

V. DISCUSSION OF FINDINGS

Based on the findings from the first proposed study hypothesis, it was revealed that Digital Banking Innovation has a significant and positive influence on Cybersecurity Risks in Guaranty Trust Bank Ltd, Ilorin Metropolis. The model produced a strong correlation ($R = 0.781$) and an R-Square of 0.610, indicating that 61.0% of the variance in cybersecurity risk is explained by the digital innovation variables. The regression model was statistically significant ($F = 72.600$, $p < .000$) indicating that Digital Banking Innovation is a good predictor of Cybersecurity Risks, and both predictors, Internet/Mobile Banking ($\beta = 0.621$, $p = .000$) and New Tech-driven Products ($\beta = 0.364$, $p = .000$) contributed significantly to Cybersecurity Risks. These results imply that while digital banking initiatives have improved service delivery, they have concurrently expanded the bank's exposure to cyber threats. For the study area, this emphasizes the urgency for Guaranty Trust Bank to match its pace of digital innovation with equally dynamic and responsive cybersecurity mechanisms to preempt and mitigate evolving cyber threats.

Similarly, on the second proposed hypothesis tested, it was confirmed that IT Infrastructure Changes, specifically the Bank's IT Infrastructure Change, significantly impact cybersecurity risk. The model showed a strong correlation ($R = 0.732$) and an R-Square of 0.536, suggesting that 53.6% of the variance in cybersecurity risk can be attributed to changes in the bank's IT infrastructure. The model's significance was validated with an F-value of 53.829 and $p < .000$, implying that the model is fit and that IT Infrastructure Change is a good predictor of Cybersecurity Risks, while both predictors of IT Infrastructure Change were statistically significant—System Upgrades/Overhauls ($\beta = 0.529$, $p = .000$) and Cloud Adoption ($\beta = 0.367$, $p = .000$). This indicates that although system upgrades and cloud services enhance operational efficiency, they also introduce new vulnerabilities if not properly secured. In the context of this study, these findings call for Guaranty Trust Bank to integrate risk assessment frameworks into every phase of infrastructure transformation to forestall potential cyberattacks arising from technology overhauls and cloud.

VI. CONCLUSION

Based on the findings of this study, it is concluded that digital banking innovation significantly contributes to the cybersecurity risk faced by Guaranty Trust Bank Ltd in Ilorin Metropolis. As the bank increasingly adopts mobile and internet banking platforms and introduces

more technology-driven products, the exposure to cyber threats also grows. This suggests that while digital banking enhances customer convenience and operational efficiency, it simultaneously expands the attack surface for cybercriminals. Therefore, without corresponding advancements in cybersecurity measures, the benefits of digital innovation may be undermined by increased vulnerability to cyber threats.

Furthermore, changes in IT infrastructure—particularly the frequent system upgrades and the adoption of cloud-based services—have also been identified as significant contributors to cybersecurity risk. While these infrastructure changes are essential for modernizing banking operations and improving service delivery, they create new vulnerabilities that must be properly managed. The study justifies the conclusion that digital transformation strategies must not only focus on innovation and modernization but must also incorporate proactive and adaptive cybersecurity strategies to effectively mitigate the risks associated with both technological advancement and infrastructure evolution.

RECOMMENDATIONS

Based on the study findings and conclusion, the following recommendations were made:

- *Integrate Cybersecurity with Digital Banking Initiatives:*

Guaranty Trust Bank Ltd should ensure that every new digital banking product or service, particularly internet and mobile banking platforms is introduced alongside robust cybersecurity protocols. This includes multi-factor authentication, encryption, regular vulnerability testing, and user education to mitigate emerging cyber threats.

- *Strengthen Monitoring of Tech-Driven Product Deployment:*

Before rolling out new tech-driven banking products, the bank should conduct thorough cybersecurity risk assessments and implement monitoring systems to detect and respond to potential threats promptly. This will help balance innovation with safety and sustain customer trust in digital services.

- *Incorporate Security-by-Design in IT Infrastructure Upgrades:*

When implementing system upgrades or overhauls, the bank should adopt a security-by-design approach, ensuring that cybersecurity measures are embedded from the planning to the deployment stages. This minimizes the chances of introducing exploitable vulnerabilities during system transitions.

- *Adopt Secure Cloud Practices:*

Given the growing cybersecurity risks associated with cloud service adoption, the bank should partner with reputable cloud service providers and implement strong access controls, regular audits, and data encryption to safeguard sensitive information and maintain compliance with industry standards.

REFERENCES

[1]. Agwulonu, C., & Ijaseun, D. (2024). GTBank's cyber-attack: A wake-up call for Nigerian banks amid recapitalisation efforts. Retrieved from *https://businessday.ng/companies/article/ gtbanks-cyber-attack-a-wake-up-call-for-nigerian-banks-amid-recapitalisation efforts/#:~:text=In%20response%20to%20fears%20that,no%20customer%20data%20was%20compromised.* 6th April, 2025.

[2]. Ahmad, A., Maynard, S. B., & Park, S. (2021). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Strategic Information Systems, 30*(2),

[3]. Aina, D. (2024). GTB confirms hackers attempt to compromise website. Retrieved from *https://punchng.com/gtb-confirms-hackers-attempt-to-compromise-website/,* 6th April, 2025.

[4]. Alhassan, S., Olanrewaju, M. A., & Adewumi, A. M. (2021). Cybersecurity in Nigerian banks: Challenges and the way forward. Cybersecurity Review, 8(2), 123–135.

[5]. Ama, G.A.N., Onwubiko, C.O. and Nwankwo, H.A. (2024) Cybersecurity Challenge in Nigeria Deposit Money Banks. *Journal of Information Security,* 15, 494-523. https://doi.org/10.4236/jis.2024.154028

[6]. Anderson, R., Barton, C., & Miller, M. (2020). Cybersecurity risk management: The essentials of data protection. *Journal of Information Security,* 19(3), 25–34.

[7]. Aro-Lambo, B. (2024). Experts Explain Attacks As GTB Restores Website. Retrieved from *https://leadership.ng/experts-explain-attacks-as-gtb-restores-website/,* 6th April, 2025.

[8]. Central Bank of Nigeria (CBN). (2022). Annual report on cybersecurity risks and financial fraud in Nigerian banks. CBN Financial Review, 30(1), 15–29.

[9]. Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3), 319–340.

[10]. Enoruwa, O. K., Onwumere, J. U. J., & Ibunor, A. E. (2023). Impact of technological innovations on bank performance in selected West African Countries (1997-2020). *International Journal of Professional Business Review,* 8(8), 1-88. DOI: 10.26668/businessreview/2023.v8i8.2270

[11]. Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2021). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 101*.

[12]. IBM. (2022). *Cost of a Data Breach Report 2022*. Retrieved from https://www.ibm.com/security/data-breach

[13]. Ibrahim, S., & Adebayo, F. (2022). Technological Advancements and Information Security Challenges in Nigerian Banks. *Journal of African Information Technology Studies*, 14(3), 72–86.

[14]. ISO (2018). *ISO 31000:2018 Risk management—Guidelines*. International Organization for Standardization.
[15]. Kaplan, S., & Garrick, B. J. (1981). *On the quantitative definition of risk*. Risk Analysis, 1(1), 11-27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x
[16]. Liu, F., & Zhang, S. (2021). A study on cybersecurity risk management in financial institutions. *Journal of Financial Technology and Security,* 6(4), 45–58.
[17]. Mothobi, O., & Grzybowski, L. (2017). Infrastructure deficiencies and adoption of mobile money in Sub-Saharan Africa. *Information Economics and Policy, 40*, 71-79.
[18]. Müller, K., & Baumgartner, D. (2023). Digital Disruptions and Organizational Cybersecurity: A Cross-European Assessment. *European Journal of Information Systems*, 32(1), 44–60.
[19]. Nigerian Communications Commission (NCC). (2023). Annual report on cybersecurity threats and vulnerabilities in Nigeria's banking sector. *NCC Report on Cybersecurity,* 17(2), 41–53.
[20]. Nigerian Deposit Insurance Corporation (NDIC). (2022). Report on online banking fraud and cybercrime activities in Nigeria. *NDIC Cybersecurity Annual Review*, 12(2), 103–118.
[21]. Nigerian Inter-Bank Settlement System [NIBSS]. (2022). *Industry fraud report 2021*. Retrieved from *https://nibss-plc.com.ng*
[22]. Okamgba J. (2024). GTB channels attack heightens cybersecurity concerns. Retrieved from *https://punchng.com/gtb-channels-attack-heightens-cybersecurity-concerns/* , 6th April, 2025.
[23]. Olayemi, T., & Uchenna, M. (2021). The Impact of Digital Banking on Cybersecurity Risk in Nigerian Deposit Money Banks. *Nigerian Journal of Cybersecurity and Information Systems*, 9(1), 33–48.
[24]. Olokede, O. A., Salami, T. O., & Akinyemi, O. (2022). The impact of technological disruption on cybersecurity risks in Nigerian banks. *Journal of Banking and Cybersecurity*, 16(1), 45–59.
[25]. Pagani, M. (2020). Digital business strategy and value creation: framing the dynamic cycle of control points. *MIS Quarterly,* 37(2), 617 – 632.
[26]. PwC Africa. (2023). *Digital banking in Africa: The race for relevance*. Retrieved from https://www.pwc.com/ng/en/publications/digital-banking-in-africa.html
[27]. Saeed, S.; Altamimi, S.A.; Alkayyal, N.A.; Alshehri, E.; Alabbad, D.A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses' Resilience: Issues and Recommendations. Sensors 2023, 23(6666), 1-20. *https://doi.org/10.3390/ s2315666*
[28]. Samuel-Ogbu, I. (2022). Digital Technology and the Transformation of the Nigerian Banking System: The Operators' Perspective. *Central Bank of Nigeria Economic and Financial Review,* 60(4), 133-150. Retrieved from https://www.cbn.gov.ng/Out/2024/RSD/Digital%20 Technology%20and%20the.pdf
[29]. Sharma, R., & Khatri, D. (2022). Defining and managing cybersecurity risk: A comprehensive framework. Journal of Information Security, 28(1), 39–53.
[30]. Sharma, S., & Mukhopadhyay, A. (2020). Cloud computing: A catalyst for digital transformation and cybersecurity risk. *Information and Computer Security, 28*(2), 269-285.
[31]. Tadapaneni, N, R. (2020). Cloud computing security challenges. International journal of innovations in engineering research and technology (IJIERT), 7(6), 1 – 6.
[32]. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly,* 27(3), 425–478.
[33]. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems, 28*(2), 118-144.
[34]. Wang, V. Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice,* 62, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415.
[35]. Westerman, G., Bonnet, D., & McAfee, A. (2014). *Leading digital: Turning technology into business transformation*. Harvard Business Review Press.
[36]. Zhang, T., & Xie, P. (2021). Understanding cybersecurity risk: A system perspective. *Journal of Risk Analysis and Cybersecurity*, 4(3), 210–223.