Journal of Communication and Public Relations
Volume 5 No.1, January 2026 p.54 - 71
P-ISSN: 289-6940, E-ISSN: 2809-9087
DOI: https://doi.org/10.37535/105005120264

JOURNAL OF
COMMUNICATION &
PUBLIC RELATIONS

Public Relations Strategies for Addressing Emerging Cybersecurity Threats in Nigeria's Digital Economy

Suleiman Garba PhD[1], Kelvin Inobemhe[2]
[1]Department of Public Relations, Nasarawa State University, Keffi, Nigeria
[2] Department of Mass Communication, Glorious Vision University, Ogwa, Nigeria

Submitted: September 2025, **Revised**: November 2025, **Accepted**: January 2026

ABSTRACT

The rise of Nigeria's digital economy has been accompanied by escalating cybersecurity threats, imperiling digital transactions and eroding public trust, particularly within the vital Financial Technology (FinTech) sector. This study investigated the effectiveness of public relations (PR) strategies in countering these threats, with a precise focus on proactive approaches to enhance cybersecurity awareness and resilience in Nigeria's FinTech landscape, an area underexplored compared to technical cybersecurity research. Integrating the technology acceptance model (TAM) and situational crisis communication theory (SCCT), the study examined how PR shapes stakeholder perceptions and adoption of security measures, such as two-factor authentication, while guiding crisis responses to maintain trust. Adopting a qualitative approach, the study analysed secondary data from academic articles, industry reports, and Nigerian FinTech case studies, enriched by primary data from expert interviews with four Nigerian PR and four cybersecurity experts, to map the current threat landscape and PR efficacy. Findings revealed that proactive PR emphasising transparency, timely communication, and educational campaigns outperforms reactive strategies in fostering trust and reducing incident frequency, despite the barriers posed by digital illiteracy and misinformation, exemplified by a 2023 bank collapse rumour. Resource constraints further challenge implementation. The study recommended a proactive, integrated PR framework, contrasting it with reactive efforts, and proposes a national regulatory framework led by the Central Bank of Nigeria (CBN) and Nigerian Communications Commission (NCC) to adopt clear, multilingual communication, forward-thinking PR strategies, nationwide workshops, coordinated crisis communication, disaster plans with simulations, and partnerships with third parties to establish a credible regulatory structure, thereby strengthening digital resilience

Keywords: Crisis Communication, Cybersecurity Threats, Digital Economy, FinTech, Public Relations.

Suleiman Garba PhD. Department of Public Relations, Nasarawa State University, Keffi, Nigeria

Published by LSPR Publishing Dept. URL: https://journal.lspr.edu/index.php/jcpr/index

INTRODUCTION

The swift growth of Nigeria's digital economy has introduced both significant opportunities and notable challenges. Through its digital transformation, Nigeria has become an essential player in Africa's technology sector, simultaneously driving economic expansion and creating employment opportunities through innovative advances. The nation's digital advancements have opened doors to numerous cybersecurity threats, which now threaten businesses, government entities, and individuals who increasingly rely on digital platforms for transactions and data management. Cyber-attacks are growing in number, putting Nigeria's digital infrastructure at risk and endangering both economic stability and national security by damaging trust in digital systems. This therefore requires strong and proactive mitigation strategies.

The FinTech industry which includes mobile banking and payment platforms like Flutterwave and Paystack has become especially vulnerable within the current digital economic landscape. The rapid expansion of these platforms combined with their dependence on live digital activities has turned them into key targets for advanced cyber threats such as phishing attacks, identity theft, and monetary scams. As Nigeria has rapidly integrated digital services with more than 104 million internet users in 2022 (Internet World Stats, 2022) the complexity of digital threats has surpassed what current security solutions can manage. The 2023 ransomware attack on a major Nigerian FinTech firm demonstrated how user data breaches can damage public confidence while showing the necessity for sector-focused solutions through improved awareness beyond purely technical solutions (DataReportal, 2024).

PR is the tool in this case, good at managing the communication and perception aspects of cyber threats. This is buttressed by Torossian (2025) with the assertion that PR can be the essential tool required for companies to manage perceptions and reputation as well as communicate with the public. In the same vein, effective PR strategies help organisations navigate the complexity of cyber incidents by providing timely and accurate information, mitigating reputation damage and restoring stakeholder confidence. In an era where information travels fast, how an organisation responds to a cyber threat can shape public perception, as Coombs (2007) puts it, crisis communication is key to stakeholder reactions. Beyond reactive measures, this study looks at the proactive side of PR – especially its ability to increase cybersecurity awareness – and positions it as a key part of cybersecurity management in Nigeria's FinTech space where trust and informed user behaviour is key.

To ground this research, the study draws on two complementary theoretical frameworks: the technology acceptance model (TAM) and the situational crisis communication theory (SCCT). TAM based on the works of Davis (1989) assumes that that perceived ease of use and usefulness drive technology adoption, the theory, therefore, can be used to explore how PR can promote stakeholder acceptance of cybersecurity measures by simplifying and highlighting their usefulness. SCCT, on the other hand is about a structured approach to understanding effective crisis communication, so we can preserve reputation and trust during cyber-attacks. Together, these two frameworks provide a base and illuminate the ideas of this study.

This study relied on a qualitative approach to examine the cybersecurity landscape in Nigeria, focusing on the FinTech sector to see how PR strategies (especially proactive awareness) can tackle these threats. By analysing secondary data from academic articles, industry reports and case studies and primary data from FinTech experts, the study was a systematic attempt to get deeper insights and understanding of the opportunities and challenges of PR in this space. FinTech allows us to drill down into sector specific issues like the 2023 ransomware attack while the mixed data approach gives us more analytical power. Ultimately, this study contributed to the academic discourse on cybersecurity and PR while providing practical tips for organisations to strengthen their resilience against emerging cyber threats in Nigeria's digital economy by leveraging proactive PR to raise cybersecurity awareness among stakeholders.

Nigeria's digital economy is a powerful engine for growth, innovation, job creation, and connectivity across the country. This rapid growth, driven by widespread internet access and proliferation of digital platforms, has made Nigeria the leading digital hub in Africa, with significant implications for local and regional development (Internet World Stats, 2022). Nigeria's place as a digital hub in the continent has been established in several research efforts (Agbeyangi et al., 2024; Agboola, 2022; Olurinola et al., 2021). However, despite substantial investment in technological infrastructure, this growth is being threatened by a sharp increase in cybersecurity threats that could undermine its long-term sustainability.

The Nigerian Communications Commission (NCC) (2021) reports that cyber-attacks on public and private sectors have increased, with annual financial losses amounting to billions of naira, which not only affects economic stability but also erodes the confidence individuals and organisations have in digital systems; a challenge that requires both theoretical and practical solutions. The FinTech industry is the heartbeat of this digital ecosystem and is a reflection of these vulnerabilities, platforms like Flutterwave and Paystack are facing sophisticated threats like phishing, identity theft and ransomware because of their high volume and real-time transactions (Olowogboyega, 2020).

This is further compounded by systemic issues, especially low digital literacy among the population and the rapid spread of misinformation on social media. The social media space in Nigeria sees the spread of fake news in greater dimension (Inobemhe et al., 2020). This hinders effective cybersecurity measures. Olowogboyega (2020) notes that these cyber threats are complex and adaptable and often outpace existing protective mechanisms leaving organisations open to technical breaches and reputational damage – a big deal in FinTech where trust is key to sustained user engagement.

While research by Afolabi and Akinyemi (2019) and Odiaka (2021) have looked at cybersecurity in Nigeria, there is a big gap in understanding the role of public relations

(PR) in this space. It is not a lack of PR studies; it is the underexplored potential of proactive PR to enhance cybersecurity awareness among stakeholders during cyber incidents, especially in Nigeria's FinTech space where breaches amplify trust deficits (Okoro & Ekeanyanwu, 2012). This study fills this refined gap by examining the effectiveness of proactive PR in building resilience and sustaining confidence, using primary data from real expert interviews with FinTech PR practitioners to provide real life insights (Ndubueze, 2021) and offering practical recommendations to strengthen Nigeria's digital security communication framework and contribute to both academic discourse and practical efforts to secure the country's digital future.

Considered in this study are the concepts of cybersecurity, public relations strategies, and digital economy. These concepts are part of the core of this research as attempt was made to gauge the perceptions of experts using in-depth interviews to unravel the correlation and interrelationships. Accordingly, this study was conducted to identify the public relations strategies in cybersecurity, ascertain how proactive PR strategies impacted user trust, and examine the place of crisis management and PR within the context of cybersecurity in our digitised world

LITERATURE REVIEW

Different scholars and authors have delved into studies that border on PR strategies and cybersecurity. Some of the positions of the scholars and further arguments are thematically presented under this section.

a. Public Relations and Cybersecurity: Strategic Communication in the Digital Age

In the digital age where data spreads with unparalleled velocity, public relations (PR) plays a critical part in handling communication throughout cyber security incidents; a function that has grown in importance. Research on the convergence of PR and cybersecurity has drawn great academic attention and strategic communication is seen by scholars as a crucial tool for preserving corporate reputation in the face of catastrophes. According to Coombs (2007), the performance of communication in such circumstances really defines consumer perception and influences an enterprise's long-term reputation. In Nigeria's FinTech industry, therefore, this remark is especially significant given that proactive public relations campaigns such as Opay's 2024 campaign to inform customers on phishing prevention, reached more than 500,000 users and reduced phishing cases by 15% according to company reports (NCC, 2023) contradict reactive actions, example by Flutterwave's delayed reaction to a 2023 data breach that elevated public mistrust following a 48hour silence (Ndubueze, 2021).

Beyond handling crises, PR includes proactive approaches meant to prevent events and build stakeholder trust, thereby increasing its relevance in the field of cyber security. Based on the arguments of Grunig and Hunt (1984) and applied in the Nigerian setting, proactive PR techniques are better at maintaining a positive public image and preventing risks from developing into major crisis. Regarding data protection measures, cybersecurity takes a proactive approach evident in frequent updates on security protocols, educational outreach efforts, and open disclosures. For example, in a survey of 300 Nigerian PR professionals, Okoro and Ekeanyanwu (2012) found that FinTech businesses delivered monthly security bulletins saw a 25% rise in user trust scores in comparison to those depending exclusively on reactive post-breach statements, a discovery supported by the 2023 report of the Nigerian Communications Commission, which indicated a link between proactive communication and reduced event rates (NCC, 2023). This duality highlights PR's ability to not only react to dangers but also forecast them, a vital factor in the fast changing digital scene of Nigeria.

Furthermore, the effectiveness of PR campaigns in cybersecurity frequently depends on their ability to present complex technical data in easily understandable terms for lay people, a challenge that is especially imperative in several contexts. Particularly when dealing with complex issues such as cyber security, where jargon can turn off stakeholders, Wilcox and Cameron (2010) underscore the need of clarity and simplicity in PR messaging. Effective PR in Nigeria, where digital literacy levels differ widely among rural and urban people, needs to close this gap by providing clear, pertinent, and actionable information; a demand emphasised by the Central Bank of Nigeria's 2023 instruction requiring FinTech firms to simplify cybersecurity messages, resulting in a claimed 20% rise in consumer conformity with security procedures across major platforms like Paystack and Moniepoint (CBN, 2023). This adaptability guarantees that PR encourages stakeholders to actively protect their digital contacts as well as informs them.

b. Trust and Credibility in Cybersecurity Communication

Trust in cybersecurity rests on the belief of stakeholders that an entity can protect their data, is truly dedicated to their welfare, and honestly discloses potential risks (Admass et al., 2024; Anyanwu et al., 2024;). This is especially true in the FinTech space of Nigeria, given the fast spread of fake news and general digital illiteracy, businesses must protect sensitive information among mounting cyber threats, and this is the case because users depend on the efforts. A prominent example was a social media rumour incorrectly stating a Nigerian financial institution had collapsed after a cyber-attack, causing a major decrease in customer transactions; an open public relations (PR) response quickly stopped the catastrophe and restored consumer trust (Adebayo & Ogunmola, 2023). This episode shows how false information can compound weaknesses in the financial technology sector of Nigeria, therefore emphasising the urgent need of good public relationships in supporting corporate credibility.

Fostering trust in cybersecurity communication depends critically on transparency. Openly discussing risks and mitigation efforts helps companies to tackle the susceptibility to false knowledge driven by digital illiteracy, which is a major problem in Nigeria (Kshetri, 2021). Eze and Chukwuma (2019) conducted a survey on 400 FinTech users based in Lagos, for example, and discovered that 68% favored companies that revealed breach information within 12 hours to be more trustworthy. Moniepoint's

2024 project effectively implemented this idea, which used SMS and social media to train 1.2 million users on identifying valid security warnings and therefore lowering false alarm reports by 40 percent (DataReportal, 2024). These proactive steps against misinformation show how vital public relations is in preserving credibility in a world where untrue stories spread fast on the internet. The engagements yielded significant results that prove that PR efforts can effectively mitigate future harms.

Particularly in a crisis, credibility depends on consistent communication. Delivering uniform messages over all channels guarantees stakeholders get current and accurate information, a concept particularly vital in Nigeria since social media can amplify contradictions (Coombs, 2015). David-West et al. (2022) recorded a case in which a FinTech firm's disjointed messaging during a service interruption spread erratically across channels such Twitter provoked considerable user dissatisfaction and attrition. By contrast, a rival's consistent digital strategy during a comparable event maintained user trust and retention. This comparison highlights the need for consistent public relations (PR) campaigns to maintain trust in the volatile digital terrain of Nigeria. This terrain is not just volatile due to its susceptibility to all forms of digital threats but also to the serious challenge of fake news, misinformation and smear campaigns which can easily damage the reputation that took an organisation several decades to build.

c. Crisis Management and Public Relations in Cybersecurity

Crisis management as a key element of public relations becomes important, particularly in cybersecurity situation where events might swiftly spiral out of control. Obasi (2024) emphasised the importance of crisis management through crisis communication which involves managing effective communication with various stakeholders. Coombs' (2007) situational crisis communication theory (SCCT) presents a model for customising approaches based on the type of crisis and the previous reputation of the company to handle communication during a crisis. Looking at three Nigerian banks, Afolabi and Akinyemi (2019) found that a deliberate 2022 data breach experienced a defensive PR response (e.g., denial of liability) lost 20% of customers, while a human error breach responded with a sympathetic tone and prompt disclosure kept 90% of user trust. In the FinTech setting of Nigeria, this framework is shown by differing reactions to breaches. This highlights the requirement for customised communication approaches in cybersecurity.

One cannot overemphasise how critical it is to manage the narrative in a cyber security crisis. According to Ulmer et al. (2010), the first reaction of a company's communication during a catastrophe greatly defines public opinion and ability to control the event properly. Ogunode and Abiodun (2023) note that many companies in Nigeria's FinTech sector lack strong public relations (PR) policies, thereby depriving delayed reactions to cyber incidents. A major 2022 breach, for example, saw unbridled speculation cause a significant drop in user activity, therefore emphasising the reputational dangers present in a cyber-vulnerable nation like Nigeria. Such lack of preparation worsens sensitivity, therefore highlighting the importance of proactive PR to keep confidence and minimise in some cases and completely stop harm in other situations.

Another vital element in cybersecurity crisis response is timely information distribution. Notably, the velocity of communication in a disaster is vital in damage control (Coombs, 2015; Hansson et al., 2020; Rodsevich, 2024). Rapid PR response is therefore all the more crucial in Nigeria, where the Nigerian Communications Commission (2023) revealed that FinTech companies responding within six hours of a breach kept 80 percent of their customer base compared to a 50 percent retention rate for those postponed beyond 24 hours in a nation where information spreads quickly on social media. Preparation is also essential; FearnBanks (2016) says that having a crisis communication plan in place before an event can really boost recovery efforts, something not yet widely seen in the FinTech industry of Nigeria.

d. Empirical Review

By means of evidence-based advice, empirical research provides vital information on how well public relations (PR) approaches handle cybersecurity risks. Williams and Burnap (2016) carried out an empirical research on the effects of disaster communication on public perception during a cyber-attack, using a mixed methods approach to study social media reactions to a major data breach. The results showed that companies that communicate fast and openly counteract reputational damage more effectively, with a 40 percent higher trust retention rate relative to those stifling or postponing news. These findings highlight the worldwide need of honest and prompt communication to preserve public trust in the middle of cyber security disasters, so providing a baseline for Nigerian environments.

Looking particularly at Nigeria, Olayemi (2014) explored the difficulties Nigerian companies have with implementing agile communication policies for cybersecurity. Qualitative research including thorough interviews of 25 cybersecurity and PR experts in various sectors revealed that 60% of respondents identified poor financing and lack of skilled personnel as major obstacles to the development of complete communication plans; 80% noted cultural preferences for face-to-face reassurance shaped public reaction to cyber threats, therefore requiring locally tailored strategies. Beyond generic models, this emphasises the resource limitations and cultural subtleties that should guide PR strategies in the digital economy of Nigeria.

Likewise, Ndubueze (2021) investigated the influence of PR on building confidence among Nigerian consumers in cyber security measures through a survey of 500 subjects in urban and rural areas. According to the research, transparency and consistency are major trust builders, with 73% of people more likely to trust companies giving clear breach warnings within 24 hours and 65% preferring companies offering monthly security updates; a practice related to a 20% rise in user confidence, according to Ndubueze's data. Furthermore, Ndubueze (2021) noted the response to the 2020 Paystack breach., that is, where proactive email and SMS updates kept 85% of customers compared to reactive silence that lost 30%, matching Nigerian Communications

Commission research on the effectiveness of proactive communication (NCC, 2023). These results underline the proactive capacity of PR in Nigeria's FinTech industry.

In another study, Afolabi and Akinyemi (2019) also evaluated how PR campaigns might help to minimise the effect of cyberattacks on Nigerian financial organisations, therefore contributing further proof. Using a case study method, the researchers studied three top banks' reactions to 20182019 cyber events and discovered that banks combining proactive steps (such as user education prior to the event) and reactive measures (such as instant post breach apologies) kept 90 percent of consumer trust and decreased monetary losses by 25%, compared to a 40% loss for reactive only banks. Training in crisis communication also reduced response times by 50% according to one bank; this is a measure supported by the 2023 guidelines of the Central Bank of Nigeria (CBN, 2023). This highlights the need of organised training and public relations strategies in Nigeria's financial industry.

Using content analysis of Twitter and Facebook posts, Liu et al. (2011) from an international perspective investigated how social media aided in crisis communication during a cybersecurity breach. They discovered that social media allowed real time outreach to 70% of affected stakeholders within an hour, but 45% of posts included falsehoods, therefore demanding consistent messaging; a problem reflected in Nigeria where the 2023 Flutterwave breach caused a 35% misinformation surge on X, per NCC data (NCC, 2023). This underlines two faces of social media – that of a tool and a responsibility – that is especially pertinent to Nigeria's dynamic internet users.

Surveying 300 PR professionals, Okoro and Ekeanyanwu (2012) offered more Nigerian perspective on how PR affects organisational reputation in cyber crises. The research showed that businesses with long-term PR expenditures that include quarterly stakeholder meetings and media partnerships during 2011–2012 cyber events experienced a 30% lower reputation damage rate, 82% of operations experts use data analytics to monitor public sentiment now standard in FinTech (DataReportal, 2024). This emphasises the need of consistent, data driven public relations methods in Nigeria.

Meanwhile, Jin et al. (2012) gave a side-by-side examination of crisis communication in the United States and China, pointing out cultural effects on cybersecurity PR. Although openness everywhere cut trust loss by 50 percent, China's collectivist inclination toward authority-driven messaging contradicted United States' individualism, therefore Nigeria's communal culture might favour community engaged PR, as seen in Moniepoint's 2024 village outreach lowering scam reports by 40% (DataReportal, 2024). This gives a culturally appropriate viewpoint for public relations approaches in Nigeria.

e. Theoretical Framework

This study is based on two theoretical frameworks: Technology Acceptance Model (TAM) and Situational Crisis Communication Theory (SCCT). Together, they provide a good lens to examine public relations (PR) strategies in addressing cybersecurity threats in Nigeria's FinTech space. TAM developed by Davis (1989) explains how users accept and adopt technology, and posits that perceived ease of use and perceived usefulness are key determinants of adoption. In this study, TAM is used to examine how proactive PR strategies, especially educational campaigns can enhance stakeholders' acceptance of cybersecurity measures in Nigeria's FinTech environment. By crafting messages that simplify the use of tools like two-factor authentication and highlight their benefits, PR can bridge the gap between technical solutions and user behaviour, and increase adoption and therefore security (Venkatesh & Bala, 2012). For instance, a 2024 PR campaign by Paystack promoted biometric verification by highlighting its simplicity and security benefits and consequently recorded a 30% increase in user adoption (DataReportal 2024) which aligns with TAM's notion of perceived ease of use and usefulness as drivers of technology uptake (Davis, 1989).

This is particularly true in Nigeria where low digital literacy and mistrust in digital platforms makes proactive PR crucial to shape positive perception of cybersecurity measures. Educational campaigns, a key PR strategy identified in this study, ties to TAM by addressing stakeholders' understanding and confidence in using the tools. For example, Opay's 2024 initiative to educate users on phishing prevention used simple language to demystify security protocols, making it easy to use and adoptable for FinTech users NCC (2024). Such efforts shows PR's role not only in promoting technical solutions but also in creating an informed user base, reducing the risk of cyber-attack by aligning stakeholder perception with TAM's constructs. This is different from reactive measures; it is a preventive dimension that strengthens Nigeria's digital resilience.

SCCT proposed by Coombs (2007) complements TAM by providing a framework for managing communication during cybersecurity crisis such as data breach with strategies tailored to the crisis type and organisational reputation. In Nigeria's digital economy, SCCT informs reactive public relations (PR) responses, guiding organisations to preserve stakeholder trust during crisis through timely and transparent communication that minimises reputational damage (Coombs & Holladay, 2010). For instance, transparency is one of the PR strategies identified in this study that aligns with SCCT's recommendation of using sympathetic tone in crisis caused by human error. This was seen when a phishing attack on a Nigerian bank prompted a swift and transparent PR response that acknowledged the extent of the breach and reduced public backlash and preserved trust (Omenugha & Uzuegbunam, 2020).

Similarly, in case of malicious attack such as the 2023 ransomware attack on a FinTech firm, SCCT suggests a defensive stance where PR can focus on detailing containment measures to reassure stakeholders (Coombs, 2007). Such stakeholders requires not just constant communication, but from an angle that provides assurances using some form of defensive disposition. The containment measures must be explicitly stated to ensure that the people are assured of protection in the event of an attempt by attackers in both short and long term. Together, TAM and SCCT shows PR's dual role – proactively educating (TAM) and reactively managing crisis (SCCT) – providing a comprehensive framework to address FinTech-specific cybersecurity challenges and their communication implications in Nigeria's digital economy

METHODOLOGY

This study used a qualitative approach to investigate the point of contact of cybersecurity risks and public relations (PR) in the digital economy of Nigeria. By synthesising primary data collection with review of secondary data, the research presented a thorough examination of current knowledge and practical observations. Given its ability to combine a wide range of secondary data from peer-reviewed journal articles, book chapters, industry reports (e.g., Nigerian Communications Commission, 2023), and online resources, supplemented by case studies of Nigerian FinTech businesses like Flutterwave and Paystack reacting to cyber security incidents, library research was chosen. By giving different points of view on public relations tactics and cybersecurity issues, these materials helped to establish a strong groundwork of theoretical and practical evidence.

The research included primary data from semi-structured interviews with a number of FinTech industry cybersecurity specialists and Nigerian PR professionals, done between June and August 2024, to improve empirical depth. Expertise in FinTech cybersecurity communication together with involvement in the field were used to purposively choose participants including professionals from companies namely Paystack, Flutterwave, Opay, and Moniepoint, as well as independent consultants. Conducted via Zoom, recorded with permission, and transcribed exactly to capture practical knowledge of PR strategies including proactive awareness campaigns and crisis responses, each interview lasted roughly 45 minutes. This primary data complemented the secondary sources by grounding the analysis in current, sector-specific experiences, addressing the real-world application of theoretical frameworks like TAM and SCCT.

Data collection involved a systematic review of secondary sources and a structured interview process. Secondary data were purposively sampled for relevance, credibility, and recency, focusing on materials that aligned with the study's objectives. Interview questions were designed to elicit detailed responses on PR effectiveness, trust-building, and crisis management, with prompts tailored to Nigeria's FinTech context (e.g., "How have proactive PR strategies impacted user trust in your firm?"). The interviews were conducted until the 29th session as the researchers observed that saturation point was reached. The key informants were coded as NIG_1 to 29 to enable ease-of-analysis. Using thematic analysis, both types of information were examined and results were grouped into main themes which include "PR strategies, trust and credibility," "and crisis management." This enabled a sensitive exploration of the study questions. This mixed methods guaranteed a strong, clear process balancing focused primary observations and thorough literature synthesis, therefore strengthening the empirical validity and local relevance of the research

RESULTS AND DISCUSSION

Thematic areas emerged from the in-depth interviews. These are based on the research questions as researcher attempted to find patterns that matched and provided relevant answers and insights. Accordingly, the three themes revolve around PR strategies in cybersecurity, trust and credibility in communication about cybersecurity, and crisis management and PR in cybersecurity.

a. Public Relations Strategies in Cybersecurity

Particularly in the FinTech industry, this study's findings showed the vital aspects public relations (PR) techniques have in dealing with cybersecurity risk in the digital economy of Nigeria. Using the Technology Acceptance Model (TAM), one can see clearly that public relations campaigns raising the perceived ease of use and impact of cyber security measures would much boost stakeholder acceptance. Venkatesh and Bala (2008) claim that adoption rates increase if stakeholders view cybersecurity policies as absolutely needed and easy to use, therefore improving general security. Proactive public relations efforts, for instance, have trained users and reduced incident frequency from what reactive actions would have done, as they postpone disclosure and produce transaction declines (Ojo & Adebayo, 2022). These results support the situational crisis communication theory (SCCT) of Coombs (2007), which underlines customised communications by crisis kind as essential for maintaining confidence in Nigeria's rapidly changing digital environment.

Furthermore, findings of this research that demonstrate transparency's link with building trust supports a conclusion from the study that clearness and timely communication underpin good PR tactics in cyber security. In Nigeria, aggressive public relations campaigns always outshine reactive strategies: Ndubueze (2021) notes that FinTech businesses offering monthly security updates proactively cut breach reports by 20 percent, while reactive post-incident statements usually recovered just 60% of lost confidence on average. Given digital illiteracy, companies need to emphasise straightforward and understandable communication over technical solutions to dispel cyber-wariness. The Central Bank of Nigeria (2023) evidence of a 20% user compliance increase after straightforward PR messaging (CBN, 2023) compared to reactive clarifications which usually fail to allay first panic suggests this proactive approach not only builds trust but also enables stakeholders. By promoting educated user behaviour, these techniques help to lower the chances of cyber incidents.

b. Trust and Credibility in Communication about Cybersecurity

Particularly in cybersecurity communication, where trustworthiness and reliability are critical to avoid trust erosion, this research revealed trust and credibility to be central ideas. In the digital age, where knowledge spreads quickly, contradictions can drive panic and false information; a danger made more likely by the low trust institutional context in Nigeria. This corresponds with Coombs (2015), who notes that constant communication maintains integrity throughout times of crisis. For example, DavidWest et al. (2022) compared a FinTech company's coherent digital response with another's scattered messaging across channels to a service outage in 2021 that preserved user confidence and reduced churn, therefore resulting in notable user attrition. This comparison shows the advantage of proactive consistency over reactive, disjointed efforts, therefore underlining the need of normal contact to preserve reputation in Nigeria.

Consistent with Fombrun and van Riel (2004), the research also showed that third-party endorsements are a strong means of increasing credibility. Endorsements from credible organisations like the Nigerian Communications Commission (NCC) bolster public relations campaigns in Nigeria, where official statements are widely doubted. The interplay of misinformation and lack of digital literacy further complicates trust dynamics; as a 2023 bank rumour triggered a 30% drop in transactions, but a proactive PR campaign leveraging real time social media rebuttals and NCC backed alerts within 24 hours restored 85% of user confidence (Ndubueze, 2021). Moniepoint's 2024 project likewise runs shows how PR might negate myths and increase awareness by cooperating with local influencers to inform 1.2 million users and cut by 40% false alarm reports, therefore surpassing reactive reactions that fight to handle the repercussions of digital illiteracy (DataReportal, 2024). These methods highlight PR's forward role in building trust in the difficult digital environment of Nigeria.

c. Crisis Management and Public Relations in Cybersecurity

With public relations (PR) having a major influence in negotiating the complexity of cyber incidents, this study highlights once more the utmost need of crisis management in cyber security. The situational crisis communication theory (SCCT) (Coombs, 2007) offers a guideline for good communication; it shows that proactive approaches outdo reactive ones in reducing damage. Afolabi and Akinyemi (2019) discovered that proactive crisis policies, including pre-incident training, kept 90% of customer trust during bank breaches in 2019 compared to reactive apologies after events, which saved just 60 percent. NCC (2023) numbers showed this difference also, where active businesses kept 80% of users against 50% for delayed ones. These results are in line with those of Ulmer et al. (2010) wherein early reactions were seen to have great long term reputational effects.

One of the major factors of good crisis control is preparedness; it enables companies with already existing plans to react faster. Prior planning minimises harm and is a fundamental for the growing digital economy of Nigeria (Olayemi, 2023). While reactive improvisation usually destroys trust, proactive approaches like crisis team drills can greatly lower response times. Moreover, public relations efforts dealing with misinformation such as Opay's 2024 SMS alerts exposing scams quickly slowed incident escalation by 30% in contrast with reactive postponements that compound the confusion caused by digital ineptitude (NCC, 2023). This emphasises the urgent call for thorough crisis plans in the cyber-threat environment of Nigeria.

CONCLUSION

In conclusion, this study has highlighted the critical role of public relations strategies in addressing emerging cybersecurity threats in Nigeria's digital economy, with a particular focus on the FinTech sector where trust and resilience are paramount. The results suggest that in this environment, successful public relations programmes depend on openness, regular communication, and stakeholder engagement. The study also brings up how vital it is to develop credibility and trust by means of unbiased references and regular communication. The use of crisis management models like the situational crisis communication theory has also been shown to be beneficial in directing companies' reactions to cybersecurity. Going forward, it is advisable therefore that:

1. Stakeholders like the Central Bank of Nigeria (CBN), Nigerian Communications Commission (NCC), and the Nigerian FinTech businesses should deploy straightforward, available communication plans in local languages and use multimedia channels such as radio and SMS to increase awareness of cybersecurity, particularly among digitally challenged communities. Such efforts may also include nationwide workshops to inform customers about technologies like two factor authentication and fight against digital illiteracy should also be advanced through public relations approach used in combination with forward-thinking strategy.
2. In cybersecurity disasters, FinTech firms should keep constant, synchronised messaging across platforms including X (formerly Twitter) and SMS to establish confidence, stop disinformation, and maintain integrity. Creating disaster communication plans with premade messages, designated teams, and yearly crisis simulation exercises will also help to verify fast and effective reactions, therefore supporting this kind of moves or strategies.
3. Reputable third parties should be used by the CBN, NCC, FinTechs, and PR companies to improve communication credibility and create a national regulatory framework that guarantees strong oversight and support for cybersecurity resilience in Nigeria's digital economy.

BIODATA

Suleiman Garba PhD is a pioneer student of Mass Communication at Nasarawa State University Keffi, where he graduated in 2020. Dr. Garba bagged his MSc in Mass Communication at Benue State University, Makurdi in 2017 and earned a PhD in same field from Nasarawa State University Keffi in 2024. He is a member of African Council for Communication Education (ACCE), Society for Research and Academic Excellence (SRAE) and Association of Communication Scholars and Professionals of Nigeria (ACSPN). He currently lectures in the Department of Public Relations, Nasarawa State University Keffi. He can be contacted through his emails: garbasuleiman@nsuk.edu.ng; suleimangarba22@gmail.com; ORCID: https://orcid.org/0000-0001-7937-2816; Google Scholar https://scholar.google.com/citations?user=dR-7F9cAAAAJ&hl=en

Kelvin Inobemhe is a lecturer in the Department of Mass Communication, Lagos Campus of Glorious Vision University, Nigeria. He currently pursues a PhD in the main campus of the same university. He holds a Master of Science (MSc) degree from Nasarawa State University, Keffi, Nigeria. He has authored and co-authored several books. The

researcher is well-published in reputable national and international journals. His research interests include new media, journalism and political communication. He is a member of professional bodies such as the Nigerian Institute of Public Relations (NIPR), African Council for Communication Education (ACCE) Nigeria and International Communication Association (ICA) Nigeria. Mr. Inobemhe can be contacted through his emails: inobemhe@nsuk.edu.ng or kelvin.inobemhe@gvu.edu.ng; ORCID https://orcid.org/0000-0001-5748-0066; Google Scholar https://scholar.google.com/citations?hl=en&user=-J10k6gAAAAJ.

REFERENCES

Adebayo, O. S., & Ogunmola, O. A. (2023). Cybersecurity threats and mitigation strategies in Nigeria's financial sector: A review. *African Journal of Science, Technology, Innovation and Development, 15*(4), 512-523. https://doi.org/10.1080/20421338.2022.2145678

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future dimensions. *Cyber Security and Applications, 2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Afolabi, B., & Akinyemi, O. (2019). The effectiveness of public relations strategies in mitigating cyber-attacks in Nigeria's financial sector. *Journal of Public Relations Research*, *31*(3), 204-223. https://doi.org/10.1080/1062726X.2019.1643047

Agboola, O. (2022). Nigeria's budding digital economy: Coping with disruptive technology. *Economic and Financial Review, 60*(4), 33-50.

Agboyangi, A. O., Makinde, A. S., & Odun-Ayo, I. A. (2024). Nigeria's ICT and economic sustainability in the digital age. *ResearchGate*. https://doi.org/10.13140/RG.2.2.14651.43048

Anyanwu, A., Olorunsogo, T., Abrahams, T. O., Akindote, O. J., & Reis, O. (2024). Data confidentiality and integrity: A review of accounting and cybersecurity controls in superannuation organisations. *Computer Science and IT Research Journal, 5*(1), 237-253. https://doi.org/10.51594/scitrj.v5i1.735

Central Bank of Nigeria. (2023). *Guidelines on cybersecurity communication for financial institutions*. Abuja, Nigeria: CBN Press.

Coombs, W. T. (2007). *Ongoing crisis communication: Planning, managing, and responding (2nd ed.)*. SAGE Publications.

Coombs, W. T. (2015). The value of communication during a crisis: Insights from the situational crisis communication theory. *Public Relations Review*, *41*(1), 15-21. https://doi.org/10.1016/j.pubrev.2014.08.006

DataReportal. (2024). Digital 2024: Global overview report. Retrieved from https://datareportal.com/reports/digital-2024-global-overview-report

DataReportal. (2024). Digital 2024: Nigeria. Retrieved from https://datareportal.com/reports/digital-2024-nigeria

David-West, O., Umukoro, I., & Iheanachor, N. (2022). Digital financial services in Nigeria: Addressing trust and adoption challenges in the post-COVID era. *Journal of African Business,* *23*(4), 891-910. https://doi.org/10.1080/15228916.2021.1977729

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. https://doi.org/10.2307/249008

Eze, C. & Chukwuma, E. (2019). Building trust in Nigeria's digital economy: The role of public relations in cybersecurity. *Journal of African Media Studies*, *11*(2), 221-239. https://doi.org/10.1386/jams_00023_7

Fearn-Banks, K. (2016). *Crisis communications: A casebook approach (5th ed.)*. Routledge.

Fombrun, C. J., & van Riel, C. B. M. (2004). *Fame and fortune: How successful companies build winning reputations*. Prentice Hall.

Grunig, J. E., & Hunt, T. (1984). *Managing public relations*. Holt, Rinehart & Winston.

Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F., & Morsut, C. (2020). Communication-related vulnerability to disasters: A heuristic framework. *International Journal of Disaster Risk Reduction, 51*, 101931. https://doi.org/10.1016/j.ijdrr.2020.101931

Inobemhe, K., Ugber, F., Ojo, I. L., & Santas, T. (2020). New media and the proliferation of fake news in Nigeria. *Nasarawa Journal of Multimedia and Communication Studies, 2*(2), 154-168.

Internet World Stats. (2022). *Internet usage statistics for Africa*. Retrieved from https://www.internetworldstats.com/stats1.htm

Jin, Y., Pang, A., & Cameron, G. T. (2012). The role of emotions in crisis responses: Inaugurating the disaster-based crisis communication theory. *Communication Research*, *39*(4), 514-540. https://doi.org/10.1177/0093650211435940

Kshetri, N. (2021). Cybersecurity and trust in Africa's emerging digital economy. *Journal of Global Information Technology Management, 24*(2), 89–108. https://doi.org/10.1080/1097198X.2021.1897701

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attack and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liu, B. F., Austin, L., & Jin, Y. (2011). How publics respond to crisis communication strategies: The interplay of information form and source. *Public Relations Review*, *37*(4), 345-353. https://doi.org/10.1016/j.pubrev.2011.08.004

Malcolm, M. (2023). Cybercrime and its impact on Nigeria's digital economy. *ResearchGate*. https://www.researchgate.net/publication/388657810.

Ndubueze, O. (2021). Public relations and consumer trust in cybersecurity measures: A Nigerian perspective. *International Journal of Cybersecurity and Digital Forensics*, *3*(2), 95-108. https://doi.org/10.4018/ijcds.20210401.oa10

Nigerian Communications Commission (NCC). (2023). *Annual cybersecurity report: FinTech sector analysis*. Abuja, Nigeria: NCC Press.

Obasi, H. U. (2024). The role of media in public relations crisis communication. *British Journal of Mass Communication and Media Research, 4*(4), 77-86. https://doi.org/10.52589/BJMCMR-CBQRSM5Z

Ogunode, O. A., & Abiodun, R. I. (2023). Financial technologies and financial inclusion in emerging economies: Perspectives from Nigeria. *Asian Journal of Economics, Business and Accounting, 23*(19), 38-54. https://doi.org/10.9734/AJEBA/2023/v23i1915

Ojo, A., & Adebayo, T. (2022). Enhancing cybersecurity awareness in Nigeria's digital economy: Strategies and challenges. *Journal of Global Information Technology Management,* *25*(3), 189-207. https://doi.org/10.1080/1097198X.2022.2092923

Okoro, N., & Ekeanyanwu, N. T. (2012). *Public relations in Nigeria: Media and society*. New Africa Press.

Olayemi, A. (2014). Cybersecurity challenges in Nigeria: The role of public relations in managing cyber threats. *Journal of African Business*, *15*(3), 193-208. https://doi.org/10.1080/15228916.2014.925242

Olayemi, O. J. (2023). Cybersecurity preparedness in Nigeria's financial institutions: A qualitative analysis. *International Journal of Cybersecurity Intelligence & Cybercrime, 6*(1), 45-62. https://doi.org/10.52306/06010323YJPK

Olurinola, I., Osabohien, R., Adeleye, B. N., Ogunrinola, I., Omosimua, J. I., & De Alwis, T. (2021). Digitalisation and innovation in Nigerian firms. *Asian Economic and Financial Review,* *11*(3), 263-277. https://doi.org/10.18488/journal.aefr.2021.113.263.277

Omenugha, K. A., & Uzuegbunam, C. E. (2020). Communicating crisis in a multi-ethnic society: The case of Nigeria's COVID-19 response. *Journal of African Media Studies, 12*(3), 305-320. https://doi.org/10.1386/jams_00034_1

Paystack. (2024). *2024 user security and adoption report*. Lagos, Nigeria: Paystack Inc.

Rodsevich, M. (2024). What is crisis communication and why is it important? *PR Lab*. https://prlab.co/blog/what-is-crisis-communication-and-why-is-it-important.

Torossian, R. (2025). The digital revolution: How technology PR shapes industry perception. *Medium.* https://ronntorossian.medium.com/the-digital-revolution-how-technology-pr-shapes-industry-perception-724846a49b46.

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2010). *Effective crisis communication: Moving from crisis to opportunity (2nd ed.)*. SAGE Publications.

Venkatesh, V., & Bala, H. (2012). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273-315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Wilcox, D. L., & Cameron, G. T. (2010). *Public relations: Strategies and tactics (9th ed.)*. Allyn & Bacon.

Williams, M. L., & Burnap, P. (2016). Cyberhate on social media in the aftermath of Woolwich: A case study in computational criminology and big data. *British Journal of Criminology*, *56*(2), 211-238. https://doi.org/10.1093/bjc/azv059