European Journal of Social Sciences Studies
ISSN: 2501-8590
ISSN-L: 2501-8590
Available on-line at: www.oapub.org/soc

DOI: 10.46827/ejsss.v10i4.1825 Volume 10 | Issue 4 | 2024

CYBERSECURITY PRACTICES AND FRAUD PREVENTION AMONG GHANAIAN TELECOMMUNICATION FIRMS, A MIXED METHOD ANALYSIS

Kwakye Agyapong[1],
Isaac Boakye[2i]
[1]PhD,
Metropolitan Consulting Group,
Ghana
[2]Accra Institute of Technology,
Ghana

Abstract:
This study explores the effectiveness of cybersecurity practices in preventing fraud within Ghanaian telecommunication firms, adopting a qualitative research approach to gain in-depth insights into the challenges and strategies involved. By focusing on the perspectives of key personnel directly involved in cybersecurity and fraud prevention, the study aims to uncover critical factors influencing the success of these practices. A case study design is employed, examining cybersecurity implementation across five major telecommunication firms in Ghana. The sample consists of 15 participants, including IT managers, cybersecurity officers, and fraud prevention specialists, selected through purposive sampling to ensure relevant and insightful data collection. Semi-structured interviews are used as the primary data collection method, allowing participants to provide detailed and nuanced information on their experiences with cybersecurity measures. Thematic analysis is employed to identify key patterns and themes within the data, highlighting the role of insider threats, regulatory frameworks, and employee behavior in contributing to fraud. The findings indicate that while robust technical measures such as encryption, multi-factor authentication, and intrusion detection systems play a significant role in reducing fraud, challenges in enforcement, compliance, and employee behavior remain critical barriers. The study concludes that a holistic approach, combining technical solutions with organizational culture improvements and stronger regulatory enforcement, is essential for enhancing cybersecurity effectiveness in Ghana's telecommunication sector. Recommendations are made for improving incident response times, regulatory support, and employee training programs, as well as fostering greater collaboration between firms and regulatory bodies to strengthen fraud prevention efforts.

[i] Correspondence: email boakyei@ait.edu.gh

Copyright © The Author(s). All Rights Reserved.

Keywords: e-learning, senior high schools, instructor readiness, implementation, Ghana

1. Introduction

In recent years, the rise of digital technologies has significantly transformed the operations of telecommunication firms worldwide. In Ghana, the telecommunication sector has grown exponentially, becoming a critical driver of economic growth and social development. As the sector continues to expand, so do the threats associated with cybersecurity. Cybersecurity practices have become an essential component of organizational strategy, particularly in telecommunication firms that handle vast amounts of sensitive data. The increasing frequency and sophistication of cyber-attacks have prompted scholars and practitioners to focus on the relationship between cybersecurity practices and fraud prevention. This research seeks to explore the current state of cybersecurity practices among Ghanaian telecommunication firms and their effectiveness in fraud prevention.

Telecommunication firms are at the forefront of technological innovation, which inherently exposes them to various cyber threats. According to Wilner and Birnbaum (2020), the proliferation of digital platforms has made telecommunication firms prime targets for cybercriminals due to the vast amount of personal and financial data they manage. Cybersecurity, therefore, is not just a technical issue but a strategic imperative for these firms. Several researchers have noted the growing importance of integrating robust cybersecurity practices into the core operations of telecommunication companies to mitigate the risks of fraud and other cyber-related crimes. For instance, Abubakar and Haruna (2019) argue that the adoption of advanced cybersecurity measures is crucial for protecting critical infrastructure and ensuring the integrity of communication networks.

The relationship between cybersecurity practices and fraud prevention has been widely studied, with varying conclusions drawn by researchers. Al-Rababah and Qatawneh (2021) suggest that effective cybersecurity measures can significantly reduce the incidence of fraud within organizations by detecting and mitigating threats before they materialize. In the context of telecommunication firms, this involves implementing comprehensive security frameworks that address potential vulnerabilities in the system. However, other scholars, such as Johnson and Willey (2018), caution that while cybersecurity is essential, it is not a panacea for fraud prevention. They argue that organizational culture and employee behavior also play critical roles in either enabling or preventing fraudulent activities. Therefore, a holistic approach that combines technical cybersecurity measures with strong governance and ethical practices is necessary for effective fraud prevention.

In Ghana, the telecommunication industry is one of the most lucrative sectors, contributing significantly to the country's GDP. However, the rapid growth of the industry has also attracted cybercriminals who exploit the relatively weak cybersecurity infrastructure in place. According to Mensah and Adjei (2022), many Ghanaian telecommunication firms still rely on outdated security protocols, making them

vulnerable to cyber-attacks. The authors highlight the need for these firms to adopt more advanced cybersecurity practices, such as the use of artificial intelligence and machine learning, to enhance their fraud detection and prevention capabilities. Furthermore, they emphasize the importance of continuous monitoring and updating of security systems to stay ahead of evolving cyber threats.

The role of regulatory bodies in enforcing cybersecurity standards in the telecommunication sector cannot be overstated. As noted by Quaye and Asante (2021), the Ghanaian government, through the National Communications Authority (NCA), has implemented several policies aimed at strengthening cybersecurity across the sector. These include mandatory cybersecurity audits, the establishment of Computer Emergency Response Teams (CERTs), and the introduction of cybersecurity awareness programs. While these initiatives have had some positive impact, Quaye and Asante (2021) argue that enforcement remains a significant challenge. Many telecommunication firms either lack the resources or the will to fully comply with these regulations, leading to persistent vulnerabilities that cybercriminals can exploit.

Research by Boateng and Darko (2020) reveals that fraud is a major issue within the Ghanaian telecommunication sector, with SIM card fraud, mobile money fraud, and phishing attacks being the most prevalent. The authors attribute the high incidence of fraud to the inadequate cybersecurity measures implemented by these firms. They point out that while some companies have invested in basic cybersecurity tools, such as firewalls and encryption, these measures are often insufficient to combat more sophisticated cyber-attacks. Boateng and Darko (2020) call for a more proactive approach to cybersecurity, including the adoption of advanced threat detection systems and the training of employees on best practices in cybersecurity and fraud prevention.

The human factor is another critical aspect of cybersecurity and fraud prevention in telecommunication firms. As highlighted by Kankam and Owusu (2021), insider threats pose a significant risk to the security of telecommunication networks. Employees who have access to sensitive data and systems can inadvertently or maliciously compromise the security of the organization. The authors argue that telecommunication firms must prioritize employee training and awareness programs to mitigate the risk of insider threats. Additionally, they suggest the implementation of stringent access controls and regular security audits to identify and address potential insider risks.

International perspectives also provide valuable insights into the cybersecurity challenges faced by telecommunication firms in Ghana. A study by Jain and Shanbhag (2019) on cybersecurity practices in Indian telecommunication companies highlights several best practices that could be applied in the Ghanaian context. These include the adoption of a risk-based approach to cybersecurity, the integration of cybersecurity into the overall business strategy, and the use of predictive analytics to identify potential threats. Jain and Shanbhag (2019) emphasize that a proactive, rather than reactive, approach to cybersecurity is essential for effectively preventing fraud and other cyber-related crimes.

Despite the growing awareness of the importance of cybersecurity, many Ghanaian telecommunication firms still face significant challenges in implementing effective security measures. According to Adusei and Frimpong (2022), limited financial resources, lack of skilled personnel, and inadequate regulatory enforcement are among the primary barriers to improving cybersecurity in the sector.

2. Statement of the Problem

The telecommunications sector in Ghana has become a critical part of the country's economic framework, serving as a backbone for communication, business transactions, and the digital economy. However, as telecommunication firms increasingly rely on digital platforms, they face growing threats from cybercriminals who exploit vulnerabilities in these systems to commit fraud. Cybersecurity has emerged as a key concern for these firms, as they are responsible for safeguarding vast amounts of sensitive data, including personal information, financial transactions, and communication records. Despite the significant risks associated with cyber threats, there is limited empirical research examining the effectiveness of cybersecurity practices in preventing fraud within Ghanaian telecommunication firms. This gap in the literature underscores the need for a focused study that addresses the specific challenges and opportunities in enhancing cybersecurity to combat fraud in this sector.

Fraud in the telecommunication sector can take many forms, including SIM card fraud, mobile money fraud, phishing, and identity theft. These fraudulent activities not only result in financial losses for companies and customers but also damage the reputation of telecommunication firms and erode public trust. According to Boateng and Darko (2020), the incidence of fraud within the Ghanaian telecommunication sector is alarmingly high, with many companies struggling to implement effective measures to detect and prevent such activities. This problem is compounded by the fact that many firms continue to rely on outdated security protocols, which are often insufficient to counter the sophisticated tactics employed by modern cybercriminals. The persistence of fraud despite existing cybersecurity measures suggests a critical gap in the current strategies employed by telecommunication firms, raising questions about the adequacy of these measures in addressing the unique challenges of the Ghanaian context.

While there is a growing body of literature on cybersecurity and fraud prevention in general, much of the existing research is focused on developed countries with advanced technological infrastructures. Studies by Jain and Shanbhag (2019) and others have highlighted best practices in cybersecurity from global perspectives, but these practices may not be directly applicable to the Ghanaian context due to differences in resources, regulatory environments, and technological capabilities. The lack of context-specific research leaves Ghanaian telecommunication firms without a clear framework for effectively addressing the cybersecurity challenges they face. This research gap is significant, as it limits the ability of these firms to develop and implement strategies that

are tailored to their specific needs, potentially leaving them vulnerable to cyber threats and fraud.

Moreover, regulatory bodies in Ghana, such as the National Communications Authority (NCA), have introduced policies aimed at strengthening cybersecurity in the telecommunication sector. However, the effectiveness of these regulations in actually reducing fraud remains unclear. Quaye and Asante (2021) argue that while the regulatory framework exists, enforcement is often inconsistent, and many firms lack the resources or the will to fully comply with the mandated cybersecurity standards. This regulatory gap not only undermines the efforts to secure the telecommunication infrastructure but also exacerbates the vulnerability of these firms to cyber-attacks and fraud. Therefore, there is a need for research that not only assesses the current cybersecurity practices but also evaluates the effectiveness of regulatory measures in mitigating fraud within the Ghanaian telecommunication sector.

Furthermore, the human factor in cybersecurity is a critical, yet often overlooked, aspect of fraud prevention. As Kankam and Owusu (2021) point out, insider threats, whether intentional or unintentional, can significantly compromise the security of telecommunication firms. Employees who have access to sensitive data and systems may inadvertently or maliciously cause security breaches that lead to fraud. However, there is limited research on how Ghanaian telecommunication firms address insider threats through employee training, access controls, and other preventive measures. This gap highlights the need for a more comprehensive approach to cybersecurity that includes not only technological solutions but also robust policies and practices related to human resource management and organizational culture.

Given the critical role that telecommunication firms play in Ghana's economy, the growing threat of cyber-related fraud represents a significant problem that warrants in-depth research. The high incidence of fraud, combined with the inadequacy of existing cybersecurity measures and regulatory enforcement, creates a pressing need for a study that explores these issues in detail. This research seeks to fill the gap in the literature by providing empirical evidence on the current state of cybersecurity practices in Ghanaian telecommunication firms and their effectiveness in preventing fraud. By addressing this research gap, the study aims to contribute to the development of more effective cybersecurity strategies that are tailored to the specific challenges faced by telecommunication firms in Ghana, ultimately helping to protect these critical institutions from the growing threat of cybercrime and fraud.

3. Objectives of the Study

The purpose of this study is to investigate the effectiveness of cybersecurity practices in preventing fraud among Ghanaian telecommunication firms. By exploring the current state of cybersecurity measures, assessing the role of regulatory frameworks, and examining the impact of insider threats, this research aims to identify gaps in existing

strategies and provide recommendations for enhancing fraud prevention in the sector. The specific objectives of the study will be to:

1) To evaluate the current cybersecurity practices employed by Ghanaian telecommunication firms in preventing fraud.
2) To assess the effectiveness of regulatory frameworks in enhancing cybersecurity and reducing fraud within the Ghanaian telecommunication sector.
3) To examine the role of insider threats and employee behavior in contributing to fraud, and how these can be mitigated through improved cybersecurity measures.

4. Theoretical Framework

In examining the effectiveness of cybersecurity practices in preventing fraud among Ghanaian telecommunication firms, the study draws on the Protection Motivation Theory (PMT) as a guiding theoretical framework. Developed by Rogers (1975), PMT explains how individuals and organizations respond to threats based on their perceived severity and vulnerability, the efficacy of the recommended protective behavior, and their self-efficacy in executing the behavior. This theory is particularly relevant in the context of cybersecurity, where organizations must assess the risks posed by cyber threats and determine the most effective measures to mitigate these risks.

PMT posits that the decision to adopt protective measures, such as cybersecurity practices, is influenced by both threat appraisal and coping appraisal. Threat appraisal involves evaluating the seriousness of the threat (e.g., the potential impact of a cyber-attack or fraud) and the likelihood of its occurrence. In the context of Ghanaian telecommunication firms, the increasing frequency and sophistication of cyber-attacks heighten the perceived severity and vulnerability to such threats. As Abubakar and Haruna (2019) suggest, the growing reliance on digital platforms and the sensitive nature of the data managed by these firms make them particularly susceptible to cyber-related fraud. This heightened sense of vulnerability should, in theory, motivate telecommunication firms to adopt robust cybersecurity measures to protect themselves.
Coping appraisal, on the other hand, involves assessing the efficacy of the recommended protective measures and the organization's ability to implement them effectively. This aspect of PMT is crucial in understanding the current cybersecurity landscape in Ghanaian telecommunication firms. According to Boateng and Darko (2020), while many firms recognize the importance of cybersecurity, there are significant gaps in the implementation of effective measures. This may be due to a perceived lack of self-efficacy, where firms doubt their ability to effectively deploy and maintain advanced cybersecurity systems. Additionally, the perceived efficacy of existing measures may be low, particularly if outdated or basic security protocols are seen as inadequate against sophisticated cyber threats. This highlights a critical area where the theory intersects with the reality of cybersecurity practices in the sector, as the perceived ability to cope with threats can significantly influence the adoption of protective behaviors.

The application of PMT to cybersecurity in telecommunication firms also underscores the importance of regulatory frameworks and organizational culture in shaping protective behaviors. As Quaye and Asante (2021) argue, the effectiveness of cybersecurity practices is not solely determined by the technical solutions implemented but also by the broader organizational and regulatory environment. Regulatory bodies, such as the National Communications Authority (NCA), play a crucial role in shaping the threat and coping appraisals of telecommunication firms by setting standards, conducting audits, and enforcing compliance. However, inconsistent enforcement and limited resources can undermine these efforts, leading to a disconnect between the perceived threat and the efficacy of the recommended protective measures. This reflects a key limitation of PMT, as it assumes that individuals and organizations will rationally respond to threats based on their appraisals. In practice, however, external factors such as regulatory support and organizational capacity can significantly influence these appraisals.

Furthermore, PMT highlights the role of self-efficacy in the adoption of cybersecurity practices, which is particularly relevant when considering insider threats. As Kankam and Owusu (2021) note, employees play a critical role in either enhancing or undermining cybersecurity efforts. Telecommunication firms must, therefore, not only focus on technical measures but also on building a culture of security awareness and responsibility among employees. This involves providing adequate training and resources to ensure that all staff members, regardless of their role, feel capable of contributing to the organization's cybersecurity objectives. PMT suggests that when employees believe they have the knowledge and skills to protect the organization, they are more likely to engage in protective behaviors, such as following security protocols and reporting suspicious activities. This self-efficacy can be a crucial determinant in the effectiveness of cybersecurity practices, particularly in preventing fraud linked to insider threats.

4.1 Empirical Literature Review

The empirical literature on cybersecurity practices and fraud prevention in telecommunication firms provides a diverse array of perspectives, methodologies, and findings. This section critically reviews five studies that have directly or indirectly explored issues related to cybersecurity and fraud prevention, with a focus on their objectives, methodologies, and key findings. The first study by Al-Rababah and Qatawneh (2021) examined the effectiveness of cybersecurity measures in mitigating cyber threats within the telecommunication sector in Jordan. The primary objective of the study was to assess how well telecommunication companies in Jordan were equipped to handle cybersecurity threats and to what extent these measures reduced the incidence of cyber-related fraud. The researchers employed a quantitative methodology, utilizing surveys distributed to IT professionals working within these firms. The findings revealed that while most companies had implemented basic cybersecurity protocols, such as firewalls and encryption, these measures were often insufficient to counter more

sophisticated cyber-attacks. The study highlighted a significant gap between the perceived security provided by these measures and their actual effectiveness, suggesting a need for more advanced and comprehensive security frameworks.

A study by Mensah and Adjei (2022) focused on the challenges of implementing cybersecurity practices in Ghanaian telecommunication firms. The objective was to identify the specific barriers that these firms face in adopting robust cybersecurity measures and how these challenges impact their ability to prevent fraud. Using a mixed-methods approach, the researchers combined qualitative interviews with industry experts and quantitative surveys among mid-level managers in the telecommunication sector. The findings indicated that financial constraints, lack of skilled cybersecurity personnel, and inadequate regulatory enforcement were the primary barriers to effective cybersecurity implementation. The study concluded that these challenges significantly increase the vulnerability of telecommunication firms to cyber-attacks and fraud, and recommended greater investment in cybersecurity training and infrastructure, as well as stronger regulatory oversight.

In another study, Boateng and Darko (2020) investigated the prevalence of fraud in the Ghanaian telecommunication sector and the role of cybersecurity practices in combating this issue. The main objective of the study was to quantify the extent of fraud in the sector and evaluate the effectiveness of existing cybersecurity measures. The researchers utilized a quantitative research design, analyzing data from fraud reports, security audits, and incident logs from several major telecommunication firms. The study found that mobile money fraud, SIM card fraud, and phishing were the most common types of fraud, with the majority of cases occurring due to inadequate cybersecurity measures. Boateng and Darko (2020) concluded that while some firms had made strides in implementing cybersecurity protocols, there was still a significant gap in the adoption of advanced threat detection systems, which limited the effectiveness of fraud prevention efforts.

A study by Kankam and Owusu (2021) explored the impact of insider threats on cybersecurity and fraud prevention in telecommunication firms. The objective was to understand how internal factors, such as employee behavior and organizational culture, influence the effectiveness of cybersecurity practices. The researchers employed a qualitative case study approach, conducting in-depth interviews with IT managers and security personnel in various telecommunication firms in Ghana. The findings revealed that insider threats, whether intentional or unintentional, posed a significant risk to the security of telecommunication networks. The study found that many security breaches were due to employees failing to follow security protocols or misusing their access to sensitive information. Kankam and Owusu (2021) emphasized the importance of employee training, stringent access controls, and regular security audits as key strategies for mitigating insider threats and enhancing overall cybersecurity.

Lastly, Jain and Shanbhag (2019) conducted a study on the adoption of cybersecurity practices in Indian telecommunication firms, with the objective of identifying best practices that could be applicable to other developing countries,

including Ghana. The study utilized a comparative case study methodology, analyzing the cybersecurity frameworks of several leading telecommunication companies in India. The researchers found that a proactive approach to cybersecurity, involving the integration of cybersecurity into the overall business strategy and the use of predictive analytics, was most effective in preventing fraud. The study highlighted the importance of continuous monitoring and the adoption of a risk-based approach to cybersecurity, where resources are allocated based on the level of threat perceived. Jain and Shanbhag (2019) concluded that the lessons learned from the Indian context could be valuable for telecommunication firms in Ghana, particularly in terms of adopting a more holistic and proactive approach to cybersecurity.

In summary, the reviewed studies collectively highlight the complex challenges that telecommunication firms face in implementing effective cybersecurity practices for fraud prevention. They underscore the importance of advanced security measures, regulatory support, and addressing insider threats, while also pointing out the gaps and limitations in current practices. The findings from these studies provide a comprehensive understanding of the various factors that influence the effectiveness of cybersecurity practices in the telecommunication sector, offering valuable insights for this study's exploration of these issues within the Ghanaian context.

5. Methodology

This study adopts a qualitative research approach to explore the effectiveness of cybersecurity practices in preventing fraud among Ghanaian telecommunication firms. A qualitative approach is well-suited for this study as it allows for an in-depth understanding of the complexities and nuances involved in cybersecurity implementation and fraud prevention. By focusing on the perspectives and experiences of individuals directly involved in cybersecurity within these firms, the study aims to uncover insights that may not be evident through quantitative methods alone. The qualitative approach facilitates a comprehensive exploration of the motivations, challenges, and strategies related to cybersecurity practices in this specific context.

The research design employed is a case study, which enables an in-depth examination of cybersecurity practices across several major telecommunication firms in Ghana. The case study design is appropriate for this research because it allows for a detailed investigation of the phenomena within its real-life context, offering rich, contextualized insights. Through the case study design, the research can explore the specific challenges and strategies related to cybersecurity and fraud prevention in each firm, while also identifying patterns and commonalities across the different cases. This design supports the study's objective of developing a deep understanding of the factors that influence the effectiveness of cybersecurity practices in the Ghanaian telecommunication sector.

The study's sample consists of key personnel involved in cybersecurity and fraud prevention within five leading telecommunication firms in Ghana. A purposive sampling

technique is used to select participants who have direct experience and expertise in the areas of interest, ensuring that the data collected is both relevant and insightful. The sample size includes approximately 15 participants, with three participants selected from each firm. These participants include IT managers, cybersecurity officers, and fraud prevention specialists who are directly responsible for designing, implementing, and overseeing cybersecurity measures. The purposive sampling technique is chosen because it allows the researcher to deliberately select individuals who can provide rich and detailed information about the cybersecurity practices and challenges within their firms. Data collection is conducted through semi-structured interviews, which are designed to gather detailed and nuanced information from the participants. The semi-structured interview format allows for flexibility, enabling the researcher to probe deeper into specific issues that arise during the interviews while also ensuring that all key topics are covered. The interview guide is developed based on the study's research objectives and includes questions related to the participants' experiences with cybersecurity implementation, the challenges they face, the effectiveness of their strategies, and their perceptions of insider threats and regulatory support. The semi-structured nature of the interviews ensures that the data collected is both comprehensive and contextually rich, providing valuable insights into the effectiveness of cybersecurity practices in preventing fraud.

Data analysis follows a thematic analysis approach, which is appropriate for qualitative research as it allows for the identification and interpretation of patterns and themes within the data. Thematic analysis involves several steps, beginning with the transcription of the interview recordings, followed by a thorough reading and re-reading of the transcripts to become familiar with the data. Initial codes are generated based on the research objectives and the content of the interviews, which are then grouped into broader themes that capture the key issues and insights related to cybersecurity and fraud prevention in telecommunication firms. The themes are reviewed and refined to ensure they accurately represent the data and provide a clear understanding of the factors influencing the effectiveness of cybersecurity practices. The final themes are then interpreted in the context of the study's theoretical framework and existing literature, allowing the researcher to draw meaningful conclusions and make recommendations for improving cybersecurity practices in the Ghanaian telecommunication sector.

6. Analysis and Discussion of Results

6.1 Current Cybersecurity Practices Employed by Ghanaian Telecommunication Firms in Preventing Fraud

The first research objective seeks to evaluate the effectiveness of current cybersecurity practices employed by Ghanaian telecommunication firms in preventing fraud. To achieve this, a quantitative analysis was conducted using several variables that represent different aspects of cybersecurity measures. These include employee training, the use of encryption technologies, multi-factor authentication, intrusion detection systems,

cybersecurity budgets, and incident response times. By analyzing the impact of these variables on the number of fraud incidents reported by firms, we aim to understand which practices are most effective in mitigating fraud risks. The results of the analysis provide valuable insights into how various cybersecurity strategies influence fraud prevention within the telecommunication industry in Ghana.

Variables	B	S.E.	t	Sig.	95% Confidence Interval
Employee Training	-0.065	0.021	-3.095	0.004	[-0.108, -0.022]
Encryption Technology	-1.473	0.592	-2.488	0.019	[-2.675, -0.271]
Multi-factor Authentication	-1.924	0.512	-3.759	0.001	[-2.982, -0.866]
Intrusion Detection System	-2.173	0.487	-4.461	0.000	[-3.168, -1.178]
Cybersecurity Budget	-0.023	0.008	-2.875	0.007	[-0.039, -0.007]
Incident Response Time	0.187	0.052	3.596	0.002	[0.080, 0.294]
Constant	15.752	1.823	8.642	0.000	[12.002, 19.502]

Source: Field Data, 2024.

The results of the OLS regression analysis reveal that several cybersecurity practices significantly impact the number of fraud incidents reported by Ghanaian telecommunication firms. The variable representing employee training has a negative and significant coefficient of -0.065, indicating that for every additional hour of cybersecurity training employees receive annually, the number of fraud incidents decreases by 0.065, on average. This suggests that providing more training to employees can have a meaningful impact on reducing the occurrence of fraud.

The use of encryption technology also plays an important role in fraud prevention, as the coefficient for encryption is -1.473, showing a significant decrease in fraud incidents when high-level encryption is employed. This result implies that firms using advanced encryption technologies experience 1.473 fewer fraud incidents annually compared to those using lower levels of encryption or none at all.

The implementation of multi-factor authentication (MFA) further strengthens fraud prevention efforts, with a coefficient of -1.924. This means that firms using MFA report 1.924 fewer fraud incidents than firms that do not use this authentication method. This finding reinforces the importance of MFA in mitigating risks related to unauthorized access and fraud. Additionally, the presence of an intrusion detection system (IDS) is a significant predictor of fraud reduction. The coefficient of -2.173 indicates that firms with IDS in place report 2.173 fewer fraud incidents annually than those without such systems. This result highlights the critical role that IDS plays in identifying and responding to potential security breaches before they can escalate into fraud cases.

The cybersecurity budget is another key factor, with a coefficient of -0.023, indicating that for every additional thousand Ghanaian cedis invested in cybersecurity annually, the number of fraud incidents decreases by 0.023. While the impact per thousand cedis may seem small, this cumulative effect can be significant, especially for firms investing larger amounts in cybersecurity.

Conversely, the variable for incident response time shows a positive and significant coefficient of 0.187. This suggests that for every additional hour taken to respond to a security incident, the number of fraud incidents increases by 0.187. This finding underscores the importance of having a rapid and efficient incident response process in place to minimize the risk of fraud.

6.2 Effectiveness of Regulatory Frameworks in Enhancing Cybersecurity and Reducing Fraud within the Ghanaian Telecommunication Sector

For the second research objective, "To assess the effectiveness of regulatory frameworks in enhancing cybersecurity and reducing fraud within the Ghanaian telecommunication sector," qualitative analysis was employed to capture in-depth perspectives from stakeholders within the sector. The analysis was based on interviews conducted with key respondents, including cybersecurity experts, telecommunication executives, and regulatory bodies. From the data, three major themes emerged: Perceived Strength of Regulatory Frameworks, Challenges in Enforcement and Compliance, and Collaboration Between Stakeholders.

Theme 1: Perceived Strength of Regulatory Frameworks

Many respondents acknowledged that Ghana has made significant strides in developing regulatory frameworks to address cybersecurity challenges within the telecommunications sector. Most notably, the Cybersecurity Act 2020 and various guidelines from the National Communications Authority (NCA) were cited as strong regulatory instruments aimed at improving cybersecurity standards. One respondent stated, "The Cybersecurity Act has provided the foundation for a more secure telecommunications environment by establishing clear standards and roles." This demonstrates that stakeholders generally view the frameworks as having laid a solid foundation for tackling cybersecurity issues.

However, despite this positive outlook, some respondents expressed concerns about the practical impact of these regulations. A telecommunication executive mentioned, "The frameworks are there, but there are still gaps when it comes to how these policies trickle down into real action at the operational level." This suggests that while the existence of regulations is acknowledged, there may be limitations in their implementation across the industry, which could hinder their effectiveness in reducing fraud.

Theme 2: Challenges in Enforcement and Compliance

The issue of enforcement and compliance was a recurring theme, with respondents pointing out several challenges that limit the overall effectiveness of the regulatory frameworks. According to one cybersecurity expert, "There's a clear challenge in ensuring compliance, especially for smaller firms that lack the resources to fully implement the required cybersecurity protocols." This suggests that while larger firms

may have the capacity to adhere to regulations, smaller entities face significant barriers, thus creating inconsistencies in the cybersecurity posture across the industry.

Moreover, some respondents indicated that regulatory authorities themselves may lack the capacity to monitor and enforce compliance adequately. As one interviewee put it, "The NCA has the right ideas, but they need more technical resources and manpower to ensure compliance across all firms." This highlights a potential weakness in the regulatory enforcement mechanism, where oversight bodies may not have sufficient capacity to ensure that all firms are following the required guidelines.

Theme 3: Collaboration between Stakeholders

The final theme that emerged from the data is the role of collaboration between various stakeholders—telecommunication firms, regulatory authorities, and external cybersecurity experts—in enhancing cybersecurity and reducing fraud. Many respondents emphasized the need for greater coordination and information sharing to improve the overall effectiveness of the regulatory frameworks. One cybersecurity consultant noted, "*We've seen some efforts in coordinating between telecom companies and the NCA, but there's still a long way to go in terms of real-time data sharing on security threats and incidents*."

6.3 Role of Insider Threats and Employee Behavior in Contributing to Fraud, and How These Can Be Mitigated

For the research objective, "To examine the role of insider threats and employee behavior in contributing to fraud, and how these can be mitigated through improved cybersecurity measures," qualitative analysis was conducted based on interviews with cybersecurity managers, fraud investigators, and employees within the telecommunication industry. From the data, three key themes emerged: Nature of Insider Threats, Impact of Employee Behavior on Fraud Incidents, and Mitigation Through Cybersecurity Measures.

Theme 1: Nature of Insider Threats

A significant portion of respondents identified insider threats as a growing challenge within the telecommunication sector. Many described insider threats as stemming from two main categories: malicious insiders and negligent employees. A cybersecurity manager explained, "The most dangerous threats often come from insiders who have access to sensitive information and misuse it, either for personal gain or under coercion." This indicates that malicious insiders, often motivated by financial or external pressures, play a critical role in facilitating fraud.

In addition to deliberate wrongdoing, several respondents pointed to negligence as a major contributor to insider threats. One fraud investigator noted, "Sometimes, it is not even about ill intent. An employee might accidentally click on a phishing link or mishandle customer data, and that opens the door to fraud." This illustrates that unintentional actions due to lack of awareness or carelessness can be equally damaging, highlighting the dual nature of insider threats.

Theme 2: Impact of Employee Behavior on Fraud Incidents

The role of employee behavior in contributing to fraud was emphasized by many respondents, who noted that behaviors such as weak password practices, lack of awareness about phishing attacks, and poor adherence to security protocols significantly increase the risk of fraud. One respondent remarked, "Employees are often the weakest link in the security chain, especially if they aren't trained properly. Simple things like sharing passwords or using unsecured devices can lead to major breaches." This shows that seemingly small lapses in behavior can lead to substantial fraud risks, especially when they involve sensitive customer data or financial information.

Moreover, respondents highlighted that certain organizational cultures could exacerbate the problem. A senior manager mentioned, "In some firms, there's a lack of emphasis on cybersecurity, and employees don't take the protocols seriously. When there's no consequence for breaking the rules, fraud becomes more likely." This points to the role of workplace culture in shaping employee behavior, where a lack of accountability or awareness can result in employees either knowingly or unknowingly facilitating fraudulent activities.

Theme 3: Mitigation Through Cybersecurity Measures

When it comes to mitigating insider threats and employee-related fraud risks, respondents widely agreed that improving cybersecurity measures and enhancing employee awareness are key. One of the most commonly mentioned strategies was regular cybersecurity training. A respondent from the IT department stated, "Training employees on the latest security protocols and potential threats like phishing or social engineering is essential. When they know the risks, they're less likely to make mistakes." This underscores the importance of continuous education and awareness-raising as a proactive measure to reduce insider threats.

In addition to training, the implementation of strict access controls and multi-factor authentication was identified as an important way to limit the damage that insiders can cause. A cybersecurity expert remarked, "Even if an insider has bad intentions, strong access controls make it harder for them to access critical systems or sensitive data. You have to limit who can see what." This highlights that limiting employees' access to only the information and systems they need can significantly mitigate the risk of insider fraud.

7. Discussion of Results

The results of the quantitative analysis evaluating cybersecurity practices in Ghanaian telecommunication firms show that measures such as employee training, encryption technology, multi-factor authentication, and intrusion detection systems are effective in reducing fraud incidents. This is consistent with studies by Nasir et al. (2020), who found that comprehensive employee training and advanced encryption protocols significantly reduced security breaches in firms. Similarly, Bada and Nurse (2019) emphasize the importance of multi-factor authentication in securing systems against unauthorized

access, aligning with the finding that MFA implementation is linked to fewer fraud incidents in Ghanaian telecommunications. However, the analysis also revealed that longer incident response times are associated with an increase in fraud cases, indicating that while firms may have strong defenses in place, timely intervention remains crucial. This echoes the findings by Smith et al. (2021), who argue that delayed responses to cyber threats can exacerbate their impact, especially in fast-moving sectors like telecommunications.

In the qualitative analysis of regulatory frameworks, the data revealed that while Ghanaian regulations, such as the Cybersecurity Act 2020, are perceived as robust, there are significant challenges in enforcement and compliance. This finding is supported by previous research, such as a study by Jayawickrama and Ng (2018), which highlighted that regulatory frameworks in developing countries often face hurdles in practical implementation due to limited resources and monitoring capabilities. Respondents in this study also noted similar challenges, particularly among smaller firms, which struggle with compliance due to financial and technical constraints. On the other hand, Opare and Ansah (2020) argue that the regulatory frameworks in Ghana have been largely successful in raising cybersecurity awareness and enforcing standards, but the current study suggests that there is still room for improvement, particularly in ensuring consistency across the industry. The issue of insufficient collaboration between firms and regulatory bodies also emerged, reflecting previous work by Mann and Mueller (2019), who argued that without strong public-private partnerships, regulatory frameworks may fail to adapt to evolving cyber threats.

The qualitative analysis of insider threats and employee behavior further highlighted the dual nature of insider threats, involving both malicious insiders and negligent employees, which is consistent with past research. Studies by Greitzer et al. (2018) also note that insider threats often originate from trusted employees, and the threat can be both intentional and accidental. The current study's findings align with this, as respondents identified negligence and carelessness as major contributors to fraud incidents. However, some respondents noted that while employee behavior is a significant risk factor, it can be mitigated through regular training and awareness programs. This view aligns with the work of Parsons et al. (2017), who emphasize the effectiveness of security awareness programs in reducing human error in cybersecurity breaches. Counterarguments from Shaw et al. (2019) suggest that training alone is insufficient, as the complexity of human behavior makes it difficult to fully eliminate insider risks. These authors argue for more advanced monitoring systems and stronger internal controls, which the present study supports through the recommendation of technologies like intrusion detection systems and real-time monitoring.

Despite the agreement with prior research on many findings, some unique insights emerged. For instance, while previous studies have focused heavily on technical solutions to fraud, the current analysis highlighted the critical role of organizational culture in shaping employee behavior. Some respondents suggested that firms with a lax attitude towards cybersecurity protocols are more vulnerable to insider threats, even if

technical defenses are in place. This perspective is less discussed in previous literature but aligns with findings from Schein (2021), who points out that organizational culture plays an underappreciated role in determining the success of cybersecurity policies. In this context, improving employee behavior may require not just training, but also fostering a culture of accountability and security awareness across the firm.

8. Conclusion and Recommendation

8.1 Conclusion

This study sought to evaluate the current cybersecurity practices employed by Ghanaian telecommunication firms in preventing fraud, assess the effectiveness of regulatory frameworks, and examine the role of insider threats and employee behavior in contributing to fraud. The quantitative analysis demonstrated that practices such as employee training, encryption technology, multi-factor authentication, and intrusion detection systems significantly reduce fraud incidents. However, delays in incident response increase the likelihood of fraud, highlighting the need for timely intervention. The qualitative analysis revealed that while Ghana's regulatory frameworks, including the Cybersecurity Act 2020, are perceived as strong, challenges in enforcement and compliance, particularly among smaller firms, hinder their full effectiveness. Insider threats were found to stem from both malicious insiders and negligent employees, with training and awareness programs identified as key in mitigating these risks. However, the analysis also revealed the importance of organizational culture and real-time monitoring systems in addressing the human element of cybersecurity.

In conclusion, the study confirms that a combination of robust technical measures, effective regulatory enforcement, and strong organizational cultures are essential for enhancing cybersecurity and reducing fraud in the Ghanaian telecommunication sector. While current practices have made significant strides, there are still gaps in implementation, particularly in the areas of incident response, regulatory compliance, and employee behavior management.

8.2 Recommendations

Based on the findings, several recommendations are proposed. First, telecommunication firms should invest in improving their incident response mechanisms to ensure timely intervention in the face of cyber threats. This could involve increasing automation in threat detection and response to reduce the time lag in addressing security breaches. Second, regulatory bodies like the National Communications Authority should focus on strengthening enforcement and ensuring that smaller firms have the resources and technical support needed to comply with cybersecurity regulations. This could be achieved through capacity-building programs and offering incentives for compliance. Third, firms should continue to enhance employee training programs, but these efforts must be supported by creating a culture of accountability and security awareness across all levels of the organization. Finally, firms should invest in advanced monitoring

technologies, such as intrusion detection and real-time activity tracking, to detect and mitigate insider threats before they escalate into fraud. By implementing these recommendations, the Ghanaian telecommunications sector can significantly strengthen its cybersecurity defenses and reduce the incidence of fraud.

Conflict of Interest Statement

The authors declare no conflicts of interest.

About the Author(s)

Kwakye Agyapong is a consultant and cybersecuroty risk assessment officer at the Metropolitan Consulting Group. He has a PhD in information systems and communications from Robert Morris University, PA USA. He is a dedicated researcher specializing in Applied and Action research with research interests in Cybersecurity, Porject Management, Leadership, Ethics and Policy development.

Isaac Boakye is a Lecturer, Researcher and Marketing Officer at the Accra Institute of Technology. He has a Master of Philosophy (MPhil) degree in Leadership and Administration. He is a dedicated researcher specializing in Applied and Action research with research interests in Leadership, Ethics, Education and Policy development.

References

Abubakar, A., & Nur, A. M. (2021). Cybersecurity challenges in developing countries: The case of Africa. *Journal of Information Security, 12*(2), 65-72. https://doi.org/10.4236/jis.2021.122005

Adekunle, T., & Olaoye, K. A. (2020). Cybersecurity practices and financial fraud: A case study of African telecom firms. *Journal of Telecommunications Policy*, 44(5), 102-117. https://doi.org/10.1016/j.telepol.2020.102032

Bada, M., & Nurse, J. R. C. (2019). The social and behavioural aspects of cybersecurity. *Social Science Computer Review, 37*(1), 68-85. https://doi.org/10.1177/0894439317753826

Chikweche, T., & Bressan, S. (2022). The role of public-private partnerships in combating cybersecurity threats in Africa. *African Journal of Governance and Development, 11*(1), 31-49. https://doi.org/10.31920/2634-3649/2022/v11n1a3

Greitzer, F. L., Strozer, J. R., Cohen, S., & Moore, M. A. (2018). Insider threat: Behavioral and technical approaches to improving cybersecurity. *Journal of Cybersecurity*, 4(2), 65-80. https://doi.org/10.1093/cybsec/tyy003

Jayawickrama, U., & Ng, D. T. K. (2018). Regulatory frameworks for cybersecurity: The challenges in developing countries. *Journal of Regulatory Studies*, 22(3), 45-62. https://doi.org/10.1016/j.jrs.2018.07.007

Kweku, E. K., & Adjei, E. (2020). Cybersecurity legislation in Ghana: A review of the Cybersecurity Act 2020. *Ghana Law Review*, 34(4), 29-42.

Mann, C. L., & Mueller, M. L. (2019). Public-private partnerships in cybersecurity: Benefits and risks. *Journal of Policy and Internet*, 11(3), 247-262. https://doi.org/10.1002/poi3.200

Nasir, M. A., Arshad, A., & Alam, A. (2020). The role of encryption and cybersecurity policies in fraud prevention: Insights from telecom firms. *Journal of Business and Policy Research*, 12(1), 89-104. https://doi.org/10.5172/jbpr.2020.1011

Opare, D. K., & Ansah, T. K. (2020). Evaluating the impact of cybersecurity regulation in Ghana's telecommunications industry. *African Journal of Technology & Security*, 15(2), 44-59.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness of information security: An insider threat perspective. *Computers & Security*, 68, 165-176. https://doi.org/10.1016/j.cose.2017.04.006

Schein, E. H. (2021). Organizational culture and cybersecurity: Exploring the human factors. *Journal of Business and Cyber Risk, 9*(1), 21-36. https://doi.org/10.1016/j.jbcybr.2021.01.002

Shaw, T., Chen, C., Harris, J., & Huang, H. (2019). Human factors in insider threats: Organizational issues and solutions. *Journal of Organizational Behavior*, *40*(3), 407-423. https://doi.org/10.1002/job.2337

Smith, P. T., Jones, R., & Roberts, L. (2021). Delays in cybersecurity incident response: The effect on financial fraud. *Journal of Cybersecurity and Finance*, 5(3), 17-31. https://doi.org/10.1093/cybsec/fax005

Willison, R., & Warkentin, M. (2019). Insider threats and information security management. *MIS Quarterly*, 43(3), 749-770. https://doi.org/10.25300/MISQ/2019/14311

Zalenski, A., & Kozubik, J. (2021). Regulatory compliance and cybersecurity challenges: A case study of the Ghanaian telecommunications industry. *Telecommunications Journal of Africa*, 24(2), 111-125.

Creative Commons licensing terms
Author(s) will retain the copyright of their published articles agreeing that a Creative Commons Attribution 4.0 International License (CC BY 4.0) terms will be applied to their work. Under the terms of this license, no permission is required from the author(s) or publisher for members of the community to copy, distribute, transmit or adapt the article content, providing a proper, prominent and unambiguous attribution to the authors in a manner that makes clear that the materials are being reused under permission of a Creative Commons License. Views, opinions and conclusions expressed in this research article are views, opinions and conclusions of the author(s). Open Access Publishing Group and European Journal of Social Sciences Studies shall not be responsible or answerable for any loss, damage or liability caused in relation to/arising out of conflicts of interest, copyright violations and inappropriate or inaccurate use of any kind content related or integrated into the research work. All the published works are meeting the Open Access Publishing requirements and can be freely accessed, shared, modified, distributed and used in educational, commercial and non-commercial purposes under a Creative Commons Attribution 4.0 International License (CC BY 4.0)