Networked Cybercrime, Bank–Fintech Collaboration and Banking Resilience in Urban Nigeria: A Communication-Centred Conceptual Framework

Muhammad Ribadu Ayuba PhD[1] & Martins Myke-Okoi Okpa PhD[2]
[1]Department of Sociology, Faculty of Social Sciences, Ahmadu Bello University, Zaria, Nigeria.
Email: mrayuba@abu.edu.ng; Tel: +2348036557188
[2]Department of Criminology and Security Studies, University of Calabar, Nigeria.
Email: okpamartins@gmail.com; Tel: +2348067263539
DOI: https://doi.org/10.63725/zajcom.v11.i1.11

Abstract

Research on cybercrime in banking has established two things fairly firmly. Fraud and cyberattacks measurably damage bank performance and reputation, and firm-level controls such as internal audits, risk management frameworks, and biometric authentication reduce that exposure without eliminating it. Across this literature, collaboration with fintech firms and regulators is repeatedly recommended as an additional safeguard. What is missing is any account of why it works. This paper synthesises that literature into a single theoretical reorientation. It treats cybercrime in banking not as a firm-level technical problem but as a networked risk located within an urban financial ecosystem, where shared digital infrastructures carry money and information alike across institutional boundaries. On that basis, the paper theorises bank–fintech collaboration as distributed security governance, drawing on situational crime prevention theory, the institutional perspective, and how threat intelligence and trust travel between organisations. It develops a conceptual framework linking urban cyber-threat exposure, collaborative intensity and banking resilience, moderated by regulatory coordination, data-sharing and communication infrastructure, and inter-organisational trust. Seven propositions are derived from the framework. An integrative review of ten empirical studies from Nigeria, South Africa, Kenya and Yemen establishes the framework's plausibility and internal coherence. Its central claim remains to be tested empirically: that collaborative intensity, under specified moderating conditions, improves banking resilience beyond what firm-level controls achieve alone. The paper closes with implications for banks, fintech firms, regulators and urban policymakers, and an agenda for comparative research on collective cybersecurity governance in rapidly urbanising, digitally inclusive economies.

Keywords: Cybercrime; Bank–Fintech Collaboration; Communication; Banking Resilience; Urban Financial Systems; Distributed Security Governance; Emerging Economies

Introduction

A city is a dense web of exchanges where people, goods, capital, and information travel at the speed of light through fibre, satellite, and radio. Contemporary cities are the nerve centres of digital finance because they are the nerve centres of

communication. The same concentration of people, institutions, capital and infrastructure that makes a city an engine of economic growth also produces dense networks of digital transactions, payment platforms, data centres and broadband connectivity. As banking has migrated onto these networks, crime has followed opportunity into cyberspace, travelling along the same channels that carry legitimate commerce and institutional trust.

Cybercrime, broadly understood, covers all forms of criminal and illicit activity in which telecommunications networks and computer systems serve as the tool, the target or the locale of offending (Kraemer-Mbula, Tang & Rush, 2013). It is committed remotely, propagates instantly, and respects no jurisdictional boundary. Anyone with a working computer and network access can be exposed, whether in an office, a bank, a business, a government department, a school or a private home (Lukonga, 2018; Gupta, 2012). The threat may be placeless in origin, but its impact is firmly place-bound. Cyberattacks are more prominent in cities where digital infrastructure, financial assets, transaction volumes and information flows cluster most densely.

No sector illustrates this convergence more clearly than banking. This is because the ultimate motive of most cybercrime is financial gain, and the banking and financial industry absorbs a disproportionate share of its harm (APWG, 2010). Internet banking fraud entails the theft of funds from bank accounts or any unauthorised transfers using online technology (Australian Federal Police, 2012), which has become a signature crime of the digital economy. Phishing, identity theft, hacking, skimming, malware infection and distributed denial-of-service (DDoS) attacks have all been documented against banks worldwide (Choo, 2011; Cherian, 2014; Raghavan & Parthiban, 2014; Rathore & Marwaha, 2015). Each of these is a communicative act before it is a financial one: a false message, a stolen credential, a manipulated signal. The scale is considerable. Kaspersky Lab (2022) estimated that cyberattacks cost banks and financial institutions roughly three billion United States dollars in 2021. Meanwhile, the migration of customers onto online and mobile channels has multiplied both the points of entry available to offenders and the volume of messages through which trust must now be won or lost (Hastings, 2015; Creado & Ramteke, 2020).

These global dynamics acquire particular intensity in Nigeria and comparable emerging economies. Cybercrime has become one of the fastest-growing categories of crime in Nigeria, notably among the educated but under-employed urban youth population (Hassan, Lass & Makinde, 2012). The sociological texture of that finding is unmistakable: blocked legitimate opportunity meets abundant digital

fluency. The policing of cyberspace, meanwhile, strains institutional capacity across much of the developing world (Akuta, 2012). Within Nigerian banking, social engineering attacks, advance-fee fraud, hacking, identity theft and unauthorised access to information manifest through automated teller machines, mobile channels and the web, eroding confidence in electronic banking among bank and non-bank publics alike (Ibikunle & Odunayo, 2013; Wada & Odulaja, 2012; Aduge-Ani, 2015). These harms are not evenly scattered across national territory. They concentrate in cities, where digital banking adoption, agent networks, fintech platforms, transaction volumes, and communication traffic are highest. Evidence from Enugu urban documents how deposit-taking banks and their customers in dense city environments constitute a distinctive ecology of cyber-fraud exposure (Chukwuma, 2022). Comparative work indicates that emerging economies face a characteristic mismatch between the velocity of digital adoption and the maturity of cyber-defence capability (Gupta & Agarwal, 2017).

The urban scale adopted here is analytical rather than merely descriptive. Three reasons make it necessary, and Section 2.1.4 develops them at length. First, the shared infrastructures through which cyber contagion propagates, including payment switches, interbank settlement platforms, telecommunications backbones and data centres, are physically sited within metropolitan jurisdictions and administratively governed through them, rather than at the level of the individual bank or the nation-state. Second, the density of banks, fintech platforms and digitally included customers that produces both opportunity and vulnerability is itself a metropolitan-concentration effect. Third, the regulatory and inter-organisational coordination on which collective defence depends is typically organised around city-centred financial hubs. A national-level analysis would average away this concentration. A firm-level analysis would miss the shared exposure altogether. Only an urban-ecosystem frame captures the scale at which risk, infrastructure and governance actually coincide.

The prevailing analytical frame in the literature nonetheless remains technical and institutionally isolated. It is also, as this paper argues, communicatively silent. Cybercrime in banking is overwhelmingly studied as a firm-level problem: a matter of one institution's firewalls, internal controls, employee training and fraud losses. This framing obscures two realities and misses a third. First, banking is systemically interconnected. A breach in one banking network can cascade through the payment system and destabilise institutions far beyond the initial target, because all banks and financial institutions are linked through shared infrastructures (Johnson, 2015; Tendulkar, 2013). The Basel Committee's call for system-wide capacity building reflects exactly this recognition that no institution acting alone

can eliminate the systemic risk of cyber technology (Boer & Vasquez, 2017). Second, this interconnection has a spatial expression. The shared infrastructures through which contagion travels, including switching platforms, interbank settlement systems, telecommunications backbones and data centres, are urban infrastructures, embedded in and governed through cities. Third, and least remarked upon, this spatial interconnection is also communicative. What travels along these shared infrastructures is not only money but information: alerts, logs, warnings, credentials, rumours and reassurances. Whether that information moves quickly, accurately and trustingly between organisations matters as much for resilience as any firewall. The banking sector faces a problem of networked threats in networked, communicating cities, and neither the firm-level technical frame nor conventional national-level policy analysis captures it adequately.

These observations point to a single primary gap. Existing scholarship has no unifying framework that treats bank–fintech collaboration as a communicative, ecosystem-scale governance mechanism. Collaboration is documented at the level of the firm, recommended at the level of policy, and left untheorised at the level of the mechanism itself. Closing that gap is the purpose of this paper.

The paper advances a theoretical reorientation. It reframes cybercrime in banking as an urban governance problem arising within a networked financial ecosystem, and theorises collaboration between banks and fintech firms as the central mechanism through which that ecosystem can be co-secured. That mechanism is fundamentally communicative. Such collaborations are not merely commercial innovation partnerships. They constitute a form of distributed security governance in which detection capability, threat intelligence and response capacity are pooled across organisational boundaries through continuous acts of communication, producing opportunity-reduction effects at the scale of the urban financial system rather than the individual institution.

The paper pursues three objectives: (i) to reconceptualise cybercrime in the banking sector as a networked urban risk situated within a communicating financial ecosystem, rather than a discrete firm-level technical failure; (ii) to theorise bank–fintech collaboration as distributed security governance, integrating situational crime prevention theory, the institutional perspective and a communication-centred account of how trust and threat intelligence travel between organisations, and to translate this into a conceptual framework with testable propositions linking urban cyber-threat exposure, collaborative intensity and banking resilience; and (iii) to derive implications for banks, fintech firms, regulators, urban policymakers and future research on collective cybersecurity governance.

Literature Review

Conceptual Review

Stream 1: Cybercrime and Banking

The term cybercrime resists precise and universally accepted definition (Kraemer-Mbula et al., 2013). Like many concepts inherited from a technology still remaking itself, it is defined according to the purpose, means, and classification adopted by whoever is doing the defining (Leukfeldt, Veenstra & Stol, 2013). At its core, the concept converges on criminality that targets an information and communication technology (ICT) system or the information it processes, together with the wider class of crimes in which computers or computer networks function as a tool, target or locale of offending (Kraemer-Mbula et al., 2013). It encompasses both cyber-enabled financial crime and traditional offences that have migrated onto the internet, acquiring new reach and velocity along the way (Aduge-Ani, 2015; Ibikunle & Odunayo, 2013; Wada & Odulaja, 2012).

Within the financial domain, cybercrime takes a characteristically profit-driven form. It includes identity theft, financial fraud, e-mail and internet fraud, and attempts to capture consumers' account credentials, internet banking details and payment card data, alongside denial-of-service attacks, unauthorised entry, hacking and website defacement (Gordon & Loeb, 2003). Typologically, the literature distinguishes phishing, DDoS attacks, hacking, identity theft, web browser fraud, theft of monetary or card data, theft and sale of company data, cyber extortion, cyberstalking and cyberterrorism. Ransomware, Trojan horse programs, logic bombs, worms and droppers rank among the most dangerous malware vectors (Gupta, 2012; Rathore & Marwaha, 2015).

Applied specifically to banks, this catalogue of attack types is well documented. Phishing supplies criminals with credentials subsequently used for credit card fraud, identity theft, and the draining of accounts (Arachchilage & Love, 2014). Skimming involves the illegitimate copying of data from electronic payment cards, frequently through devices installed at automated teller machines (Choo, 2011). DDoS attacks render banking services unavailable by overwhelming them with traffic, damaging reputation and creating cover for the planting of malware and spyware (Cherian, 2014). Botnets, Trojan horses and phishing e-mails are deployed to trick employees and customers into surrendering credentials, enabling direct theft from personal accounts (Creado & Ramteke, 2020; Akinbowale, Klingelhöfer & Zerihun, 2020). Insider vulnerability compounds these external threats. Because confidential data traverses end-to-end customer appliances such as smartphones and tablets, a single infected customer device can threaten a bank's entire network

if inadequately protected (Uddin, Ali & Hassan, 2020; Alese, Thompson, Alowolodu & Blessing, 2018). This stream establishes that cyber-enabled financial crime against banks is well catalogued at the level of attack technique. What it does not explain is how banks might jointly defend against a threat that no single institution's controls can fully contain.

Stream 2: Fintech and Third-Party Cyber Risk

The digitalisation of banking has transformed both service delivery and the architecture of criminal opportunity. Automated teller machines and electronic channels allow customers to transact outside business hours. Online and mobile banking permit account management without a branch visit. The drift toward a cashless model routes transactions through apps, application programming interfaces, and third-party payment platforms, and every prompt and confirmation along the way is a potential point of compromise (Creado & Ramteke, 2020). The same innovation that extended banking onto fintech-operated infrastructure has expanded the attack surface available to offenders, making e-banking simultaneously a convenience and a vulnerability (Equinix, 2021; Aduge-Ani, 2015).

Because banks continue to outsource technology-based operational support to specialist fintech firms, perpetrators intrude into banking systems through black spots in the technology infrastructure that no single institution fully surveys. Scholars have accordingly called for personal data protection regimes holding technology firms accountable, as data processors, for breaches arising from this outsourced infrastructure, a measure intended to strengthen customer confidence in electronic commerce amid rising security incidents. The literature also cautions that fintech adoption is not risk-free. The cyber and operational risks of adopting fintech can themselves depress bank performance where governance of the partnership is weak (Al-shari & Lokhande, 2023). This stream identifies third-party and platform-mediated risk as a category distinct from Stream 1's direct attacks on the bank itself. It also establishes the governance problem that the paper's conceptual framework must address: how banks and fintech firms manage the risk each introduces into the other's systems.

Stream 3: Cybersecurity Information Sharing (Central Stream)

This third stream is central to the argument of the paper, because it supplies the mechanism through which the risks identified in Streams 1 and 2 are actually managed in practice. Urban sociologists have long understood cities not merely as physical agglomerations but as dense communication systems, in which information about opportunity, danger and reputation circulates rapidly and

consequentially. Extending this insight to digital finance, a cyber-threat is first of all a piece of information travelling through a channel: a phishing signature, a malware indicator, a fraud alert, a warning exchanged between compliance officers at rival banks. Whether that information reaches the right recipient in time, surviving the noise of competitive secrecy, legal caution and organisational silo-thinking, is decisive for collective resilience.

Three concepts sharpen this point. Shared threat intelligence is not a static technical artefact but an information flow that must be produced, transmitted, received, interpreted and acted upon under time pressure. Its value depends on an information-sharing network whose participants are willing to disclose what they know despite the information asymmetry that ordinarily separates competitors. Inter-organisational trust is built, tested and repaired through repeated exchange, through the honesty of incident reporting, the promptness of warnings, and the willingness of one institution to admit vulnerability to another. It is not possessed as a fixed attribute. Third, the speed and accuracy with which threat information travels matters as much as its content. Information that arrives too late, too vague, or at the wrong recipient confers no protective advantage, however accurate it may be. The empirical corpus reviewed in Section 2.2 offers direct support here. Bank management personnel interviewed by Ogoh (2016), without prompting from communication theory, independently named effective communication and industry collaboration among their frontline defences against cybercrime. This stream treats that as grounded testimony and a central finding rather than an incidental one.

Read this way, the recurring recommendation elsewhere in the literature that banks collaborate, coordinate and communicate (Ogoh, 2016) is under-specified. It names the need for information sharing without asking what makes such sharing fast, honest and trusted rather than slow, guarded and largely ceremonial. Section 4.1 takes up that question directly through the construct of collaborative intensity.

Stream 4: Urban and Networked Financial Infrastructure

A fourth stream establishes why cyber risk in banking cannot be confined to the individual firm. As the financial sector relies ever more heavily on cyber technology for operations and service delivery, banks are exposed to a systemic technology risk that cannot simply be switched off. A breach in one banking network can shake the entire financial system, because all banks and financial institutions are interconnected, and institutions linked to a compromised system face disruption of their own operations (Johnson, 2015; Tendulkar, 2013). For this reason, the Basel Committee urges banks and financial institutions globally to build

system-wide capacity to withstand cyber shocks. Systemic cyber risk can be mitigated only through collective capacity building; no one institution acting alone can eliminate it (Boer & Vasquez, 2017).

This paper presses the systemic insight one step further, into the terrain of urban sociology, through a direct logical chain. Urban financial infrastructure produces interdependence between institutions that share it. Interdependence creates pathways along which a single compromise can produce contagion. Contagion at scale constitutes a collective risk that no institution's boundary can contain. The shared infrastructures through which such contagion propagates, including payment switches, settlement platforms, telecommunications backbones, cloud and data-centre facilities, and agent and ATM networks, are physically sited in cities and operationally governed through them. The density of banks, fintech platforms and digitally included customers in metropolitan centres means that both the opportunity structure of financial cybercrime and the contagion pathways of systemic cyber risk are urban phenomena. Nigerian evidence is suggestive. Cyber fraud against deposit-taking banks and their publics clusters in dense urban settings such as Enugu urban (Chukwuma, 2022), and electronic fraud nationally flows through the very channels whose penetration is deepest in cities: ATM, mobile, web and point-of-sale (Nwobia, Adigwe, Ezu & Okoye, 2020). This stream establishes the spatial scale at which collective risk operates. It does not, on its own, explain why competing institutions would act jointly to manage that risk, which is the question taken up in Stream 5.

Stream 5: Inter-Organisational Governance

A fifth stream, drawn from collaborative and network governance and from institutional theory, addresses the question the preceding streams leave open. Why would competing banks and fintech firms share sensitive cyber-threat information and coordinate their defences, rather than compete on security as they compete on price and service? Collaborative and network-governance scholarship holds that where risk is jointly produced, as Stream 4 establishes it is, governance responses are more effective when distributed across the organisations sharing the risk than when left to each organisation's unilateral discretion. Unilateral action displaces rather than eliminates threat within a shared system. Institutional theory supplies a complementary answer, developed at length in Section 3.2. Organisations converge on shared security practices not only because those practices work, but because they confer regulatory legitimacy, professional standing and public trust, outcomes no single firm can secure alone in an ecosystem where a rival's breach can still damage public confidence in banking generally.

Complementary organisational prescriptions illustrate this governance logic in practice. Granåsen and Andersson (2016) propose dedicated multidisciplinary risk units within banks that combine technical and non-technical expertise, mirroring inside the firm the inter-organisational pooling of competence that bank–fintech collaboration achieves outside it. Mayahi and Humaid (2016) emphasise capacity building through employee training and infrastructure investment, a form of institutional professionalisation that diffuses across the field independently of any single bank's calculated returns. This stream, together with the enforcement backstop supplied by public agencies such as the Economic and Financial Crimes Commission (EFCC, 2015), identifies inter-organisational governance as the appropriate response architecture for ecosystem-level risk, rather than either technical hardening (Stream 1) or unilateral risk management (Stream 2).

Positioned against these five streams, distributed security governance, the concept developed in Section 3 and operationalised in Section 4, is not a sixth freestanding idea. It is a specific synthesis of the five. It takes the attack catalogue of Stream 1 and the platform-mediated risk of Stream 2 as the opportunities to be reduced. It takes the interdependence and contagion pathways of Stream 4 as the scale at which reduction must occur. It takes the collaborative and institutional logic of Stream 5 as the reason organisations act jointly rather than alone. And it takes the information-sharing mechanics of Stream 3 as the connective tissue without which none of the other four streams' prescriptions can function between organisations that remain, in most other respects, competitors.

Empirical Review

Akintoye, Ogunode, Ajayi and Abimbola (2022) examined the impact of cybersecurity on the financial innovation of deposit money banks in Nigeria, surveying fifty-six purposively selected bank staff and analysing the results through descriptive statistics and multiple regression. Cybersecurity, proxied by risk management and bank monitoring, exerted a positive and statistically significant effect on financial innovation, leading the authors to recommend regular review and strengthening of risk management frameworks. The study usefully establishes that security and innovation are complements rather than rivals. Its limitation for present purposes is that both constructs are measured wholly within the walls of the individual bank, with no attention to what passes between institutions.

Muritala, Ijaiya and Adeniran (2017) traced the fraud–performance relationship in the Nigerian banking industry through a longitudinal design covering 5,238 staff implicated in fraud and forgery between 2000 and 2013, analysed using cointegration and vector error correction techniques. Both the amount and the

incidence of fraud depressed bank performance, prompting a recommendation that banks strengthen internal control systems. The study documents the performance costs of fraud with considerable rigour, but treats the bank throughout as a closed system whose defences are exclusively internal, an assumption this paper contests.

Nwekpa, Ezezue, Nwabuike and Ibeme (2019) assessed the effect of cybercrime on e-business performance at Konga.com in Abakaliki, Ebonyi State, using an ex-post facto survey analysed through Pearson correlation and t-statistics. Malicious agents emerged as strong inhibitors of e-business performance and a serious threat to its growth, leading the authors to recommend biometric technology over conventional password and code encryption. The study usefully extends the evidence base beyond banks into the platform economy with which banks increasingly interlock, though its single-platform design limits how far its findings can travel.

Nwobia, Adigwe, Ezu and Okoye (2020) examined electronic fraud and the performance of deposit money banks in Nigeria between 2008 and 2018, drawing secondary data from NIBSS and NDIC publications and applying ordinary least squares and multivariate panel regression. They found a negative though statistically insignificant relationship between electronic fraud channels and financial performance, and recommended improved collaboration between deposit money banks, the Central Bank of Nigeria and other stakeholders through the Nigeria Electronic Fraud Forum (NeFF). This is among the few studies in the corpus to gesture explicitly toward inter-organisational and regulatory coordination, rather than firm-level control, as the appropriate response architecture.

Ogoh (2016) explored the role of management in combating cybercrime within Nigeria's banking industry through semi-structured interviews with twenty bank management participants in the South-South geopolitical zone. Policy compliance and implementation, awareness creation, inclusive banking, mandatory training, effective communication, and industry collaboration all emerged as consequential. This finding deserves attention. Practitioners themselves, without any prompting from communication theory, named effective communication as a frontline defence, which lends direct practical support to the communicative reading developed in this paper.

Akinbowale, Klingelhöfer and Zerihun (2019) assessed the impact of cyber fraud on the South African banking industry through a qualitative survey of staff across seventeen licensed banks, tested with chi-square, Fisher's exact and Spearman procedures. Cyber fraud exerted a highly significant impact, damaging the reputation of several banks, leading the authors to recommend a review of the

means available to curb cyber fraud and its associated risks. The study demonstrates that reputational and therefore trust-related damage is a first-order consequence of cybercrime, a finding the conceptual framework below treats as a communicative casualty as much as a financial one.

Bonaneri (2021) studied the management of cyber fraud in Kenyan commercial banks through a cross-sectional case study of Chase Bank, combining questionnaires and interviews with eight departmental representatives. Strong internal control emerged as the most effective preventive mechanism, with technological infrastructure exerting a major effect. The recommendation was for systems and structures that reduce the opportunities for cyber fraud. This explicit invocation of opportunity reduction gives direct empirical resonance to situational crime prevention theory.

Khan, Malik, Nazir and Khan (2017) conducted a systematic analysis of 101 articles on the use of biometric systems for enhancing cybersecurity in conventional and Islamic banking. Biometric competencies were found to boost the productivity of banking operations, leading the authors to conclude that biometric solutions could resolve cyberattacks, minimise cybercrime risk, and build strong client–bank relationships by providing a secure atmosphere. The study exemplifies technological target hardening. Its emphasis on customer peace of mind quietly reveals that security technologies function institutionally as producers of trust, and trust is a communicative achievement rather than a purely technical one.

Al-shari and Lokhande (2023) explored the relationship between the risks of adopting fintech in banks and bank performance, using the balanced scorecard and partial least squares structural equation modelling on questionnaire data from 263 branch-level managers in Yemen. Cyber and operational risks of fintech adoption negatively affected performance, and the authors recommended that banks adopt fintech specifically as a defence against cyber risk. The study is doubly instructive. It confirms the performance relevance of fintech engagement while warning that poorly governed adoption imports new risk, which is the basis for the trust and governance moderators specified in Section 4.

Chukwuma (2022) examined deposit-taking banks and cyber fraud among the public in Enugu urban, Enugu State, Nigeria, situating fraud exposure within a specifically urban banking public. Of the ten studies reviewed, it comes closest to the spatial sensibility this paper advocates, documenting how the density of banked populations in city environments shapes the ecology of victimisation.

Generally, the empirical corpus reviewed, converges on three findings: Cybercrime measurably damages bank performance and reputation. Internal controls, risk management frameworks and security technologies mitigate that damage. And collaboration, with fintech firms, regulators and industry forums, recurs across the corpus as the recommended path forward, almost as an article of faith. The corpus nonetheless stops short of theorising why collaboration works, under what conditions it works, and, a point this paper adds, through what communicative mechanisms it functions day to day.

Theoretical Framework

The paper rests on three complementary theoretical pillars. Each is necessary because, alone, none of the other two can answer the question it is built to answer. Situational crime prevention theory supplies the micro-logic of criminal opportunity and its reduction. It explains what must change in the immediate environment for an attack to become harder to execute, but it is silent on why separate, competing organisations would coordinate that change with one another. The institutional perspective supplies the meso- and macro-logic of why organisations coordinate, converge and build legitimacy around shared security practices. It explains why competing banks and fintech firms would be willing to act jointly at all, but it does not specify the operational content of what they must do, nor the practical medium through which their coordination is carried out. A communication-centred understanding of networks supplies that missing connective logic. It explains how information, trust and warning actually move between organisations sharing an urban financial ecosystem. Without it, neither situational prevention nor institutional convergence can function in practice. A rule known but never communicated protects nothing, and a partnership legitimated on paper but silent in operation reduces no opportunity.

Their synthesis yields the notion of distributed security governance: an arrangement in which the opportunity-reducing techniques identified by situational crime prevention theory are implemented not by isolated institutions but by a coordinated, communicating ecosystem of banks, fintech firms, regulators and infrastructure providers, at the scale of the networked city. The institutional perspective supplies the rules and legitimacy that make such coordination durable, and communication theory supplies the channels through which it operates. Situational prevention without institutional coordination produces displacement of offending from hardened to softer targets. Institutional coordination without situational content produces ceremonial compliance. Either without functioning communication produces well-intentioned silence. Their combination is theorised to produce resilience: the capacity of the urban financial ecosystem to anticipate, absorb, adapt

to and recover from networked threats. This synthesis anchors the conceptual framework developed in Section 4.

Situational Crime Prevention Theory

Situational crime prevention theory was propounded by Clarke (1980) and seeks a greater understanding of crime and more effective prevention strategies, through attention to the physical, organisational and social environments that make crime possible. It encompasses both immediate settings and wider social arrangements. Clarke summarises the approach as the science and art of decreasing the number of opportunities for crime, using measures directed at highly specific forms of crime and involving the management, design or manipulation of the immediate environment in a systematic and permanent way.

The theory's foundational assumptions are that more opportunities lead to more crime, that easier opportunities attract more offenders, and that the ready availability of easy opportunities can sustain a criminal career. Prevention can proceed along two routes: changing the offender's disposition, or reducing the offender's opportunities. The theory's distinctive wager is on the second route, on the premise that crime can be reduced effectively by altering situations rather than dispositions. Clarke (1980) organises preventive measures into three broad categories, namely degrees of surveillance, target hardening and environmental management, elaborated into sixteen opportunity-reducing techniques: target hardening, access control, deflecting offenders, controlling facilitators, entry and exit screening, formal surveillance, surveillance by employees, natural surveillance, target removal, identifying property, reducing temptation, denying benefits, rule setting, stimulating conscience, controlling disinhibitors and facilitating compliance.

The translation of these techniques into the digital banking environment is direct. Target hardening corresponds to encryption, multilevel authentication, and biometric verification (Alese et al., 2018; Khan et al., 2017; Nwekpa et al., 2019). Access control corresponds to credential management, privilege restriction, and entry screening of devices and transactions. Formal and employee surveillance correspond to real-time transaction monitoring, fraud analytics, and internal audit (Akintoye et al., 2022). Controlling facilitators corresponds to securing the third-party technologies and customer devices through which intrusion occurs (Uddin et al., 2020). Denying benefits corresponds to transaction reversal regimes, account freezing, and the disruption of monetisation channels. Cybercriminals exploit loopholes, or opportunity structures, in online banking platforms, and the theory's prescription is to close them systematically and permanently. Each of these

techniques depends on some prior act of communication, whether a rule made known, a device recognised, or a suspicious pattern flagged. Without it, the most elegant opportunity-reducing design remains inert.

Two refinements are required when the theory is carried from the street corner to the networked city. First, the situation of financial cybercrime is not a discrete physical place but a distributed socio-technical environment spanning many organisations. The opportunity exploited by an offender may arise in a fintech application programming interface, traverse a telecommunications network, and culminate in a bank account. No single place manager controls this environment. Second, opportunity reduction at one node, undertaken unilaterally, tends to displace offending to less protected nodes within the same urban ecosystem rather than eliminating it. Both refinements point to the same conclusion. In a networked financial ecosystem, situational prevention is necessarily a collective accomplishment, requiring coordinated environmental management across institutional boundaries. This is exactly the work that bank–fintech collaboration performs, and explaining how such coordination becomes possible and durable requires two further theoretical lenses.

The Institutional Perspective

The institutional perspective holds that organisations are embedded in regulative, normative and cultural-cognitive environments that shape their structures and practices as much as technical efficiency does. Organisations adopt practices not only because those practices work but because they confer legitimacy in the eyes of regulators, peers, customers and the public. Organisational fields tend over time toward convergence on practices defined as appropriate, through coercive pressure from regulation, mimetic pressure from uncertainty, and normative pressure from professionalisation.

Applied to cybersecurity in banking, the perspective illuminates three dynamics invisible to a purely situational analysis. First, regulative pressure. Supervisory and standard-setting bodies, including the Basel Committee globally (Boer & Vasquez, 2017) and in Nigeria the Central Bank of Nigeria, the Nigeria Electronic Fraud Forum (Nwobia et al., 2020) and enforcement agencies such as the Economic and Financial Crimes Commission (EFCC, 2015), define the rules, expectations and sanctions within which banks' security choices are made, and can compel the inter-organisational coordination that voluntary action under-supplies. Second, normative and mimetic pressure. As leading banks institutionalise security partnerships, dedicated multidisciplinary risk units (Granåsen & Andersson, 2016) and systematic capacity building (Mayahi & Humaid, 2016), these arrangements

diffuse across the field as markers of sound management, independent of any individual bank's calculated returns. Third, legitimacy and trust. Because banking rests ultimately on public confidence, cybersecurity functions institutionally as a producer of trust. Cyber fraud damages reputation and confidence (Akinbowale et al., 2019), while visible security competence builds the strong client–bank relationships on which performance depends (Khan et al., 2017).

These three dynamics together answer the question that a purely situational or purely commercial account of bank behaviour cannot. Why would competing banks and fintech firms share sensitive cyber-threat information at all, given that disclosure carries reputational risk and no direct competitive advantage? The institutional answer is fourfold. First, coercive pressure changes the calculus of disclosure by making it mandatory and universal rather than voluntary and unilateral. Where regulators such as the Central Bank of Nigeria and the Nigeria Electronic Fraud Forum require reporting from every licensed institution, no single bank bears a competitive cost that its rivals escape, which removes the free-rider incentive to stay silent. Second, mimetic pressure operates under uncertainty. Because no bank can fully observe the threat landscape on its own, imitating peers who participate in intelligence-sharing arrangements is a rational response to not knowing what one does not know, and non-participation risks looking, to regulators and the market alike, like an institution with something to hide. Third, normative pressure reframes disclosure as a professional obligation rather than a discretionary courtesy. As information sharing becomes an institutionalised marker of sound risk management within the banking and fintech field, withholding known threats that later harm a peer institution becomes reputationally costlier than disclosing them. Fourth, and consistent with the systemic interdependence established in Stream 4 of Section 2.1, the logic is ultimately self-interested rather than altruistic. Because banks are linked through shared infrastructure, a rival's undisclosed breach today is tomorrow's contagion risk to one's own institution, which converts information sharing from a favour extended to competitors into a hedge against one's own systemic exposure.

The institutional perspective thus explains both the demand for collaboration, in the form of legitimacy and regulatory compliance alongside risk reduction, and the conditions of its durability in rule frameworks, professional norms and trust. It also warns that collaboration can be ceremonial, adopted for appearance while decoupled from practice, which is why the conceptual framework below treats collaborative intensity rather than the mere existence of partnership as the operative construct. Legitimacy itself is never simply possessed. It is conferred through

communication, through what regulators announce, what peers observe, and what publics are told, which is the connective tissue supplied by the third theoretical lens.

Communication as the Connective Tissue of Urban Security Governance

Neither situational prevention nor institutional convergence can operate without a third ingredient: the actual transmission of meaning between organisations that must act, in effect, as strangers cooperating under pressure. The sociology of communication offers three concepts that sharpen this point. The first is the elementary idea, familiar since the earliest theories of communication, that any exchange of information travels through a channel from sender to receiver and is always vulnerable to noise, whether distortion, delay, or simple failure to arrive. Applied to banking cybersecurity, a fraud alert generated inside one institution is of no defensive value to the ecosystem until it survives the noise of competitive secrecy, legal caution and organisational silo-thinking to reach a second institution in time to matter. The second is the sociological concept of the network society, which holds that power and advantage accrue less to those who hold the most resources than to those who occupy the most central positions in flows of information. Translated into banking, this suggests that resilience belongs not to the bank with the largest security budget but to the bank, and the city, best positioned within a well-connected communication network. The third is risk communication, long established in the sociology of disaster and public health. How a threat is communicated, including its timing, tone, credibility, and audience, shapes collective response as much as the objective severity of the threat itself. A cyber-threat that is detected but not communicated, or communicated too late, too vaguely, or to the wrong audience, produces the same harm as a threat that was never detected at all.

These ideas recast bank–fintech collaboration as a communication system: a set of channels, norms and habits through which signals about danger are supposed to travel faster than the danger itself. Where the channel is open, trusted and well used, situational prevention and institutional legitimacy reinforce one another and resilience follows. Where the channel is noisy, guarded or absent, both situational techniques and institutional rules operate in isolation, node by node, bank by bank, each institution hardening its own walls while remaining silent about what it sees over them. This is precisely the pattern the literature reviewed in Section 2 repeatedly shows.

Conceptual Framework

Building on the foregoing synthesis, this section develops the paper's conceptual framework. The framework links three core constructs, namely urban cyber-threat

exposure, bank–fintech collaborative intensity, and banking resilience and institutional performance. It specifies three moderating conditions: regulatory coordination, data-sharing and communication infrastructures, and inter-organisational trust networks.

Urban Cyber-threat Exposure	**→ Bank–Fintech Collaborative intensity**	**→Banking Resilience and Institutional performance**
Digital infrastructure density Transaction volume and velocity Attack surface breadth Inclusion–security gap	Joint secure platform development Shared threat intelligence Real-time monitoring and response Continuous risk communication and disclosure Joint capability building	Anticipation, absorption, adaptation, recovery Performance, reputation and public trust
Moderating Conditions Regulatory coordination •Data-sharing and communication infrastructures •Inter-organisational trust networks	**Moderating Conditions** Regulatory coordination •Data-sharing and communication infrastructures •Inter-organisational trust networks	**Moderating Conditions** Regulatory coordination •Data-sharing and communication infrastructures •Inter-organisational trust networks

Figure 1: Conceptual framework linking urban cyber-threat exposure, bank–fintech collaborative intensity, and banking resilience and institutional performance, with moderating conditions. Source: Authors' conceptualisation (2026).

Core Constructs

Urban cyber-threat exposure denotes the degree to which a banking institution, and the urban financial ecosystem in which it is embedded, is open to networked attack. It is a function of digital infrastructure density (data centres, payment switches, telecommunications backbones, ATM and agent networks), transaction volume and velocity, the breadth of the digital attack surface (channels, platforms,

interconnections and third-party dependencies), and the pace of digital financial inclusion relative to the maturity of security capability. Exposure so defined is an ecological property. It attaches to the city-level ecosystem as well as to its constituent institutions, because shared infrastructures transmit compromise across organisational boundaries (Johnson, 2015; Tendulkar, 2013).

Bank–fintech collaborative intensity denotes the depth, scope and quality of cooperation between banks and fintech firms in the governance of cyber risk. It ranges from arm's-length procurement of security products, through joint development of secure platforms and shared threat-intelligence arrangements, to fully integrated real-time monitoring, response and recovery capabilities. Intensity is deliberately distinguished from the mere existence of partnership, since ceremonial or poorly governed collaboration may add third-party risk rather than reduce it (Al-shari & Lokhande, 2023). Because collaboration is at root a set of communicative exchanges, intensity is best measured not by the existence of a partnership agreement but by the frequency, honesty and speed with which information about threats actually moves between the parties. High-intensity collaboration operationalises, across organisational boundaries, the opportunity-reducing techniques of situational prevention: target hardening, access control, surveillance, controlling facilitators and denying benefits (Clarke, 1980).

Banking resilience and institutional performance denotes the outcome complex: the capacity of banks, and of the urban financial ecosystem collectively, to anticipate, absorb, adapt to and recover from cyberattack, together with the downstream institutional outcomes that resilience protects, including financial performance, service continuity, regulatory standing, reputation and public trust (Muritala et al., 2017; Akinbowale et al., 2019; Nwobia et al., 2020).

Moderating Conditions

Three conditions govern the strength of the relationships among the core constructs.

Regulatory coordination, meaning the capacity of central banks, fraud forums and enforcement agencies to set standards, mandate reporting and orchestrate collective response (Boer & Vasquez, 2017; Nwobia et al., 2020; EFCC, 2015), supplies the regulative scaffolding that converts voluntary cooperation into durable governance.

Data-sharing and communication infrastructures, meaning secure, interoperable arrangements together with the shared protocols and vocabularies that make them usable for exchanging threat intelligence, fraud signatures and incident

data across institutions, determine whether collaboration can operate at the speed of networked attack. Without them, collective intelligence remains aspirational.

Inter-organisational trust networks, meaning the relational confidence among banks, fintech firms and regulators built through repeated interaction, professional norms and accountability arrangements such as data protection liability, determine whether sensitive information is actually shared and whether partnerships deepen beyond ceremony.

Propositions

The framework yields seven propositions amenable to future empirical testing.

Proposition 1: Urban cyber-threat exposure increases with the density of digital financial infrastructure and with the velocity of digital financial inclusion relative to security capability. Exposure is therefore systematically higher in rapidly digitalising cities of emerging economies.

Proposition 2: Ceteris paribus, higher urban cyber-threat exposure is associated with lower banking resilience and weaker institutional performance, through both direct loss channels (fraud, theft, disruption) and indirect channels (reputational damage and erosion of public trust).

Proposition 3: Bank–fintech collaborative intensity attenuates the negative relationship between exposure and resilience, because high-intensity collaboration implements opportunity-reducing techniques at the scale of the ecosystem, limiting both successful attacks and cross-institutional displacement.

Proposition 4: The resilience benefit of collaborative intensity is stronger where regulatory coordination is high, because regulation aligns incentives, mandates participation, and suppresses free-riding in collective security provision.

Proposition 5: The resilience benefit of collaborative intensity is stronger where data-sharing infrastructures are developed, because shared, real-time intelligence is the operational medium through which distributed security governance functions.

Proposition 6: The resilience benefit of collaborative intensity is conditional on inter-organisational trust. Where trust and partnership governance are weak, collaboration adds third-party risk and may diminish rather than enhance resilience.

Proposition 7: The resilience benefit of collaborative intensity is stronger where communication between banks, fintech firms and regulators is frequent, honest and timely, because information that does not travel in time confers no protective advantage regardless of its underlying accuracy.

Boundary Conditions

The framework is specified for digitally intensive urban contexts, and its stakes are highest in rapidly urbanising emerging economies, Nigeria prominent among them, where digital financial inclusion expands faster than security capability (Gupta & Agarwal, 2017; Lukonga, 2018; Hassan et al., 2012). In such settings, the moderators are typically at their weakest exactly where exposure is at its strongest, and communication infrastructure is often the weakest moderator of all. This is why the framework directs analytical and policy attention to regulatory coordination, data-sharing and communication infrastructure, and trust-building as the levers of urban financial resilience.

Methodology

This paper adopts a theory-building integrative review methodology grounded in systematic engagement with secondary literature. The approach suits the paper's theoretical orientation and is widely used in criminological and social-scientific scholarship where the objective is critical synthesis and conceptual extension of existing knowledge rather than the generation of new primary empirical data. The method proceeds in four stages: systematic identification of relevant scholarship; screening against explicit inclusion and exclusion criteria; analytical rather than merely descriptive review of a defined empirical corpus; and theoretical integration, in which reviewed findings are interrogated against the explanatory resources of situational crime prevention theory, the institutional perspective and the communication-centred reading developed in this paper, to construct the conceptual framework presented in Section 4.

The identification stage searched Google Scholar and relevant Nigerian institutional repositories using combinations of the search terms cybercrime, bank fraud, fintech collaboration, cyber risk, information sharing, banking resilience and urban financial infrastructure, restricted to publications from 2010 to 2024. This search returned an initial pool of 71 records. The records were screened first at title and abstract level, and then in full text against explicit inclusion criteria: direct empirical or conceptual engagement with cybercrime, banking fraud, fintech risk, inter-organisational security collaboration, or urban and networked financial infrastructure; publication in a peer-reviewed journal, dissertation, or institutional report; and a clearly stated method. Exclusion criteria covered studies with no identifiable methodology, duplicate reports of the same dataset, and sources addressing cybercrime outside the financial sector with no transferable implication for banking. Screening reduced the initial pool to 33 records, of which ten empirical studies were retained for detailed analytical review on the basis of methodological transparency and joint coverage of the constructs of interest: Akintoye et al. (2022),

Muritala et al. (2017), Nwekpa et al. (2019), Nwobia et al. (2020), Ogoh (2016), Akinbowale et al. (2019), Bonaneri (2021), Khan et al. (2017), Al-shari and Lokhande (2023) and Chukwuma (2022). The corpus deliberately spans quantitative, qualitative and systematic-review designs; bank-level, platform-level and sector-level units of analysis; and Nigerian, South African, Kenyan and Yemeni settings, permitting analytical generalisation across emerging-economy banking contexts.

Quality was appraised for each retained study against three criteria: methodological transparency, meaning whether sampling, data collection and analytical technique were clearly reported; relevance, meaning direct engagement with cybercrime, banking performance or inter-organisational collaboration; and currency, meaning publication within the search's date range, with earlier foundational sources such as Clarke (1980) retained for theoretical rather than empirical purposes. No study meeting these criteria was excluded from the final draft on quality grounds alone.

The analytical procedure involved thematic content analysis of the reviewed materials, guided by the study's theoretical propositions. Each retained study was read in full and coded manually against five a priori themes derived from the theoretical framework in Section 3 and the five literature streams in Section 2.1: cyber-threat exposure, situational mitigation mechanisms, inter-organisational collaboration and coordination, communication practice, and resilience and performance outcomes. Coded excerpts were then synthesised into the analytical narratives presented in Section 6, organised around the same five themes. The limitations of the method are acknowledged. An integrative review of this kind can establish the plausibility and internal coherence of a framework but not its empirical validity.

Discussion

The synthesis of the reviewed literature, read through the theoretical lenses adopted, yields five interlocking findings.

Internal Controls and Risk Management as Situational Target Hardening

The first and most consistent theme in the corpus is that opportunity reduction within the firm works. Regular review and strengthening of risk management frameworks improve the security–innovation balance of deposit money banks (Akintoye et al., 2022). Strong internal control is the most effective single preventive mechanism against cyber fraud (Bonaneri, 2021). Strengthened internal control systems detect and prevent fraudulent activity and protect bank assets (Muritala et al., 2017). Biometric and multilevel authentication technologies harden

targets against credential-based attacks while reassuring customers (Khan et al., 2017; Nwekpa et al., 2019; Alese et al., 2018). In the vocabulary of Clarke (1980), these are the techniques of target hardening, access control, and formal surveillance translated into the digital banking environment. The framework's contribution is to show that these firm-level measures, while necessary, are insufficient. Implemented unilaterally in a networked ecosystem, they protect the hardened node while displacing offending toward softer ones, leaving system-level exposure, and therefore each institution's residual exposure through shared infrastructure, largely intact (Johnson, 2015; Tendulkar, 2013).

Collaboration as Distributed Security Governance

The second theme is the repeated but under-theorised appearance of collaboration in the corpus's recommendations. Improved collaboration among deposit money banks, the Central Bank of Nigeria and other stakeholders through the Nigeria Electronic Fraud Forum is urged as the response to electronic fraud (Nwobia et al., 2020). Industry collaboration features among the management practices that demonstrably combat cybercrime (Ogoh, 2016). Fintech adoption is recommended precisely as a defence against cyber risk (Al-shari & Lokhande, 2023). The strategic alliance between banks and fintech firms grants banks access to cutting-edge cybersecurity technologies, including machine learning algorithms for threat detection, advanced encryption and real-time monitoring systems, together with specialised expertise capable of assessing existing infrastructure, identifying weaknesses and developing customised defence strategies. The present framework explains why these arrangements work. They implement situational prevention at the scale at which the opportunity structure actually exists, and they do so through channels of communication that carry pooled threat intelligence, converting each institution's detection into every institution's foresight. Joint platform development closes the inter-organisational black spots through which intruders enter, and coordinated response denies offenders the benefit of displacement. Collaboration is not an adjunct to security. It is the form security takes in a networked financial ecosystem, and communication is the currency it spends.

The Moderating Conditions in Practice

The third theme concerns the conditions under which collaboration delivers. The corpus shows regulatory coordination operating as the scaffolding of collective action, from the Basel Committee's system-wide capacity-building agenda (Boer & Vasquez, 2017) to the CBN–NeFF architecture in Nigeria (Nwobia et al., 2020) and the enforcement backstop of the EFCC (2015). It shows the centrality of data and intelligence sharing to real-time defence, and the dependence of sharing on secure infrastructures, common protocols, and clear accountability for data handling. It

also shows trust functioning in both directions. Visible security competence builds client–bank trust and reputation (Khan et al., 2017; Akinbowale et al., 2019), while weakly governed fintech adoption imports cyber and operational risk that damages performance (Al-shari & Lokhande, 2023). These observations substantiate Propositions 4 through 7. The same collaborative tie can be an asset or a liability depending on the regulatory, infrastructural, communicative and relational conditions in which it is embedded.

The Urban Stakes in Emerging Economies

The fourth theme returns the analysis to the city. Cyber fraud exposure clusters where banked publics, digital channels and platform commerce are densest, which is to say in the urban centres of emerging economies (Chukwuma, 2022; Nwekpa et al., 2019). The comparative evidence indicates that such economies digitalise faster than they secure (Gupta & Agarwal, 2017; Lukonga, 2018). Nigeria exemplifies the conjunction: rapid digital financial inclusion, an urban youth population among whom cybercrime has grown rapidly (Hassan et al., 2012), and institutional capacity still catching up with the policing demands of cyberspace (Akuta, 2012). It follows that the resilience of digital finance in such settings is an urban governance problem in the full sense. It implicates not only bank boardrooms and supervisory authorities but the planning, infrastructure and institutional ecology of cities themselves. On the evidence assembled here, moving the analytical frame from how banks defend to how cities co-secure digital finance is a substantive redirection of both research and policy.

Communication as the Infrastructure of Trust and Collective Urban Defence

A fifth thread, dispersed until now, deserves to be drawn together explicitly. Across the corpus, the studies that come closest to identifying what actually works are all, on inspection, describing communicative phenomena without naming them as such. Ogoh's (2016) practitioners named effective communication among their frontline defences. Khan et al. (2017) found that security technology builds strong client–bank relationships. Akinbowale et al. (2019) showed that cyber fraud damages reputation. Messages sent and received, relationships built or eroded through repeated exchange, confidence won or lost in public perception: all of these are communicative achievements before they are anything else. Yet none of the reviewed studies treats communication as an object of analysis in its own right. It appears everywhere as a background condition and nowhere as a variable to be measured, strengthened or governed. This paper's contribution is to name that background condition and bring it to the foreground. In a networked urban financial ecosystem, resilience is in no small part a communication achievement, and improving it will depend as much on redesigning how banks, fintech firms,

regulators and the urban publics they serve talk to one another as on any new technology of detection or defence.

Conclusion and Recommendations

Conclusion

This paper set out to rethink cybercrime and banking resilience for an era of networked threats in networked, communicating cities. It has argued, first, that the prevailing firm-level technical framing of cybercrime in banking is analytically inadequate. Because banks are interconnected through shared, urban-sited infrastructures that carry both money and information, exposure, vulnerability and resilience are properties of an urban financial ecosystem rather than of isolated institutions. Second, drawing on situational crime prevention theory, the institutional perspective and a communication-centred understanding of networks, it has theorised bank–fintech collaboration as distributed security governance: the implementation of opportunity-reducing techniques at the scale of the ecosystem, made possible and durable by regulative coordination, professional norms, trust, and, running beneath all three, the everyday transmission of accurate and timely information between organisations that must learn to speak to one another under pressure. Third, it has developed a conceptual framework linking urban cyber-threat exposure, collaborative intensity and banking resilience, specified seven testable propositions, and identified regulatory coordination, data-sharing and communication infrastructures, and trust networks as the moderating conditions on which the framework's promise depends.

The synthesis of ten empirical studies from Nigeria, South Africa, Kenya and Yemen substantiates the framework's plausibility. Cybercrime measurably damages bank performance and reputation. Firm-level controls mitigate but cannot eliminate exposure in a networked system. And collaboration, with fintech firms, regulators and industry forums, recurs across the corpus as the practitioner-endorsed path forward, even where, as this paper has shown, its communicative machinery is rarely examined directly. The contribution of this study to the growing body of cyber-criminological and sociological scholarship on Nigerian cyberspace and banking infrastructure is threefold: a reconceptualisation of the problem at the urban-ecosystem scale; a theorised, proposition-generating account of the mechanism, namely collaborative intensity under enabling conditions, through which resilience is produced; and an insistence that this mechanism is ultimately a communicative one. In rapidly urbanising emerging economies, where digital financial inclusion outpaces both security capability and the communication

infrastructure needed to defend it, the stakes of getting this governance architecture right are considerable.

Recommendations

For banks, the priority is to move from procurement to partnership. This means leveraging fintech collaborations to develop customised cybersecurity solutions aligned with each bank's specific needs and infrastructure, while institutionalising multidisciplinary risk units and continuous capacity building so that collaborative intelligence is absorbed, communicated internally and acted upon rather than merely contracted (Granåsen & Andersson, 2016; Mayahi & Humaid, 2016).

For fintech firms, the priority is partnership governance. This means accepting accountability for data protection as data processors, investing in the transparency and disclosure practices that build inter-organisational trust, and recognising that poorly governed and poorly communicated integration imports the high risks collaboration exists to reduce (Al-shari & Lokhande, 2023).

For regulators and urban policymakers, the priority is to supply the moderating conditions on which distributed security governance depends: a firm regulatory and policy framework for cybersecurity in the banking sector, strengthened cross-industry coordination through structures such as the Nigeria Electronic Fraud Forum, mandated and secure threat-intelligence sharing and communication protocols, and sustained monitoring of the long-term effects of cybersecurity investments (Nwobia et al., 2020; Boer & Vasquez, 2017). City governments and infrastructure agencies should in turn treat payment systems, data centres and telecommunications backbones as critical urban infrastructure, integrating their protection into urban resilience planning rather than leaving it wholly to sectoral regulation.

For communication and public-facing institutions, banks, regulators and consumer-protection bodies should invest directly in the quality of the ordinary messages through which customers are warned about cyber risk, including SMS alerts, in-app notifications, radio and community announcements. A public that cannot distinguish a genuine bank message from a fraudulent one remains the ecosystem's most exposed node, whatever the sophistication of back-end defences.

For researchers, the seven propositions advanced here constitute an agenda. Comparative, multi-city empirical studies should measure urban cyber-threat exposure, collaborative intensity and the quality of inter-organisational communication directly, test their interaction on resilience and performance

outcomes, and probe the moderating force of regulatory coordination, data-sharing and communication infrastructure, and trust. Such work would carry the study of cybercrime and banking beyond the question of how individual banks defend themselves, toward the question this paper has sought to open: how the organisations that jointly constitute an urban financial ecosystem can govern their collective security through structured, trust-bearing communication.

References

Aduge-Ani, D. C. (2015). Cybercrime: Implications and control measures. *Journal of Law, Policy and Globalisation*, 34, 173–181.

Aduge-Ani, D. I. (2015). Electronic banking and fraud in Nigeria: Challenges of conformity and challenges to conformity. *European Scientific Journal*, 11(17), 142–162.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2019). The assessment of the impact of cyber fraud in the South African banking industry. *Journal of Financial Crime*, 1, 1–15.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced scorecard: A survey of literature. *Journal of Financial Crime,* 27(3), 945–958.

Akintoye, R., Ogunode, O., Ajayi, M., & Abimbola, A. J. (2022). Cybersecurity and financial innovation of selected deposit money banks in Nigeria. Universal *Journal of Accounting and Finance,* 10(3), 643–652.

Akuta, M. C. (2012). Policing the cyberspace: Challenges and strategies. In The Road to Democracy in Nigeria (pp. 151–170). Springer.

Alese, B. K., Thompson, A. F. B., Alowolodu, O. D., & Blessing, E. O. (2018). Multilevel authentication system for stemming crime in online banking. *Interdisciplinary Journal of Information, Knowledge, and Management,* 13, 79–94.

Al-shari, H. A., & Lokhande, M. A. (2023). The relationship between the risks of adopting FinTech in banks and their impact on performance. *Cogent Business & Management,* 10(1), 1–35.

APWG. (2010). Phishing activity trends report, 2nd quarter 2010. Anti-Phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q2_2010.pdf

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour*, 38, 304–312.

Australian Federal Police. (2012). Internet banking fraud. https://www.afp.gov.au/sites/default/files/PDF/Reports/2012%20Internet%20Banking%2 0Fraud.pdf

Boer, M., & Vasquez, J. (2017). Cyber security and financial stability: How cyber-attacks could materially impact the global financial system.

Bonaneri, N. N. (2021). University of Nairobi, 91p.

Cherian, S. (2014). Understanding DDoS attacks and their implications for banks. *Journal of Information Systems Security*, 8(1), 67–82.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security,* 33(8), 719–731.

Chukwuma, O. V. (2022). Deposit-taking banks and cyber fraud among the public in Enugu urban, Enugu State, Nigeria. *Global Research Journal of Accounting and Finance,* 10, 1–13.

Clarke, R. V. G. (1980). "Situational" crime prevention: Theory and practice. *The British Journal of Criminology,* 20(2), 136–147.

Creado, A., & Ramteke, R. (2020). Hacking and its impact on the banking sector: A case study analysis. *Journal of Information Security,* 7(4), 321–339.

Economic and Financial Crimes Commission (EFCC). (2015). About us. https://efccnigeria.org/efcc/about-efcc

Equinix. (2021). Keeping critical infrastructure safe from cyber attacks. https://blog.equinix.com/blog/2021/09/07/keeping-critical-infrastructure-safe-from-cyber-attacks/

Gordon, L. A., & Loeb, M. P. (2003). Cybersecurity and economic incentives. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 9p.

Granåsen, K. F., & Andersson, S. (2016). Managing cyber risk in banks: A multidisciplinary approach. *Journal of Financial Perspectives,* 4(3), 79–95.

Gupta, R., & Agarwal, S. P. (2017). A comparative study of cyber threats in emerging economies. *An International Journal of Management & Information Technology,* 8(2), 24–28.

Gupta, S. (2012). Cybercrimes: A decade of IT and law enforcement perspectives in India. Procedia Technology, 4, 115–120. https://doi.org/10.1016/j.protcy.2012.05.022

Hassan, N. M., Lass, M. M., & Makinde, S. O. (2012). Cybercrime and its impacts on Nigerian society: An empirical study. I*nformation Management and Business Review,* 4(5), 265–272.

Hastings, B. (2015). Cybersecurity: A growing concern for banking. J*ournal of Investment Compliance,* 16(3), 5–7. https://doi.org/10.1108/JIC-01-2015-0005

Ibikunle, F., & Odunayo, O. (2013). Identity theft in online banking: A comparative analysis of Nigerian and South African banking sectors. *Journal of Financial Risk Management*, 4(2), 101–118.

Johnson, K. N. (2015). Managing cyber risk. *Georgia Law Review,* 50(2), 548–592.

Kaspersky Lab. (2022). APT trends report Q4 2021. https://media.kasperskydaily.com/wp-content/uploads/sites/85/2022/02/17063001/APT-Trends-Report-Q4-2021.pdf

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2017). Utilising biometric system for enhancing cyber security in banking sector: A systematic analysis. IEEE Access, 99(1), 1–10.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change,* 80(3), 541–555.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cybercrime and the organisation of the police: The results of two empirical studies in the Netherlands. *Journal of Cyber Criminology*, 7(1), 1–7.

Lukonga, I. (2018). Cybercrime in Africa: Policies and practical computing solutions. *International Journal of Computer Applications,* 179(38), 1–4.

Mayahi, H., & Humaid, M. S. (2016). Building capacity for cybersecurity: Employee training and technology infrastructure. *Information Systems Security,* 25(4), 219–228.

Muritala, T. A., Ijaiya, M. A., & Adeniran, D. S. (2017). Fraud and bank performance nexus: Evidence from Nigeria using vector error correction model. *Journal of Business Finance*, 3(1), 21–29.

Nwekpa, K. C., Ezezue, B. O., Nwabuike, C. C., & Ibeme, P. N. (2019). Effect of cybercrime on the performance of e-business in Konga.com. International Digital Organisation for Scientific Research (IDOSR) *Journal of Arts and Management*, 4(2), 87–97.

Nwobia, C., Adigwe, P. K., Ezu, G. K., & Okoye, N. J. (2020). Electronic fraud and performance of deposit money banks in Nigeria: 2008–2018. *International Journal of Business and Management,* 15(6), 126–136.

Ogoh, B. E. (2016). The role management plays in combating cybercrime within Nigeria's banking industry. *Journal of Social Sciences,* 27(1), 53–58.

Raghavan, A., & Parthiban, L. (2014). The effect of cybercrime on a bank's finances. International *Journal of Current Research and Academic Review,* 2(2), 173–178.

Rathore, D. S. H., & Marwaha, K. (2015). Cyber crime in banking sector. *Law Mantra Think Beyond Others*, 2(7), 1–7.

Tendulkar, R. (2013). Cyber-crime, securities markets and systemic risk. *Chartered Financial Analyst (CFA) Digest*, 43(4), 35–43.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Social Science Research Network Electronic Journal,* 22(4), 239–309.

Wada, T., & Odulaja, D. (2012). The impact of cybercrime on banking operations in Nigeria. *Journal of Internet Banking and Commerce,* 17(3), 1–9.