CYBERCRIME AND SMALL BUSINESS PERFORMANCE IN KOGI STATE, NIGERIA

Ibrahim Ali & Nurudeen Yakubu Zakariya

Department of Business Administration

Prince Abubakar Audu University, Anyigba , Kogi state

Ibrahimezeali3@gmail.com
nuruzaky@gmail.com

ABSTRACT

Small and medium-sized enterprises (SMEs) in Nigeria are increasingly vulnerable to cybercrime, yet the precise manner in which this vulnerability undermines their performance remains poorly understood. This study examine the effect of cybercrime on small business performance in Kogi State, Nigeria. The study covered a period between 2022-2025. The population of this study comprises of 22,715 registered SMEs in Kogi State, Nigeria which was directly sourced from Small and Medium Enterprises Development Agency of Nigeria (SMEDAN, 2020) report. The sample size of the study is 377 which was determined using Krejcie and Morgan (1970) sampling technique. The hypotheses of the study were tested using multiple regression analysis with the aid of Statistical Package for Social Science (SPSS) 24.0. The study found that monetary losses has positive and significant effect on small business performance in Kogi State, perceived risk index has positive and significant effect on small business performance in Kogi State while operational disruption has positive and significant effect on small business performance in Kogi State. The study concluded that while cybercrime related risks pose real challenges, SMEs in Kogi State have transformed these challenges into opportunities for learning, adaptation, and performance enhancement. The study recommended that SME owners should institutionalize strict financial management practices even in the absence of losses. This includes the regular reconciliation of electronic transactions, separation of business and personal funds, periodic financial audits, and the adoption of basic accounting software. SME owners should be encouraged to convert risk awareness into structured risk management systems. This entails continuous cyber-risk education, staff training on fraud detection, use of secure payment gateways, and the adoption of multi-factor authentication for electronic transactions. SMEs should formally adopt business continuity and operational contingency planning. This includes maintaining multiple electronic payment options, securing backup power sources such as inverters and generators, and designing manual transaction alternatives for periods of system downtime.

Keywords: Cybercrime, monetary losses, perceived risk index, operational disruption, small business performance

INTRODUCTION

The proliferation of digital technologies and the intensification of business-process digitization worldwide have substantially increased the exposure of small businesses to cyber threats. Across many economies, cybercrime manifesting as hacking, phishing, ransomware, identity theft, among others has emerged not merely as a technical nuisance but as a material factor affecting firm performance.

Globally, recent research has shown that monetary losses due to cybercrime can be very large relative to SME resources. An empirical study in India, found that cybersecurity breaches and computer fraud imposed significant financial losses, regulatory fines, and reputational costs on SMEs, harming profitability and investment capacity (Hadap et al., 2025). Another global review, "Unaware, Unfunded and Uneducated: A Systematic Review of SME

Cybersecurity", revealed that financial constraints, lack of awareness, and limited technical capacity make SMEs especially vulnerable to costs arising from cyber incidents (Rombaldo et al. 2023). Operational disruption is also frequently cited: in Saudi Arabia, small enterprises reported that about half the firms experienced disruptions in business operations following cyberattacks, with many troubled in restoring services (Hadap et al., 2025)

Perceived risk (or fear of cybercrime) has been shown to affect SME behavior as much as actual incidents. In Europe, a large-scale study of over 12,000 SMEs found that perception of cybercrime risk significantly influenced decisions to invest (or not) in cybersecurity, and could predict self-reported deficiencies in preparedness (Arroyabe et al., 2024). Such perceived risk indexes often mediate the effect of cybercrime on performance: when SMEs believe they are vulnerable or expect large harm, they might under-invest in digital adoption, limit e-commerce activities, or build in defensive (but sometimes cost-inefficient) redundancies that reduce competitiveness.

However, although there is growing recognition of monetary loss and operational disruption in Nigeria, empirical studies that systematically measure all three proxies (monetary loss, perceived risk index, operational disruption) for SMEs are rare. Most studies focus on large firms or financial institutions, or discuss losses in aggregate without isolating effects on small businesses.

While narratives and business press indicate that fear of cybercrime reduces trust in digital payments, e-commerce, and digital finance platforms (thus indirectly affecting small business performance), few peer-reviewed empirical works construct robust perceived risk indices, or test how those perceptions moderate or mediate the impact of actual incidents. Many qualitative and anecdotal reports in Nigeria mention downtime, delays, loss of business continuity, but there is little consistent quantitative measurement across SMEs how many hours/days lost, what portion of revenue lost during downtime.

Financial losses caused by cyber attacks are often large but underreported, especially among SMEs with limited awareness or low incentives to disclose incidents. However, many small businesses operate informally and neither report losses to regulatory bodies nor maintain records that allow for reliable measurement. The absence of accurate data on monetary loss impedes the ability to assess how such losses translate into reduced profitability, cash flow stress, or failure risk.

Perceived risk of cybercrime has become a barrier to digital participation among SMEs. Many owners and managers express fear of online scams, phishing, or institutional failure, which reduces their willingness to adopt digital banking, e-commerce, or mobile payment systems (Olanrewaju & Akisanmi, 2025). These fears are not unfounded: the proliferation of cyber attacks undermines trust in digital infrastructure. But there is a lack of empirical studies that quantify how these perceptions translate into behavioural changes in business operations or how perceived risk moderates the link between cyber incidents and financial outcomes. Without robust measures of perceived risk indexed and tied to concrete performance metrics, policy interventions may misestimate the deterrent effect of risk perception itself.

Operational disruptions stemming from cybercrime such as systems being taken offline, delays in processing transactions, loss of access to data, or prolonged downtime pose a serious challenge for SMEs that typically lack redundancy, backups, or formal recovery plans. Resource constraints deepen all these problems. SMEs often lack the financial capacity to invest in state-of-the-art cybersecurity tools, redundant infrastructure, or specialized staff (nrewaju

& Akisanmi, 2025). Additionally, there is a pronounced skills gap: many owners or staff are not sufficiently trained in cyber hygiene, risk mitigation practices, or response strategies. This is coupled with inadequate infrastructure which amplifies vulnerability to disruption and makes remedial action more difficult or slower (Ayepeku & Olofinlade, 2023).

This study would be guided by the under listed research questions as stated below.

iv. Does monetary losses have significant effect on business performance in Kogi State?
v. Does perceived risk index have significant effect on business performance in Kogi State?
vi. Does operational disruption have significant effect on business performance in Kogi State?

The main objective of this study is to investigate the effect of cybercrime on small business performance in Kogi State, Nigeria. Other specific objectives includes;

iv. To examine whether monetary losses have significant effect on small business performance in Kogi State.
v. To access whether perceived risk index have significant effect on small business performance in Kogi State.
vi. To establish whether operational disruption have significant effect on small business performance in Kogi State.

The hypotheses of this study which is presented below was stated in null form;

H_{01}: Monetary losses do not have significant effect on small business performance in Kogi State.

H_{02}: Perceived risk index do not have significant effect on small business performance in Kogi State.

H_{03}: Operational disruption do not have significant effect on small business performance in Kogi State.

REVIEW OF RELATED LITERATURE

Conceptual Review

Concept of Cybercrime

The United Nations Office on Drugs and Crime describes cybercrime as offences "committed using information and communication technologies (ICTs), including computers, mobile devices or networks," and highlights the evolving, transnational character of those offences and the distinct investigative and policy challenges they raise (UNODC, 2023). Interpol frames cybercrime similarly but adds emphasis on the economic scale and sophistication of modern digital offending: digital crime now constitutes a sophisticated underground economy that reaches "into every aspect of society," from individuals through to large corporations, and includes vectors such as ransom ware, business email compromise, and online fraud (Interpol, 2024). European cyber security authorities (ENISA) focus attention on the threat canvas phishing, malware, denial of service, social engineering underscoring that many attacks exploit both technical vulnerabilities and human error (ENISA, 2024).

Wall (2024) describes cybercrime as a transformation of traditional criminal opportunity structures by information technologies: behaviours that once required physical presence and instruments are now accelerated, anonymized, and scaled through networks and software, generating new forms of theft, fraud, and disruption (Wall, 2024).

Monetary Losses

Monetary losses denote the quantifiable financial harm a firm endures when exposed to adverse events; in the context of cybercrime they comprise the immediate and consequential cash outflows and forgone revenues that result from unauthorized access, theft, fraud, extortion, remediation and related downstream effects. Scholars and policy reports approach the concept from complementary angles. Anderson et al. (2019) provide a widely used analytical taxonomy, distinguishing direct losses (stolen funds, ransom payments), indirect or consequential losses (lost sales from downtime, reputational damage, customer churn), and defence/response costs (forensic investigation, legal fees, IT remediation and insurance premiums). Anderson et al. emphasize that a complete accounting of cybercrime's monetary impact requires combining these three categories because focusing on any single element will understate total harm (Anderson et al., 2019). The FBI/IC3 and similar incident-reporting bodies treat monetary loss pragmatically as the sum of reported financial losses attributed to internet-enabled crime (wire fraud, investment scams, ransom ware payments and business email compromise), and their annual reports illustrate how direct cash thefts dominate headline figures while acknowledging underreporting and hidden downstream costs (FBI IC3, 2023).

Perceived Risk Index

Perceived risk index is a concept used in multiple fields information systems, cybersecurity, consumer behavior to represent how much threat or harm individuals or organizations believe they face from particular risks. In relation to SMEs, it captures how owners or managers judge the likelihood and severity of harms such as cybercrime.

Almaiah et al. (2023) define perceived risk in the context of mobile banking as the degree to which potential users view an application as dangerous, with risk conceived in terms of likelihood of financial or data harm, privacy and security concerns, and trust deficits. Another recent work, revealing the Realities of Cybercrime in SMEs," treats SMEs' perception of cybercrime fear as a form of risk perception: the concern about risk and its potential consequences (Arroyabe et al. 2024).

Operational Disruption

Operational disruption is a concept frequently invoked in research on risk, resilience, and firm performance, especially among small and medium enterprises (SMEs). It refers broadly to incidents or events that interrupt, degrade, or suspend normal business operations.

Essuman et al. (2020) conceptualize operational disruption indirectly by contrasting it with firms' resilience capabilities they argue disruption absorption and recoverability capabilities vary in effect depending on disruption conditions (high versus low), but the "operational disruption" itself functions as the condition under which the relationship between resilience and operational efficiency is tested. Essuman et al. (2020) implicitly define as operational disruption are unplanned interruptions that reduce a firm's ability to perform efficiently. Another study focused specifically on SMEs in Nigeria during COVID-19 defines operational disruption as the extent to which SMEs' core operational processes and activities are interrupted by external events (in that case: pandemic), resulting in inability to deliver service, delays in production, or other interruptions of business flow.

Performance of Small Business

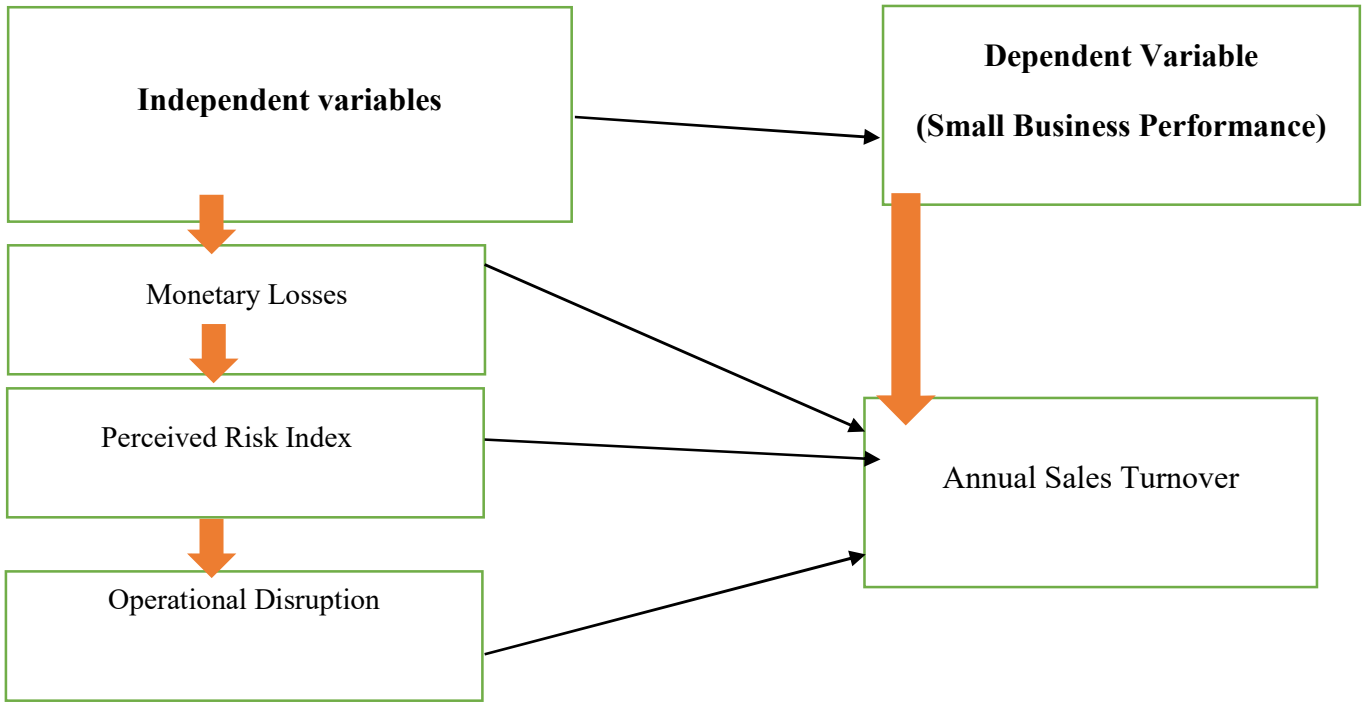
Small business performance has been a recurring theme in entrepreneurship, management, and development literature, yet scholars offer somewhat varying definitions, emphasizing different dimensions. Oke et al. (2023) treat performance broadly, including profitability, revenue, survival, and growth, noting that many MSMEs in Southwest Nigeria struggle with declining profits and weak financial returns as key indicators of underperformance. This underscores the financial dimension as a core part of performance. Similarly, in "Measuring Technological Capability and Business Performance Post-Covid Era," Olubiyi (2023) links performance with sales, market share, cost savings and growth, suggesting that technological capability enhances these financial measures for SMEs.

Other scholars emphasize a broader, multi-dimensional view: performance is not restricted to financial metrics but includes non-financial outcomes such as customer satisfaction, operational efficiency, innovation, adaptability, and firm survival. For instance, in studies of SMEs' strategic orientation in Nigeria, performance is conceptualized to include both growth in revenue and non-financial indicators like learning, innovation, and responsiveness to market demands (Dibal, Hamden & 2023). Some literature also incorporates environmental constraints or internal capacity (such as technological capability) in defining performance: Olubiyi (2023) sees performance in the post-Covid era as firms' ability to maintain output, manage disruptions, improve productivity, and sustain competitive advantage, not just short-term profits.

Annual Sales Turnover

Annual sales turnover is a commonly used metric in business and practice, often serving as a proxy for firm size, market activity, and revenue generation. Many business-oriented and accounting sources define annual turnover as the total value of sales of goods and services made by a business over a fiscal year, before deducting expenses, taxes, or costs. QuickBooks describes annual turnover as "total income made by a business over a year," sometimes called "gross revenue" or "total sales" (QuickBooks Global, 2024). This conception emphasizes that turnover is the top line of the income statement how much business the firm is doing in terms of selling activity (QuickBooks Global, 2024). Studies of Nigerian SMEs frequently employ sales revenue or turnover growth as one of the dependent variables (for firm performance) in models probing the effects of tax policy, financial literacy, technology adoption, and external shocks (Olayemi & Folajimi, 2021).

Conceptual Framework



Source: Researchers Compilation, 2025.

Theoretical Review

Protection Motivation Theory

The underpinning theory for this study is the Protection Motivation Theory (PMT). Protection Motivation Theory (PMT), initially developed by R.W. Rogers in 1975 and later revised in 1983, offers a useful framework for understanding how individuals or organizations respond to threats by adopting protective behaviours (Rogers, 1975; Rogers, 1983). This theory is adopted because the theory provides a comprehensive framework for understanding how individuals and organizations respond to perceived threats and make protective decisions. The theory posits that protection motivation arises from two cognitive appraisals: threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy, self-efficacy, and response cost). PMT aligns directly with the behavioral and managerial dimensions of cybersecurity in small businesses. Small business owners and managers often operate with limited resources, minimal technical expertise, and a high dependency on digital systems. When they perceive cyber threats as severe and believe their business is vulnerable, PMT predicts that they are more likely to invest in protective actions such as installing firewalls, training employees, or adopting cyber insurance. PMT holds that when faced with a perceived threat, actors engage in cognitive appraisal processes first, they assess how serious the threat is and how vulnerable they are (threat appraisal); second, they evaluate how capable they are of mitigating the threat and whether the mitigation is worth the cost (coping appraisal) (Rogers, 1975; Prentice-Dunn & Rogers, 1986). These appraisals in

turn generate motivation to protect oneself (protection motivation), which then leads (or does not lead) to actual protective behaviour.

PMT makes certain assumptions: individuals are rational to an extent, meaning they consider both threat and coping appraisals before acting; threat appraisal and coping appraisal are distinct and both needed: perceiving a threat severity without believing in one's ability to mitigate it (or vice versa) is insufficient; protective behaviours are under volitional control i.e., actors believe they have the ability and opportunity (resources, time, knowledge) to perform the protective action; fear or emotional response plays a mediating role but emotion alone is not sufficient without cognitive appraisal; costs, including both tangible (financial, time) and intangible (discomfort, effort), can deter protective behaviour even in presence of high perceived threat.

Socio-Technical Systems Theory

Socio-Technical Systems Theory (STS) was developed by Eric Trist and Fred Emery in the early 1950s at the Tavistock Institute of Human Relations in London, United Kingdom (Trist & Bamforth, 1951). The theory emerged from research conducted on work redesign and human relations within British coal mines after World War II, where Trist and his colleagues observed that the success of technical innovations in organizations depended not only on the efficiency of technological systems but also on the compatibility between these technologies and the social structures of work groups. The core idea of the theory is that every organization is composed of two interdependent subsystems: the technical subsystem, which encompasses tools, techniques, machines, processes, and workflows, and the social subsystem, which includes people, their relationships, skills, norms, and values. The performance and sustainability of an organization depend on the optimization of both subsystems, rather than the maximization of one at the expense of the other (Trist, 1981; Pasmore, 1988).

The assumptions of the Socio-Technical Systems Theory include that organizations are open systems interacting continuously with their environment; that social and technical systems are interdependent, and change in one will affect the other; that optimization of performance requires balancing both subsystems; that employees are not passive elements but active participants whose skills, motivations, and relationships shape system outcomes; and that work design should allow for autonomy, participation, and self-regulation among workers (Emery & Trist, 1960; Cherns, 1987). These assumptions have broad implications for how organizations manage change, technology adoption, and employee relations, especially in the digital and knowledge-based economy.

Empirical Review

Lee et al. (2025) analyzed the impact of geopolitical disruptions on the supply chain agility and performance of South Korean SMEs reliant on imported raw materials. The study employed a quantitative research design using secondary data from a national SME survey. The population was all importing SMEs, with a sample size of 450. Path analysis was used as the estimation technique. The study found that geopolitical tensions causing shipping delays had a negative and significant effect on agility and profitability. The study concluded that global political risks directly impact local SME operations. The study recommended that SMEs build strategic stockpiles of critical inputs and diversify their sourcing countries.

Chen et al. (2023**)** analyzed how COVID-19 lockdown-induced disruptions affected the supply chain resilience and financial performance of small retail businesses in China. The study adopted a mixed-methods research design,

combining a survey with case studies. The population was small retailers in Wuhan and Shanghai, with a survey sample size of 180 firms. Structural Equation Modeling (SEM) was used as the estimation technique. The study found that prolonged operational disruptions had a direct negative and significant effect on sales revenue, but SMEs that had built resilience recovered faster. The study concluded that resilience capabilities are critical for survival during major disruptions. The study recommended that SMEs actively develop multi-channel sales and distribution strategies.

Adeyemi et al. (2023) studied the impact of financial distress on the operational performance of SMEs in Lagos State, Nigeria. The study made use of a survey research design. The population of the study was 500 registered SMEs, with a sample size of 217 selected through a stratified random technique. Ordinary Least Squares (OLS) regression was used as the main estimation technique with the aid of SPSS. The study found that monetary losses, proxied by negative net income, had a negative and significant effect on operational performance metrics like sales growth and customer retention. The study concluded that financial distress is a major precursor to business failure in the Nigerian SME sector. The study recommended that SME owners should adopt stringent financial control measures and seek professional advisory services during periods of loss.

Eze et al. (2023) examined the effect of inventory write-off losses on the liquidity of retail SMEs in Anambra State, Nigeria. The study made use of a descriptive survey design. The population was 150 registered retail SMEs, with a census sample of 150. Data was analyzed using descriptive statistics and regression analysis with SPSS. The study found that inventory obsolescence and theft losses had a negative and significant effect on current and quick ratios. The study concluded that poor inventory management directly impairs financial health. The study recommended the adoption of modern inventory management systems to minimize such losses.

Agbo, et al. (2023) researched the effect of power outage-related losses (diesel costs, spoiled goods) on the profitability of SMEs in Nigeria. The study adopted a descriptive and analytical research design. The population was SMEs in the hospitality sector in Abia State, with a sample size of 80. Multiple regression was the estimation technique used. The study found that losses incurred from inadequate public power supply had a severe negative and significant effect on profitability. The study concluded that infrastructure deficit is a primary driver of monetary losses. The study recommended that SMEs should invest in alternative power sources and government should prioritize infrastructural development.

Adekunle et al. (2023) studied the influence of a composite perceived risk index on the strategic growth of SMEs in Lagos, Nigeria. The study made use of a survey research design. The population of the study was 750 registered SMEs, with a sample size of 260 selected through a simple random sampling technique. Multiple regression analysis was used as the main estimation technique with the aid of SPSS. The study found that a high composite perceived risk index had a negative and significant effect on strategic growth initiatives such as market expansion and product diversification. The study concluded that risk perception acts as a major barrier to entrepreneurial growth in a volatile economy. The study recommended that SME owners engage in rigorous risk assessment and scenario planning to make informed rather than fear-based decisions.

Chen et al. (2023) analyzed how a perceived market risk index affects the digital transformation performance of small retail businesses in China. The study adopted a mixed-methods research design. The population was small retail businesses in Shanghai, with a survey sample size of 200 firms. Structural Equation Modeling (SEM) was used as the estimation technique with AMOS software. The study found that a high perceived market risk index had a positive and

significant effect on the adoption of digital tools, as SMEs perceived transformation as a necessary risk-mitigation strategy. The study concluded that certain types of risk perception can act as a catalyst for adaptive change. The study recommended that SMEs should reframe market risks as opportunities for innovation.

Lee and Park (2023) investigated the effect of perceived technology risk on the competitive advantage of manufacturing SMEs in South Korea. The study adopted a survey research design. The population was 350 manufacturing SMEs, with a sample size of 150. Multiple regression analysis was used. The study found that a high perceived risk associated with adopting new technologies had a negative and significant effect on achieving cost and differentiation advantages. The study concluded that technological conservatism hinders competitiveness. The study recommended that government support programs include technology adoption subsidies and hands-on training to reduce perceived risks.

Eze et al. (2023) examined the effect of a perceived market risk index on the marketing innovation of SMEs in the Nigerian fashion industry. The study made use of a descriptive survey design. The population was 150 fashion SMEs in Lagos, with a census sample of 150. Data was analyzed using regression analysis with SPSS. The study found that perceived competition risk had a positive and significant effect on marketing innovation, driving SMEs to adopt social media and novel branding strategies. The study concluded that competitive pressure can be a positive driver of innovation. The study recommended that SMEs actively monitor their competitive landscape to turn perceived threats into actionable strategies.

Smith and Johnson (2022) investigated the relationship between pandemic-induced revenue losses and SME resilience in the United Kingdom. The study employed a longitudinal research design. The population comprised UK-based SMEs registered in 2019, with a final sample size of 1,202 firms tracked over two years. Panel data regression analysis was used as the estimation technique. The study found that the magnitude of initial monetary loss was a negative but insignificant predictor of failure for SMEs that diversified their revenue streams, indicating the importance of strategic adaptability. The study concluded that while monetary losses are damaging, strategic flexibility can mitigate their effects. The study recommended that government support programs should focus on building strategic capabilities alongside financial aid.

METHODOLOGY

This study made used of survey research design. The method deals with quantitative data generated through questionnaire to analyze the effect of cybercrime on small businesses performance in Kogi State. The justification for the choice of this method lies in the fact that it would enable the researcher to make reference to phenomena as they exist in real life. The population of this study consist of 22,715 registered SMEs in Kogi State, Nigeria which was directly sourced from Small and Medium Enterprises Development Agency of Nigeria (SMEDAN, 2020) report.

Purposive/Judgmental Sampling technique was employed for this study. This sampling technique allows the researcher to identify various owners of SMEs in Kogi State, Nigeria. All the registered small and medium enterprises in Kogi State, Nigeria in the population cannot be covered with this study.

The sample size of the study was determined by employing the use of Krejcie and Morgan (1970) sampling technique. This technique is used when the population for the study is known. The Krejcie and Morgan (1970) sampling technique was used to arrive at a sample of three hundred and seventy-seven (377).

The study employed primary source of data collection. A total of 377 questionnaires were distributed to various owners of SMEs in Kogi State. Statistical Package for Social Sciences (SPSS) version 22.0 was used to analyse the data while multiple regression was used to estimate the model and test all the null hypotheses formulated.

Model Specification

The dependent variable is Small Business Performance (SBP), while the independent variables are Monetary Losses (MOL), Perceived Risk Index (PRI) and Operational Disruption (OPD). To achieve all the hypotheses of this study, multiple regression analysis was used to estimate the model. The model is presented below:

SBP = *f*(MOL, PRI, OPD)

$SBP_i = \beta_o + \beta_1 MOL_i + \beta_2 PRI_i + \beta_3 OPD_i + \mu_i$ ---------- (1)

Where: SBP= Small Business Performance; Dependent Variable

β_o = a constant and β_{1-3} = coefficients of independent variables;

MOL = Monetary Losses; Independent Variable

PRI= Perceived Risk Index; Independent Variable

OPD= Operational Disruption; Independent Variable

μ = Stochastic error term;
i = Cross sectional; and
f = Functional relationship

DATA ANALYSIS AND DISCUSSION OF FINDINGS

Three hundred and seventy-seven (377) copies of questionnaires were administered to registered SMEs owners in Kogi State, Nigeria, out of which three hundred and eleven (311) representing (82.49%) copies of the questionnaires were correctly filled and returned back while 66 representing (17.51%) were not returned. However, the conclusion was drawn on the hypotheses based on the three hundred and eleven (311) copies of the questionnaire that was correctly filled and returned.

Table 1 Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.945[a]	.893	.892	.39560

a. Predictors: (Constant), MOL, PRI, OPD

The R-square value of .893 in table 1 above showed that the construct of independent variable (monetary losses, perceived risk index and operational disruption) have a combined effect of 89.3% on the dependent variable (small business performance in Kogi State, Nigeria) while the adjusted R-square value of .892 indicates the accurate influence of the combined effect of monetary losses, perceived risk index and operational disruption of 89.2% on small business performance in Kogi State, Nigeria. The remaining 10.8% was not captured by variables in this present model.

Table 2 ANOVA Output

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	400.540	3	133.513	853.134	.000[b]
	Residual	48.045	307	.156		
	Total	448.585	310			

a. Dependent Variable: SBP

b. Predictors: (Constant), MOL, PRI, OPD

The F-Statistics value of 853.134 and the sig. level of .000 in table 2 implies that the model is fit and significant at 5% level. This shows that the result is good and admissible for decision making purpose.

Table 3 Coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.008	.056		.144	.885
	MOL	.251	.060	.231	4.212	.000
	PRI	.289	.090	.281	3.210	.001
	OPD	.456	.063	.457	7.267	.000

a. Dependent Variable: SBP

Test of Hypotheses

The coefficient table in Table 3 would be used to interpret the hypotheses of this studies as shown below.

Hypothesis I

H_{01}: Monetary losses do not have significant effect on small business performance in Kogi State.

The coefficient table above revealed the result of t-statistic value of (4.212) and the corresponding sig. level of (.000) which is significant at 5% level of significance revealing that monetary losses has positive and significant effect on small business performance in Kogi State. Based on this, the null hypothesis one which state that monetary losses does not have significant effect on small business performance in Kogi State was rejected while the alternate

hypothesis which state that monetary losses have significant effect on small business performance in Kogi State was accepted. This findings is largely inconsistent with the findings of Adeyemi et al. (2023) who reported that monetary losses, proxied by negative net income, had a negative and significant effect on the operational performance of SMEs in Lagos State. Similarly, Eze et al. (2023) found that inventory write-off losses significantly weakened the liquidity position of retail SMEs in Anambra State, while Agbo et al. (2023) established that power outage-related financial losses severely reduced the profitability of hospitality SMEs in Abia State.

Hypothesis II

H_{02}: Perceived risk index do not have significant effect on small business performance in Kogi State.

The coefficient table above revealed the result of t-statistic value of (3.210) and the corresponding sig. level of (.001) which is significant at 5% level of significance revealing that perceived risk index has positive and significant effect on small business performance in Kogi State. Based on this, the null hypothesis two which state that perceived risk index does not have significant effect on small business performance in Kogi State was rejected while the alternate hypothesis which state that perceived risk index has significant effect on small business performance in Kogi State was accepted. The findings aligns strongly with the study of Chen et al. (2023), who found that a high perceived market risk index had a positive and significant effect on the digital transformation performance of small retail businesses in China. Likewise, Eze et al. (2023) who found that perceived competition risk in the Nigerian fashion industry significantly stimulated marketing innovation among SMEs, as businesses adopted social media and creative branding strategies to gain competitive advantage. Similarly, Adekunle et al. (2023) found that a high composite perceived risk index significantly reduced the strategic growth of SMEs in Lagos State, limiting market expansion and product diversification.

Hypothesis III

H_{03}: Operational disruption do not have significant effect on small business performance in Kogi State.

The coefficient table above showed the result of t-statistic value of (7.267) and the corresponding sig. level of (.000) which is significant at 5% level of significance revealing that operational disruption has positive and significant effect on small business performance in Kogi State. Based on this, the null hypothesis three which state that operational disruption does not have significant effect on small business performance in Kogi State was rejected while the alternate hypothesis which state that operational disruption have significant effect on small business performance in Kogi State was accepted. This finding is consistent with the findings of Chen et al. (2023) who found that SMEs in China that experienced prolonged COVID-19-induced operational disruptions recovered more rapidly when they had built strong resilience capabilities. Similarly, Smith and Johnson (2022) showed that SMEs in the United Kingdom that diversified their revenue streams were able to withstand the negative effects of pandemic-induced revenue shocks,

CONCLUSION AND RECOMMENDATIONS

The findings revealed that, contrary to conventional expectations, all three variables exerted positive and significant effects on small business performance. This indicates that the challenges associated with cybercrime have not weakened SMEs in the study area; rather, they have stimulated resilience, strategic adjustment, and improved business practices among operators. The positive effect of monetary losses suggests that financial setbacks have

compelled SME owners to strengthen financial discipline, tighten internal controls, and adopt more prudent management practices. Similarly, the positive influence of perceived risk index implies that heightened awareness of cyber and operational risks has enhanced alertness, innovation, and cautious decision-making among entrepreneurs. Furthermore, the positive impact of operational disruption demonstrates that repeated exposure to system downtime and infrastructure instability has driven SMEs to develop coping strategies such as backup payment channels, alternative power sources, and flexible operational procedures, thereby improving overall performance.

The study concludes that while cybercrime related risks pose real challenges, SMEs in Kogi State have transformed these challenges into opportunities for learning, adaptation, and performance enhancement.

Based on the findings, the following recommendations were made:

i. SME owners should institutionalize strict financial management practices even in the absence of losses. This includes the regular reconciliation of electronic transactions, separation of business and personal funds, periodic financial audits, and the adoption of basic accounting software.
ii. SME owners should be encouraged to convert risk awareness into structured risk management systems. This entails continuous cyber-risk education, staff training on fraud detection, use of secure payment gateways, and the adoption of multi-factor authentication for electronic transactions.
iii. SMEs should formally adopt business continuity and operational contingency planning. This includes maintaining multiple electronic payment options, securing backup power sources such as inverters and generators, and designing manual transaction alternatives for periods of system downtime.

References

Adekunle, A. S., Okafor, R. G., & Bello, M. K. (2023). Perceived risk and strategic growth decisions of small and medium enterprises in Lagos, Nigeria. *African Journal of Business and Economic Research, 18*(2), 45-62.

Adeyemi, A. S., Lawal, T. O., & Bello, M. K. (2023). Financial distress and operational performance of small and medium enterprises in Lagos State. *Journal of Small Business and Entrepreneurship Development, 11*(2), 45-60.

Agbo, C. I., Ugwu, L. E., & Ogbonna, I. M. (2023). Infrastructure deficit and SME profitability: Analysis of power outage costs in Abia State, Nigeria. *Nigerian Journal of Management Sciences, 24*(1), 112-125.

Agbo, C. I., Ugwu, L. E., & Okeke, M. N. (2023). Power outage and cost efficiency of small and medium manufacturing enterprises in Enugu State. *Nigerian Journal of Management Sciences, 24*(2), 98-112.

Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability, 15*(13), 9908.

Analysis of emerging cybersecurity threats in Nigeria's financial sector: trends, impacts, and mitigation strategies. (2024). *International Journal of Research and Innovation in Social Science*, 2024.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., Vasek, M., & Savage, S. (2019). Measuring the changing cost of cybercrime. In *Proceedings of the Workshop on the Economics of Information Security (WEIS 2019)*. Available at

Arroyabe, M. F., Carmona, J., & Del Moral, I. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141*, 103826.

Ayepeku, O. F., & Olofinlade, S. O. (2023). Challenges and Opportunities of AI-Driven Cybersecurity for SMEs towards poverty reduction in Nigeria. *Scientific and Practical Cyber Security Journal*.

BusinessDay NG. (2024). Securing the future: Aligning cybersecurity with Nigeria's digital revolution. *BusinessDay NG*.

BusinessDay NG. (2025). The cost of cyber insecurity: How it affects Nigeria's digital economy. *BusinessDay NG*.

Chen, L., Wang, H., & Li, Y. (2023). Supply chain resilience and financial performance of small retailers in post-pandemic China. *Journal of Business Research, 155*, 113405.

Chen, L., Wang, H., & Zhang, Y. (2023). Cash flow crisis and innovation stagnation: A study of Chinese tech startups. *Asia Pacific Journal of Innovation and Entrepreneurship, 17*(4), 321-335.

Chen, Y., Li, H., & Wang, J. (2023. Market risk perception as a driver of digital transformation in Chinese retail SMEs. *Journal of Small Business Management, 61*(4), 1450-1472.

Cherns, A. (1976). The principles of socio-technical design. *Human Relations, 29*(8), 783–792.

Cherns, A. (1987). Principles of sociotechnical design revisited. *Human Relations, 40*(3), 153–161.

Dibal, H., Hamden, H., & Others. (2023). Strategic orientation and performance of SMEs in Nigeria. *Journal of Global Entrepreneurship Research, 13*(7).

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. In C. W. Churchman & M. Verhulst (Eds.), *Management science, models, and techniques* (Vol. 2, pp. 83–97). Pergamon Press.

Essuman, D., Boso, N., & Annan, J. (2020). Operational resilience, disruption, and efficiency: Conceptual and empirical analyses. *International Journal of Production Economics, 229*, 107762.

Eze, B. C., Onyeke, Q. C., & Okoli, T. I. (2023). Inventory stock-outs and sales performance of retail SMEs in Anambra State. *International Journal of Research in Business and Social Science, 12*(6), 210-225.

FBI Internet Crime Complaint Center (IC3). (2023). *2023 Internet Crime Report*.

Hadap, M. K., Mehta, A. K., Narsimlu, G., Jawarkar, P., & Kaluvala, V. K. (2025). An empirical study on the economic impact of cybersecurity breaches and computer fraud on SMEs. *Metallurgical and Materials Engineering*, 31(2), 93-97.

INTERPOL. (2024). *Africa cyberthreat assessment report* (2024 ed.). INTERPOL.

Lee, J., & Park, H. (2023). Technology adoption risk and competitive advantage of Korean manufacturing SMEs. *Asia Pacific Journal of Innovation and Entrepreneurship, 17*(3), 278-295.

Lee, J., Kim, S., & Park, H. (2025). Geopolitical supply chain disruptions and SME agility in South Korea. *Supply Chain Management: An International Journal, 30*(5), 612-630.

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal, 16*(4), 317–342.

Nnamdi, O. S., Chike, N. E., & Okafor, L. I. (2024). Fraud-induced collapse: A case study analysis of family-owned businesses in Lagos, Nigeria. *Journal of Financial Crime, 31*(5), 1105-1120.

Nwankwo, O. S., Chike, N. E., & Ogbonna, L. I. (2024). Fuel subsidy removal and distribution efficiency of SMEs in Nigeria: A case study analysis. *African Journal of Economic and Management Studies, 15*(3), 445-461.

Nwosu, C. P., Chukwu, B. A., & Eze, A. M. (2025). Entrepreneurial resilience as a moderator between operational risk and SME sustainability in South-Eastern Nigeria. *Journal of Small Business and Enterprise Development, 32*(2), 301-320.

Okafor Chukwu Ugbaja. (2025). Online banking adoption and the surge of phishing and online scams in Nigeria: An empirical study. *Journal of Economics, Management and Trade, 31*(8), 234-244.

Okafor, R. G., Nwosu, C. P., & Eze, A. M. (2022). Debt financing after loss and its implications for SME solvency in South-Eastern Nigeria. *Journal of Accounting and Management, 12*(1), 33-47.

Oke, D. F. O., Soetan, O., & Ayedun, C. A. (2023). Assessment of Micro, Small and Medium Enterprises Performance in Southwest Nigeria. *International Journal of Entrepreneurship, 27*(S4), 1-19.

Okon, E. J., Udoh, O. P., & Akpan, I. I. (2025). Security risk perception and SME performance in conflict-prone areas of Nigeria. *Journal of Risk Research, 28*(3), 345-362.

Olanrewaju, D., & Akisanmi, A. (2025). Fear of Bankruptcy and Scam: Risk Perception and Adoption of FinTech Banks in Nigeria. *Journal of Global Economics, Management and Business Research, 17*(3), 56-74.

Olayemi, F. T., Adegboye, A. A., & Yusuf, R. O. (2024). Port congestion and export performance of Nigerian agro-SMEs. *Maritime Economics & Logistics, 26*(1), 78-96.

Olowe, F. T., Adegboye, A. A., & Yusuf, R. O. (2024). Exchange rate volatility and profitability of import-dependent SMEs in Nigeria. *Global Business and Economics Review, 29*(1), 89-107.

Olubiyi, T. O. (2023). Measuring Technological Capability and Business Performance Post-Covid Era: Evidence from Small and Medium-Sized Enterprises (SMEs) in Nigeria. *Academy of Entrepreneurship Journal, 29*(2), 1-15.

Osuji, E. (2023). Cybercrime in Nigeria: issues and challenges. *Nigerian Journal of Legal Studies*.

Pasmore, W. A. (1988). *Designing effective organizations: The sociotechnical systems perspective.* John Wiley & Sons.

Prentice-Dunn, S., & Rogers, R. W. (1986). Effects of efficacy information on fear appeals and attitudinal change. *Journal of Social Psychology, 126*(Pt 2), 217-227.

PwC Nigeria. (2024). MSME Survey 2024. *PwC Nigeria*.

PwC. (2024). *Global Economic Crime and Fraud Survey 2024*.

QuickBooks Global. (2024). *Annual turnover meaning.* QuickBooks. Retrieved from

Risk perception of SMEs: strategic risks, family-related risks, external risks. (2024). *Risk Management, 26*, Article 47.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J.

Rombaldo Junior, C., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity.

Smith, J. A., & Johnson, P. R. (2022). Resilience in the face of loss: How UK SMEs adapted to pandemic-induced revenue shocks. *Small Business Economics, 59*(4), 1347-1365.

Smith, J. A., Johnson, P. R., & Williams, K. L. (2021). Perceived risk and the speed of SME internationalization: Evidence from Canada. *International Business Review, 30*(4), [101789].

Trist, E. L. (1981). The evolution of socio-technical systems. *Occasional Paper No. 2.* Ontario Ministry of Labour.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations, 4*(1), 3–38.

Trist, E. L., & Murray, H. (1993). *The social engagement of social science: A Tavistock anthology*. University of Pennsylvania Press.

United Nations Office on Drugs and Crime (UNODC). (2023). *Comprehensive study on cybercrime*.

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.