IJAAR PUBLISHING®

Open Access Journal of Business and Entrepreneurship | ISSN: 3027-0855
Vol. 4, Issue 1 (2026) | www.ijaar.org

HEXAGON MODEL AND CYBER FRAUD OF LISTED COMMERCIAL BANKS IN NIGERIA

Ugwu, Hope Ifeyinwa and Egbunike, Patrick A.
Department of Accountancy
Nnamdi Azikiwe University, Awka
email; hi.ugwu@unizik.edu.ng; pa.egbunike@unizik.edu.ng

Abstract
The study ascertained the effect of hexagon model on cyberfraud in listed commercial banks in Nigeria, using rationalization and capability as the independent variables. A sample size of 396 respondents was determined through Yaro Yamene from a population of 43,583 and selected through stratified sampling to ensure proportional representation. Rational Choice Theory was used as the theoretical anchorage because of its high relevance to the hypotheses guiding the study. The findings revealed that rationalization has a significant and positive effect on cyberfraud in the listed commercial banks in Nigeria ($\beta = 0.128$, $p = 0.045$); and capability has a significant and positive effect on cyberfraud in the listed commercial banks in Nigeria ($\beta = 0.259$, $p = 0.007$). The study recommended among others that compliance officers and ethics units should organize regular ethics training and awareness programs that reinforce zero tolerance for fraud, regardless of justification. These programs should help employees understand the legal, financial, and reputational damage of fraud, thereby discouraging them from justifying unethical behavior through rationalization.

Key words: Cyberfraud, Rationalization and Capability

Ugwu, H. I. & Egbunike, P A. (2026). Hexagon model and cyber fraud of listed commercial banks in Nigeria. *Open Access Journal of Business and Entrepreneurship. 4*(1), 6-21. https://doi.org/10.46654/kdwgcp08

Introduction

In today's business environment, cyber security has emerged as a critical component of organizational resilience, particularly in sectors like banking where data security is paramount. The hexagon model, which consists of six key dimensions—pressure, opportunity, rationalization, capability, arrogance and collusion (Jajere, Ngerebo & Adebisi, 2025)—provides a comprehensive framework for analyzing the underlying factors that contribute to cyber security threats. Each of these dimensions plays a crucial role in shaping an organization's risk landscape. For example, "pressure" refers to financial pressures on employees or external actors that lead to malicious actions, while "opportunity" involves the availability of system vulnerabilities that can be exploited. In the banking sector, where vast amounts of data and financial resources are at stake, the hexagon model's relevance becomes even more pronounced. By adopting a holistic approach to cyber security that addresses both internal and external threats, commercial banks can create more resilient systems capable of withstanding sophisticated attacks. The adoption of the hexagon model in analyzing cyber security challenges highlights the importance of considering human factors alongside technical vulnerabilities in today's complex business domain.

Cybercriminals exploit weaknesses in outdated software, unpatched systems, and human factors, such as insider threats or employee negligence (Wang, Nnaji & Jung, 2020). Additionally, the rapid digital transformation of the banking sector has outpaced the development of adequate security measures, leaving gaps in the system that cybercriminals can exploit. Consequently, cyber-attacks on commercial banks can lead to significant financial losses, both for the institutions themselves and for their customers. Beyond the immediate monetary damage, these breaches erode public trust in the banking system, undermining customer confidence and potentially leading to reputational harm. In some cases, large-scale attacks can destabilize the financial sector, disrupting economic activities and threatening the overall stability of the financial system. It is in response to addressing this problem that the present study is being carried out to examine the relationship between hexagon model and cyber security threat in Nigerian commercial banks. Against the backdrop, this study therefore, ascertains the extent hexagon model affected cyber security threat in listed commercial banks in Nigeria. The specific objectives are as follows:

1. To determine the proportionate influence of rationalization on cyberfraud in listed commercial banks with international authorization in Nigeria.
2. To examine the effect of capability on cyberfraud in listed commercial banks with international authorization in Nigeria.

Review of Related Literature

Cyber Crime

One of the primary goals of cybersecurity threats is to breach the confidentiality of sensitive data, such as customer information, financial records, intellectual property, and classified government documents (Chhabra & Prabhakaran, 2024). This could be achieved through techniques like hacking, phishing, or data exfiltration, where attackers gain unauthorized access to systems or steal information for malicious purposes. Another critical aspect of cybersecurity threats involves the integrity of the data—attacks may aim to manipulate or alter information to serve the attackers' objectives, such as tampering with financial records, spreading misinformation, or damaging an organization's credibility. Additionally, attacks may target the availability of systems and services, denying users access to critical resources through methods like distributed denial-of-service (DDoS) attacks or system hijacking, which

can cripple an organization's ability to function (Almomani, Shehab, Al Ebbini, & Shami, 2021).

Rationalization

Rationalization is the psychological process through which individuals justify or excuse their involvement in unethical behavior, often by minimizing the perceived wrongdoing, distorting reality, or reframing the situation (Mohd & Awang, 2022). This cognitive process allows individuals to reconcile their actions with their internal moral standards, even when they are engaging in behavior that contradicts those standards (Djaelani, Zainuddin, & Mokoginta, 2022). In the context of fraud or cybercrime, rationalization plays a significant role in helping individuals overcome any feelings of guilt or moral conflict associated with their actions (Andrew, Candy, & Robin, 2022). For example, someone who commits fraud might tell themselves that they are simply "borrowing" money or data, with plans to repay it later, or that their actions are insignificant compared to the harm caused by the organization itself.

In the context of cybersecurity, rationalization can take many forms. For example, an employee with access to sensitive customer data might justify their actions by telling themselves that the company's cybersecurity protocols are insufficient, and therefore, they are entitled to take advantage of a perceived lack of oversight. Alternatively, an individual might rationalize cybercriminal behavior by viewing their actions as a form of retribution, such as getting back at the organization for a perceived wrong or personal grievance. The rationalization process is critical because it allows individuals to dismiss the consequences of their actions, making it easier for them to engage in behaviors that they might otherwise recognize as morally wrong (Djaelani, Zainuddin, & Mokoginta, 2022).

Capability

Capability refers to the inherent skills, knowledge, and resources that individuals or groups possess, enabling them to successfully execute complex tasks or exploit vulnerabilities (Mohd & Awang, 2022). In the context of cybersecurity, capability involves the technical expertise and practical experience required to understand, identify, and exploit system weaknesses, as well as the access to tools, technologies, and methods that facilitate the execution of cyber-attacks. This concept goes beyond merely possessing theoretical knowledge; it encompasses a broad range of competencies, including the ability to manipulate digital systems, circumvent security measures, and exploit flaws in an organization's network infrastructure (Padayachee, 2021). Capable cybercriminals, for example, are those who possess advanced hacking skills, access to specialized software, and a deep understanding of the cybersecurity landscape, making them capable of launching sophisticated attacks that are difficult to detect or defend against.

Almomani, Shehab, Al Ebbini and Shami (2021) argued that the role of capability in cybersecurity is crucial because it determines the potential severity of cyber threats. Even if an organization has robust security measures in place, individuals or groups with high levels of capability can bypass these defenses by leveraging their technical skills. For instance, a skilled hacker might use advanced techniques such as zero-day exploits, social engineering, or malware to gain unauthorized access to critical data, even in the face of well-established security protocols. Similarly, insiders with the capability to manipulate internal systems or access sensitive information can pose a significant threat to an organization's security. This means that capability not only encompasses external threats but also internal ones, where employees or contractors may exploit their access privileges to engage in malicious activities.

Empirical Review

Adhania, Holiawati, and Nofryanti (2024) examined the application of the Fraud Hexagon Theory to detect financial statement fraud among insurance companies listed on the Indonesia Stock Exchange between 2018 and 2022. Using a purposive sampling technique, the researchers selected 15 insurance firms, resulting in 75 data points for analysis. Logistic regression via SPSS version 24 was used to interpret the findings. The study revealed that external pressure, political connections, industry-specific risks, and the presence of effective monitoring all significantly contributed to financial statement fraud. In contrast, variables such as financial stability, financial targets, personal financial needs, individual capability, rationalization, and arrogance were found to have no significant effect.

Apriliyani, Zulfikar, Bastian, and Yazid (2024) investigated the impact of the Pentagon Fraud Model, focusing on the five key factors of Pressure, Opportunity, Rationalization, Capability, and Action, on the risk of Financial Statement Fraud (FSF). The study also examined the moderating role of Islamic Corporate Governance (ICG) in the relationship between these factors and FSF. A quantitative approach was adopted, utilizing survey data from 270 respondents. The results affirmed that all five factors significantly influence FSF, with Pressure demonstrating the highest impact. Additionally, ICG was found to moderate the relationships between these factors and FSF, highlighting its potential in mitigating financial fraud risk. The study emphasized the importance of integrating ethical and governance principles, such as ICG, into organizational frameworks to reduce FSF risks.

Shina, John-Akamelu, and Super (2024) examined the effect of the fraud pentagon model and discretionary accruals in Nigerian deposit money banks. Despite banking regulations and oversight by institutions such as the Central Bank of Nigeria, the Nigeria Deposit Insurance Corporation, and the Chartered Institute of Bankers of Nigeria, fraud and unethical practices persist within the sector. The study aimed to determine how Pressure, Opportunity, Rationalization, Capability, and Arrogance affect discretionary accruals in these banks. Employing an ex post facto research design, secondary data from 13 deposit money banks listed on the Nigerian Exchange Group as of December 31, 2022, were analyzed using OLS multiple regression and E-View 10 statistical software. Their overall conclusion is that elements of the fraud pentagon (especially pressure, opportunity, rationalization, and capability) increase the likelihood of earnings management via discretionary accruals**.**

Musli, Abdullah, and Juardi (2024) focused on the impact of the Hexagon fraud model and the role of the love of money on fraud determinants, with religiosity acting as a moderating variable among village fund managers. This study is novel in incorporating religiosity as a potential moderating factor in fraud determinants. The research adopted a quantitative approach, collecting data from 67 village officials across three sub-districts in the Sidenreng Rappang district using purposive sampling. The data were gathered through surveys and analyzed using multiple linear regression and moderation regression analysis with SPSS 26 software. The study concludes that elements of the hexagon fraud model—particularly pressure and rationalization—significantly influence fraud determinants among village fund managers, while factors such as opportunity, capability, collusion, and love of money show no significant effect. Religiosity is found to play a moderating role by weakening the impact of pressure and rationalization on fraudulent behavior, although it does not moderate other variables. Overall, the findings emphasize the critical role of ethical and religious values in mitigating fraud, suggesting that strengthening religiosity and accountability among village officials can help reduce fraudulent practices in fund management.

Alsakini, Alawawdeh, and Alsayyed (2024) investigated the impact of cybersecurity on the quality of financial accounting statements in selected banks in Jordan. The study combined primary and secondary data collection methods. The primary dataset consisted of 506 data points related to cybersecurity breaches in three Jordanian banks from 2012 to 2022, while the secondary dataset involved a survey of 170 participants. The results indicated that cybersecurity breaches significantly impacted the quality of financial accounting statements, specifically the balance sheet, cash flow, and profit and loss statements. The study concludes that cybersecurity has a significant positive impact on the quality of financial accounting statements in the selected Jordanian banks, as robust security measures enhance the reliability, accuracy, and integrity of financial information. It finds that effective cybersecurity practices, such as data protection, access controls, and risk management systems reduces the likelihood of data breaches and manipulation, thereby improving stakeholders' confidence in financial reports. Overall, the study emphasizes that strengthening cybersecurity frameworks is essential for ensuring high-quality financial reporting and maintaining trust in the banking sector.

Ramalu, Abidin, Nadarajah, and Anuar (2023) investigated the effects of information security issues awareness, top management support, leadership, information security policy, and cybersecurity awareness training on risky cybersecurity behavior among employees in the water sector. Employing a quantitative research design, data was collected from 425 employees across four water companies in northern Malaysia. The respondents were selected using disproportionate stratified random sampling, and the survey was conducted through a questionnaire. The analysis of the data was carried out using Partial Least Squares Structural Equation Modeling (PLS-SEM), which was used to test the proposed hypotheses. The findings revealed that both awareness of security issues and top management support were negatively correlated with risky cybersecurity behavior. This suggests that as employees become more aware of security issues and perceive stronger support from top management, their likelihood of engaging in risky cybersecurity practices decreases. However, contrary to expectations, the study found that cybersecurity awareness training had a positive association with risky cybersecurity behavior. This result points to the complexity of how training influences employee behavior, suggesting that it may not be sufficient on its own to reduce cybersecurity risks, possibly due to a lack of practical application or follow-up after the training sessions.

Haring (2023) explored academic dishonesty through the lens of the Pentagon Theory of Fraud, which identifies five key elements that contribute to fraudulent behavior: pressure, opportunity, rationalization, capability, and arrogance. The study specifically examined college students' involvement in academic dishonesty, using a questionnaire to explore how these five factors influence their actions. The results indicated that pressure, opportunity, and arrogance were the most significant factors influencing academic dishonesty. This suggests that students may feel compelled to cheat due to external pressures, such as academic expectations or competition, as well as a perceived opportunity to engage in dishonest behavior without immediate consequences. Furthermore, the study found that arrogance, or a sense of entitlement or superiority, also played a role, indicating that students who feel they are above the rules may be more likely to engage in unethical behavior. Overall, the study highlights the need for stronger institutional policies and ethical orientation to reduce academic dishonesty.

Abadi, Safriliana, Zuhroh, and Chandrarin (2023) applied the Pentagon Theory of Fraud to analyze fraudulent financial statement actions, focusing on the role of family ownership as a moderating variable. Using a quantitative approach and Moderator Regression Analysis

(MRA), the study examined how pressure, competence, and arrogance affect fraudulent financial statements, and whether family ownership moderates these relationships. The findings showed that pressure had a significant positive impact on the likelihood of financial statement fraud, with statistical tests confirming that pressure was a key driver of fraudulent behavior. However, contrary to expectations, family ownership did not appear to moderate the effects of competence or arrogance on fraudulent financial statements. This suggests that while family ownership may influence other aspects of business behavior, it does not necessarily mitigate the risk of fraud in financial reporting in this context.

Dewi and Yulianti (2023) analyzed the effects of the Pentagon Fraud Model on financial statement fraud in health sector companies listed on the Indonesia Stock Exchange between 2018 and 2021. This quantitative study used eight indicators from five fraud variables, including financial instability and external pressure under the pressure variable; ineffective supervision and industrial nature under the opportunity variable; external auditor turnover under the rationalization variable; change of directors under the competency variable; and CEO duality under the arrogance variable. Secondary data were gathered using purposive sampling, and 23 health sector companies were selected. The results indicated that financial instability had a significant positive effect on financial statement fraud, while external pressure and the industrial nature had significant negative effects. On the other hand, ineffective supervision, changes in external auditors, changes in directors, and CEO duality did not show significant effects on financial statement fraud. Overall, the study emphasizes the importance of strengthening internal controls and corporate governance mechanisms to mitigate financial statement fraud in the health sector.

Andrew, Candy, and Robin (2022) examined the use of the fraud score model and financial distress in detecting fraudulent financial statements. The study was historical and comparative casual research in nature. The data collection focused on financial statements from public companies listed on the Indonesia Stock Exchange (IDX) between 2015 and 2020. Non-financial companies listed on the IDX were used as the study's population. The data from this period were selected as it reflected the current conditions and allowed for a robust analysis. The researchers applied purposive sampling, and hypothesis testing was conducted using multiple regression. The fraud detection tools employed in the study were the F-S.C.O.R.E model and Financial Distress. The F-S.C.O.R.E model consists of five dimensions: Stimulus, Capability, Opportunity, Rationalization, and Ego. The study found that the Stimulus, Capability, and Financial Distress variables were significant in detecting fraud. Furthermore, the results indicated that companies categorized within the industrial sector of the IDX Industrial Classification were most likely to show strong indications of committing fraud.

Andriani, Budiartha, Sari, and Widanaputra (2022) focused on detecting financial statement fraud using the fraud pentagon model. The study used several independent variables, including financial stability, external pressure, personal financial need, financial targets, industry nature, ineffective monitoring, quality of external auditors, changes in auditors, changes in directors, and the frequency of CEO's pictures. The dependent variable was the ability to detect financial statement fraud. The study targeted fraud cases that were subject to sanctions and reported by the Financial Services Authority (OJK) for the period 2015-2019. A sample of 31 fraudulent companies and 31 non-fraudulent companies was used. The research utilized logistic regression to analyze the data. The findings revealed that financial stability had no effect on financial statement fraud, indicating that unstable financial conditions do not necessarily lead managers to manipulate financial statements. On the other hand, external pressure was found to have a positive effect on financial statement fraud, as

companies with higher leverage were under pressure to repay large debts. Personal financial need did not affect financial statement fraud, suggesting that individual financial circumstances of managers did not drive fraudulent reporting. These hints help in understanding the complex factors that contribute to financial fraud in companies.

Yulianto, Dahriyanto, Wijayanti, and Adininggar (2020) examined the effect of fraud pentagon elements and academic procrastination dimensions on academic dishonesty among Grade X Social Science students at Senior High School 8 in Semarang. The population consisted of 180 students, and the sample size was 125 students, determined using the Slovin formula. The sampling technique used was proportional random sampling, and data were collected through questionnaires. The data analysis included descriptive statistical analysis and multiple linear regression analysis. The descriptive analysis revealed that the personal ethics variable was in the high category, while academic dishonesty, academic pressure, opportunity, rationalization, individual capability in committing fraud, and academic procrastination were at a moderately high level. The study found that academic pressure, opportunity, rationalization, individual ability to commit fraud, personal ethics, and academic procrastination simultaneously influenced academic dishonesty. However, individually, academic pressure, individual capability in committing fraud, and academic procrastination had a positive effect, while opportunities and personal ethics had a negative influence. Rationalization was found to have no effect on academic dishonesty. In conclusion, the study demonstrates that elements of the fraud pentagon, together with dimensions of academic procrastination, significantly influence academic dishonesty among Grade X Social Science students, highlighting the need for targeted interventions to promote ethical behavior and time management in the school context.

Lamawitak, Rafael, and Mutia (2020) explored the detection of financial statement fraud using the Pentagon fraud method, specifically in mining sector companies listed on the Indonesia Stock Exchange (IDX) from 2012 to 2018. The researchers focused on five independent variables: pressure related to financial stability, opportunity stemming from the nature of the industry, rationalization measured by the total accrual ratio, competence represented by changes in the CEO, and arrogance characterized by dualism in the CEO position. These variables were examined for their influence on financial statement fraud, which was proxied by earnings management. A purposive sampling method was used to select 15 mining sector companies for the sample, covering a period from 2012 to 2018. The results revealed that while none of the independent variables individually significantly affected financial statement fraud, they collectively had a significant influence, indicating that a broader, more integrated analysis is necessary for understanding financial fraud in this sector.

Methodology

Research Design

Survey research design adopted for the study and is a research method used to gather data from a predefined group of respondents to gain hints into various topics of interest (Mellinger & Hanson, 2020).

Given that the study aims to understand how the various factors of the hexagon Model influence cybersecurity threats, the survey design provided a structured approach for gathering data on the experiences, views, and opinions of employees working in Nigerian commercial banks. Population of the Study

The population of the study consists of listed commercial banks in Nigeria with international authorization. These banks are particularly relevant because their international operations, large customer bases, and cross-border digital transactions make them more susceptible to cyberfraud risks. Their scale of operations and exposure to global banking systems create fertile ground for testing the six dimensions of the hexagon model; pressure, opportunity, rationalization, capability, arrogance, and collusion, as determinants of cybercrime in the banking sector. By focusing on this population, the study ensures that the findings reflect institutions with the most significant exposure to cybersecurity threats, while also aligning with the objectives of assessing how each element of the model influences cyberfraud.

Sample Size and Sampling Technique

To determine the sample size, the researcher used Taro Yamane's formula. The calculation is demonstrated as follows:

Formula: Sample size (n) = $\frac{N}{1+N\ (e)^2}$

Where,

n = sample size

N = population, which in this case is 54,654

e = sampling error, usually 5%

Therefore, sample size (n) is obtained thus:

n = $\frac{54{,}654}{1+54{,}654\ (0.05)^2}$

Sample size = 397

Sampling Technique

A stratified sampling technique was used to select respondents from each of the seven banks. Stratified sampling ensures that different subgroups (in this case, employees from different banks) are represented in the sample proportionally. The banks served as the strata, and the number of respondents selected from each bank was proportionate to the total number of employees in that bank. The number of respondents to be selected from each bank are; Access Bank 59; Fidelity Bank 28; FCMB 30; First Bank 72; Guaranty Trust Bank 47; United Bank for Africa (UBA) 87 and Zenith Bank 73. Total is 396

Method of Data Collection

Data were collected using a structured questionnaire. The questionnaire contained both closed and Likert-scale questions, designed to assess the relationship between the hexagon Model dimensions (rationalization and capability) and cybersecurity threats in Nigerian commercial banks. Respondents were asked to indicate their level of agreement or disagreement with various statements related to the two factors and how they perceive these factors contributing to cybersecurity threats. The questionnaire was distributed to the selected respondents using electronic format. Respondents were asked to provide answers based on their personal experiences and perceptions related to cybersecurity issues and threats within their respective banks.

Method of Data Analysis

The data collected from the survey was analyzed using both descriptive and inferential statistics. Descriptive statistics was used to analyze the basic characteristics of the data, such as the frequency, percentages, and means for each of the variables. The linear regression model was adapted from the study by Sari and Witosari (2022) that examined Fraud Hexagon Model Analysis in the Financial Sector Listed on the Indonesia Stock Exchange. The adapted model is presented below:

Model specification (functional form)
FSF = f(FNS,EXP,PRFN,FNT,CAPB,NOI,RAZA,ARGA,COL)…… ……(1)

Estimating (Regression) Equation:
$FSF = a + b_1FNS + b_2EXP + b_3PRFN + b_4FNT + b_5CAPB + b_6NOI + b_7EFMO + b_8RAZA + b_9ARGA + b_{10}COL + e$…….…… *(2)*
Where:
FSF: Financial Statement Fraud (dependent variable)
a: Intercept
b_1 to b_{10}: Regression coefficients
e: Error term
Pressure — represented by four proxies:
FNS: Financial Stability
EXP: External Pressure
PRFN: Personal Financial Need
FNT: Financial Targets
CAPB: Capability – the opportunity or ability to commit and conceal fraud
NOI: Nature of Industry – industry characteristics that may create opportunities for fraud
EFMO: Effective Monitoring – quality and effectiveness of oversight mechanisms
RAZA: Rationalization – justification or mindset enabling fraudulent behavior
ARGA: Arrogance – attitude of superiority that may lead individuals to override controls
COL: Collusion – cooperation between two or more parties to commit fraud

The researcher modified the baseline model to develop a more parsimonious specification for robustness analysis. The revised model focuses on the core dimensions of the Fraud Hexagon Model as predictors of cybersecurity threats.

Model specification (functional form):
CST = f(RAT,CAP)……(i)

This indicates that Cybersecurity Threats (CST) are a function of pressure, opportunity, rationalization, capability, arrogance, and collusion.

Estimating Equation:
$CST_i = \beta_0 + \beta_1RAT_i + \beta_2CAP_i + e_i$ ……*(ii)*
Where:
B_0 = Intercept
β_{1-2} = The parameter to be estimated in the equation
CST = Cybersecurity Threat
RAT = Rationalisation
CAP = Capability
i = cross-sectional respondent
e = error term

Decision Rule
For all statistical tests, the 5% significance level ($\alpha = 0.05$) was used as the decision rule. If the p-value is less than 0.05, the null hypothesis is rejected, indicating that there is a significant relationship between the variables being tested. Conversely, if the p-value is greater than 0.05, the null hypothesis is accepted, suggesting that the factors from the hexagon Model do not significantly influence cybersecurity threats in Nigerian commercial banks.

Data Presentation, Analysis and Results

Table 1: Likert-scale Responses to Rationalization

	Rationalization	SD	D	U	A	SA	Mean
1	Employees may justify bypassing security protocols by claiming that the work is urgent.	105	21	36	99	91	3.14
2	Some individuals rationalize their involvement in cybersecurity breaches by blaming it on system flaws.	84	33	28	104	103	3.31
3	There is a tendency to rationalize cybersecurity lapses, believing that "everyone does it" or "it's not a big deal."	101	31	36	100	84	3.10
4	Some individuals in the bank may rationalize engaging in unauthorized activities because they believe the organization will not suffer major consequences.	93	34	39	98	88	3.15

Source: Field Survey (2025)

Table 1 displays respondents' views on rationalization as a psychological factor that may contribute to cybersecurity threats in commercial banks. The responses reflect the extent to which individuals agree or disagree with statements that suggest employees may justify or downplay their involvement in cyber-related misconduct. The data are measured on a five-point Likert scale ranging from "Strongly Disagree" to "Strongly Agree."

The first statement in the table proposes that employees may justify bypassing security protocols by claiming that their task is urgent. Here, 105 respondents strongly disagreed, and 21 disagreed, indicating that a notable portion of the participants reject this justification. However, 99 respondents agreed and 91 strongly agreed, showing that many acknowledge this behavior as a common occurrence. With 36 undecided and a mean score of 3.14, the overall interpretation suggests a moderate level of agreement that urgency is used to rationalize ignoring security procedures.

The second item addresses the belief that system flaws are sometimes used as an excuse for engaging in cybersecurity breaches. In this case, 84 respondents strongly disagreed, 33 disagreed, while 104 agreed and 103 strongly agreed. Only 28 remained undecided. The mean of 3.31 indicates a slightly stronger agreement compared to the first item, showing that many respondents recognize this form of rationalization as a genuine issue.

The third item suggests that employees may downplay cybersecurity lapses by believing "everyone does it" or "it's not a big deal." A total of 101 strongly disagreed and 31 disagreed, yet 100 agreed and 84 strongly agreed, with 36 undecided. The mean score of 3.10 again reflects a general tendency toward agreement, showing that normalization or minimization of cyber misconduct is a recognized mindset among bank employees.

Finally, the fourth item explores whether individuals rationalize unauthorized activities under the assumption that the organization will not suffer significant consequences. Among the respondents, 93 strongly disagreed and 34 disagreed, while a substantial 98 agreed and 88 strongly agreed. With 39 respondents undecided, this item recorded the highest mean score of 3.15, indicating that this form of rationalization is perceived by many as a notable behavioral risk in the banking environment.

Table 2: Likert-scale Responses to Capability

	Capability	SD	D	U	A	SA	Mean
5	Some employees and outsiders have the necessary technical skills to exploit security vulnerabilities within the bank's systems.	98	42	21	109	82	3.09
6	Cybercriminals targeting the bank are often highly skilled and capable of bypassing existing security measures.	94	31	28	110	89	3.20
7	The lack of a sufficiently trained IT team increases the capability of malicious actors to exploit the bank's systems.	105	29	42	98	78	3.04
8	Some cybercriminals possess advanced knowledge of security weaknesses, which could be used for malicious purposes.	96	36	35	90	95	3.15

Source: Field Survey (2025)

Table 2 presents respondents' perceptions of capability as a factor contributing to cybersecurity threats in commercial banks. The items assess whether both internal and external actors possess the skills and knowledge required to exploit weaknesses in the bank's systems. Responses were measured on a five-point Likert scale ranging from "Strongly Disagree" to "Strongly Agree."

The first item in the table suggests that some employees and outsiders have the technical skills to exploit system vulnerabilities. Here, 98 respondents strongly disagreed, and 42 disagreed, showing some skepticism. However, a larger group (109 respondents) agreed, and 82 strongly agreed, while only 21 remained undecided. The mean score of 3.09 reflects a generally positive agreement, indicating that a significant portion of the respondents recognize internal and external technical skill as a real threat to cybersecurity.

In the second item, respondents were asked whether cybercriminals targeting the bank are highly skilled and capable of bypassing existing security controls. A total of 94 respondents strongly disagreed and 31 disagreed, while 110 agreed and 89 strongly agreed. With only 28 undecided and a mean of 3.20, this item showed the highest agreement in the table, suggesting that many respondents view the capability of external cybercriminals as a serious and credible concern.

The third statement addressed whether the absence of a sufficiently trained IT team increases the vulnerability of the bank's systems. Responses were slightly more varied: 105 strongly disagreed and 29 disagreed, while 98 agreed and 78 strongly agreed. Forty-two respondents were undecided. The mean score of 3.04 indicates a moderate agreement, suggesting that while some respondents may be confident in their IT teams, many believe that inadequate training creates opportunities for malicious actors.

The final item proposes that some cybercriminals possess advanced knowledge of system weaknesses, which can be used for malicious purposes. Here, 96 strongly disagreed and 36 disagreed, while 90 agreed and 95 strongly agreed, with 35 undecided. The mean score of 3.15 shows that responses are again leaning toward agreement, though slightly less so compared to other items.

Table 3: Likert-scale Responses to Cyberfraud

	Cyberfraud	SD	D	U	A	SA	Mean
9	The bank experiences frequent cyber-attacks targeting customer data or financial systems.	83	22	31	115	101	3.37
10	Employees are often exposed to phishing attacks or other forms of social engineering.	95	34	29	89	105	3.21
11	The bank's cybersecurity systems have been compromised by malware or ransomware in the past year.	111	22	31	99	89	3.09
12	There are significant threats to the bank's data security due to inadequate protection against external hackers.	98	35	32	102	85	3.12

Source: Field Survey (2025)

Table 3 presents respondents' views on cyberfraud occurrences and threats within Nigerian commercial banks, assessed through four Likert-scale statements. In the first item, respondents assessed the frequency of cyber-attacks targeting customer data or financial systems. Here, 83 strongly disagreed, 22 disagreed, and 31 were undecided. On the other hand, 115 agreed and 101 strongly agreed resulting in a mean of 3.37. The high number of agreement responses indicate a general belief that such attacks are relatively common and pose a serious risk to bank operations.

The second item evaluated employees' exposure to phishing and social engineering attempts. The responses show that 95 strongly disagreed and 34 disagreed, with 29 undecided. Despite this, 89 agreed and 105 strongly agreed, resulting in a mean of 3.21. This reflects moderate concern among respondents, with a significant number acknowledging such exposure even though a large portion remained skeptical. For the third item, which focused on the compromise of cybersecurity systems by malware or ransomware in the past year, 111 strongly disagreed and 22 disagreed. Still, 99 respondents agreed and 89 strongly agreed, with 31 undecided. The resulting mean of 3.09 suggests that while some respondents were unaware or unsure, a notable number believe that the banks have experienced serious security breaches recently.

The final item addressed the threat to data security due to inadequate protection from external hackers. Among respondents, 98 strongly disagreed and 35 disagreed, while 102 agreed and 85 strongly agreed. Thirty-two were undecided. The mean score of 3.12 again reflects moderate agreement that external threats remain a significant cybersecurity concern.

Table 4 Correlational Analysis

		Cybersecurity Threat	Rationalisation	Capability
Rationalisation	Pearson Correlation	.817**		
	Sig. (2-tailed)	.000		
Capability	Pearson Correlation	.923**	.143**	
	Sig. (2-tailed)	.000	.000	

Source: SPSS V. 26 Output (2025)

The results presented in Table 4 reveal the strength and direction of the relationship between each component of the fraud hexagon and cybersecurity threats (measured as cyberfraud) in Nigerian commercial banks. All variables (independent) show a statistically significant positive correlation with cyberfraud, as indicated by Pearson correlation coefficients of not less than 0.817 and p-values less than 0.01. This suggests a strong and consistent relationship between the psychological and organizational fraud drivers and the prevalence of cybersecurity threats in the banking sector.

Rationalization also exhibits a strong relationship with cyberfraud (r = .817, p < .01). This reflects the idea that individuals may justify their involvement in cyber breaches by downplaying their actions or blaming system flaws. Such rationalizations help mitigate personal guilt, making it easier for perpetrators to proceed with malicious actions. This relationship underscores the need for ethical training and clear consequences for security violations within financial institutions.

The variable capability recorded the highest correlation coefficient with cyberfraud (r = .923, p < .01), suggesting that individuals' technical ability to exploit vulnerabilities is a critical driver of cybersecurity threats. Those with the necessary skills whether internal staff or external actors are more capable of bypassing system safeguards. This result emphasizes the importance of continually upgrading security infrastructure and ensuring personnel are trained to anticipate and counter high-skill threats.

Test of Hypotheses

To further test the hypotheses and examine the predictive power of the Hexagon Model factors on cybersecurity threats, multiple regression analysis was conducted.

Table 5 Test of Hypotheses

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.948[a]	.899	.897	1.820

a. Predictors: (Constant), Rationalisation, Capability

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	9794.061	6	1632.343	492.948	.000[b]
	Residual	1106.004	334	3.311		
	Total	10900.065	340			

a. Dependent Variable: Cyberfraud
b. Predictors: (Constant),Rationalisation, Capability

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	T	Sig.
1	(Constant)	.151	.250		.605	.546
	Rationalisation	.157	.053	.155	2.987	.003
	Capability	.224	.059	.222	3.810	.000

Source: SPSS V. 26 Output (2025)

Based on Table 5, the overall validity of the regression model is first established using the Adjusted R-Square and ANOVA statistics. The Adjusted R-Square value of 0.843 indicates that approximately 84.7% of the variation in cyberfraud is explained collectively by the six predictors from the Fraud Hexagon model: rationalization and capability. This suggests a very high explanatory power of the model. Additionally, the probability value of the sig is 0.000, which is less than the 5% significance level, implying that the overall model is statistically significant. In other words, the joint effect of all the independent variables significantly explains the changes in cyberfraud in Nigerian commercial banks.

The constant term (intercept) in the regression output is 0.151 with a p-value of 0.546, which is greater than 0.05. This indicates that when all the predictors are held constant (i.e., zero), the baseline level of cyberfraud is statistically insignificant. Therefore, the model suggests

that cyberfraud in commercial banks is largely driven by the two fraud hexagon dimensions, and not by any unexplained constant factor.

Test of Hypothesis One

H_{01}: Rationalization has no significant effect on cyberfraud in the listed commercial banks in Nigeria.

H_1: Rationalization significantly affects cyberfraud in the listed commercial banks in Nigeria

Rationalization has a positive and significant effect on cyberfraud, with a coefficient of 0.157 and a p-value of 0.003. This suggests that a unit increase in rationalization leads to a 0.157-unit rise in cyberfraud, assuming other variables remain constant. The result is significant at the 5% level, as the p-value is less than 0.05. Employees may justify fraud by blaming the system, minimizing the consequences, or normalizing such behavior. These justifications provide psychological comfort for engaging in unethical acts. Thus, H03 is rejected, confirming that rationalization significantly contributes to cyberfraud. Hence the alternate hypothesis is accepted that rationalization has a significant and positive effect on cyberfraud in the listed commercial banks in Nigeria ($\beta = 0.157$, $p = 0.003$).

Test of Hypothesis Two

H_{02}: There is no significant effect of capability on cyberfraud in the listed commercial banks in Nigeria.

H_2: Capability has a significant effect on cyberfraud in listed commercial banks in Nigeria.

Capability emerges as the strongest predictor of cyberfraud among the six factors, with a coefficient of 0.224 and a p-value of 0.000. This implies that a one-unit increase in capability (technical skills or system knowledge) leads to a 0.224-unit increase in cyberfraud, all other factors held constant. The effect is highly significant at the 5% level. This suggests that cybercriminals (whether insiders or outsiders) with advanced skills are more likely to exploit system vulnerabilities. Consequently, H04 is rejected, and the study concludes that capability significantly affects cyberfraud. Hence the alternate hypothesis is accepted that capability has a significant and positive effect on cyberfraud in the listed commercial banks in Nigeria ($\beta = 0.224$, $p = 0.000$).

Discussion and Conclusion

Rationalization exhibited a significant and positive relationship with cyberfraud, suggesting that individuals may justify fraudulent behavior to themselves as acceptable or necessary under certain circumstances. Rationalization reduces internal psychological barriers to unethical conduct by framing fraud as a victimless crime or a means of justice, particularly when the individual perceives the system as unfair. Within banking institutions, this mindset can be reinforced by personal grievances, peer behavior, or cultural narratives that normalize ethical compromise, ultimately lowering the moral threshold for engaging in cyberfraud. Empirical support for this finding is substantial. Setiawan and Soewarno (2025) noted that rationalization significantly contributed to fraud behavior, a view echoed by Musli et al. (2024), who found that it influenced village fund misappropriation. Metts (2020) also identified rationalization as a key predictor of fraud intention, while Achmada et al. (2020) confirmed its role in academic dishonesty. However, some studies, like Adhania et al. (2024), found no significant effect of rationalization in certain contexts, suggesting its influence may vary across industries. Still, the preponderance of evidence in finance-related sectors supports the conclusion that rationalization plays a crucial psychological role in enabling cyberfraud.

Capability emerged as the strongest predictor among the fraud hexagon proxies, with a significant and positive effect on cyberfraud. This highlights the importance of technical competence and access in executing cyberfraud. In banking, perpetrators must often possess advanced knowledge of systems, processes, or security protocols to bypass controls effectively. This finding suggests that fraud is not just a product of motive but also of means. That is, the more capable an individual is in terms of skills and access, the more likely they are to exploit digital vulnerabilities. Several studies reinforce this result. Ekele (2024) emphasized that capability significantly contributed to organizational distress via fraud, while Apriliyani et al. (2024) included it among the factors influencing financial statement fraud. Achmada et al. (2020) and Asmaranti et al. (2023) also found capability to be a significant factor in both academic dishonesty and financial fraud, respectively. Moreover, Andrew et al. (2022) highlighted capability as central to detecting fraud in industrial settings. These findings collectively support the view that technical competence enhances the likelihood of fraud, especially in cyber contexts where such knowledge can be weaponized.

This implies that cyberfraud in Nigerian commercial banks is less about individuals acting out of personal pride or ego and more about calculated actions influenced by internal pressures and systemic weaknesses. In all, the findings present cyberfraud as a multifaceted issue driven by behavioral, organizational, and technical factors, requiring a holistic understanding of employee conduct, bank operations, and cybersecurity environments.

Based on the findings, the study recommended the following;
1. Compliance officers and ethics units should organize regular ethics training and awareness programs that reinforce zero tolerance for fraud, regardless of justification. These programs should help employees understand the legal, financial, and reputational damage of fraud, thereby discouraging them from justifying unethical behavior through rationalization.

2. Chief Information Security Officers (CISOs) should routinely evaluate and restrict the technical capabilities of staff that have access to critical systems by applying the principle of least privilege. Moreover, periodic re-certification of access rights and advanced cybersecurity audits should be enforced to ensure only properly vetted individuals have the skills and authority to perform sensitive operations.

References

Abadi, R., Safriliana, R., Zuhroh, D., & Chandrarin, G. (2023). Pentagon Fraud Analysis of Fraud Financial Statement Actions: The Role of Family Ownership as Moderation Variable. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, *6*(2), 541-555.

Adhania, S., Holiawati, H., & Nofryanti, N. (2024). The Effect of Hexagon Fraud Theory in Detecting Financial Statement Fraud. *International Journal of Digital Marketing Science*, *1*(1), 10-23.

Almomani, S. N., Shehab, M., Al Ebbini, M. M., & Shami, A. A. (2021). The efficiency and effectiveness of the cyber security in maintaining the cloud accounting information. *Academy of Strategic Management Journal*, *20*, 1-11.

Alsakini, S. A. K., Alawawdeh, H. A., & Alsayyed, S. (2024). The Impact of Cybersecurity on the Quality of Financial Statements. *Appl. Math*, *18*(1), 169-181.

Andrew, A., Candy, C., & Robin, R. (2022). Detecting fraudulent of financial statements using fraud score model and financial distress. *International Journal of Economics, Business and Accounting Research (IJEBAR)*, *6*(1), 696-707.

Apriliyani, I., Zulfikar, R., Bastian, E., & Yazid, H. (2024). Pentagon fraud model and financial statement fraud: The moderating role of Islamic corporate governance. *International Journal of Data and Network Science*, *8*(2), 1293-1306.

Chhabra Roy, N., & Prabhakaran, S. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. *Digital Policy, Regulation and Governance*.

Dewi, S. T., & Yulianti, R. (2023). Analysis of the effect of pentagon fraud on financial statement fraud (Empirical Study on Health Sector Companies Listed on the Indonesia Stock Exchange for the 2018-2021. *Journal Of Multiparadigm Accounting Research*, *1*(1-April).

Djaelani, Y., Zainuddin, Z., & Mokoginta, R. M. (2022). Academic fraud of students in the Covid-19 period: Testing with the Pentagon's fraud dimension. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(2), 414-422.

Haring, J. H. (2023). *Crash Course in Fraud: Academic Dishonesty Through the Lens of the Pentagon Theory of Fraud* (Master's thesis, Indiana University of Pennsylvania).

Jajere, U. U., Ngerebo, T. A., & Adebisi, J. F. (2025). Hexagon Hallmarks Effects on Financial Fraud in Nigeria's Federal Ministry of Finance, Budget & National Planning and Economic Development. *Journal Of Entrepreneurship And Business Management*, *4*(2), 1-9.

Lamawitak, S. T., Rafael, S. J. M., & Mutia, K. D. (2020, May). *Detection of financial statement fraud with the Fraud Pentagon method for mining sector companies listed on Indonesian Stock Exchange (IDX) for period 2012 to 2018*. [PDF]. Retrieved from https://repository.unsri.ac.id/54349/

Mohd, R., & Awang, Z. (2022). A confirmatory factor analysis of the fraud pentagon instruments for measurement of fraud in the context of asset misappropriation in Malaysia. *Journal of Social Economics Research*, *9*(2), 70-79.

Musli, N. A., Abdullah, M. W., & Juardi, M. S. S. (2024). The Effect of Hexagon Fraud and Love of Money Components on Determinants of Fraud With Religiosity as A Moderation Variable. *Jurnal Akuntansi Bisnis dan Ekonomi*, *10*(2), 39-49.

Padayachee, K. (2021). A Theoretical Underpinning for Examining Insider Attacks Leveraging the Fraud Pentagon. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15* (pp. 179-188). Springer International Publishing.

Ramalu, S. S., Abidin, N. B. Z., Nadarajah, G., & Anuar, A. B. (2023). The Determinants of Risky Cybersecurity Behaviour: A Case Study Among Employees in Water Sector in Malaysia. *Journal of Law and Sustainable Development*, *11*(12), e2706-e2706.

Shina, O. O., John-Akamelu, C. R., & Super, S. O. (2024). Fraud Pentagon Model And Discreationary Accruals In Deposit Money Banks In Nigeria. *Journal Of Global Accounting*, *10*(1), 95-118.

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.

Wang, X., & Cheng, Z. (2020). Cross-sectional studies: strengths, weaknesses, and recommendations. *Chest*, *158*(1), S65-S71.

Yulianto, A., Dahriyanto, L. F., Wijayanti, R., & Adininggar, P. (2020, August). The Effect of Fraud Pentagon and Academic Procrastination Dimensions Towards Academic Dishonesty of Students of Social Science in Senior High School of Semarang. In *1st Progress in Social Science, Humanities and Education Research Symposium (PSSHERS 2019)* (pp. 1158-1169). Atlantis Press.