



Design of a Quantitative Cyber Risk Assessment Framework for Fintech Organizations in Nigeria

Adejumo Modupe Anthonia

Corresponding Author Email: annieade01@gmail.com

Fatimah Adamu-Fika

fateemahfika@gmail.com

Abdulrahman Tunde Alabelewe

abdulrahman.alabelewe@gmail.com

Samson Adeyinka

Samson.adeyinka@afit.edu.ng

Dauda Sule

daudas@gmail.com

and

Renshaw Onah Benjamin

renshawbenjamin4@gmail.com

Abstract

The rapid expansion of financial technology (Fintech) in Nigeria has intensified the need for advanced cybersecurity risk management. Traditional risk assessment methods in the sector rely on qualitative labels such as High or Low, which are subjective and fail to show explicit monetary exposure. To address this gap, this study developed a localized Quantitative Cyber Risk Assessment Framework to measure and prioritize cyber threats in financial terms for Nigerian fintech organizations. Adopting a design science and quantitative research approach, a web based Decision Support System (DSS) was engineered using Next.js and TypeScript. The risk engine operationalized Single Loss Expectancy (SLE), Annualized Loss Expectancy (ALE), and Return on Security

Investment (ROSI), calibrated with NIBSS and FITC fraud data, applying a verified 2.1% fraud to transaction ratio as the Exposure Factor. A controlled simulation of a hypothetical fintech organization showed an unmitigated Annualized Loss Expectancy of ₦390,600,000, reduced to ₦58,590,000 after applying anti phishing controls costing ₦50,000,000, yielding a Return on Security Investment of 564.02%. The study concluded that localized quantitative frameworks replace subjective judgment with actionable financial intelligence, optimizing cybersecurity planning, budgeting, and regulatory compliance in the Nigerian fintech sector.

Keywords: Cyber Risk Quantification, Annualized Loss Expectancy, Fintech Cybersecurity, Decision Support System, Nigeria.

Introduction

The rapid digitization of financial services in Nigeria, driven by Central Bank of Nigeria (CBN) initiatives such as the Cashless 2.0 policy, has increased adoption of mobile banking, electronic payments, and Point of Sale systems, expanding the attack surface for cyber threats. Data from the Nigeria Inter Bank Settlement System (NIBSS) shows a persistent rise in fraud incidents, yet many fintech organizations still lack the capability to quantify potential losses arising from cyber threats. Most existing risk assessment approaches rely on qualitative classifications such as High, Medium, or Low, which are subjective and do not provide the financial precision required for decision making, making it difficult to justify cybersecurity investments (Anthony & Jesudasimi, 2025). Expected Utility Theory and Protection Motivation Theory jointly underpin this study. Expected Utility Theory suggests that a rational decision maker approves a security control only when the expected reduction in loss exceeds its cost, while Protection Motivation Theory explains that protective action depends on both threat appraisal and coping appraisal. The proposed framework operationalizes both by quantifying threat severity as Annualized Loss Expectancy and coping efficacy as Return on Security Investment. Collectively, prior studies confirm that a localized, code based Decision Support System calibrated with the 2.1% Nigerian fraud ratio has not previously been implemented. This study addresses that gap by embedding the ratio into an automated Next.js and TypeScript risk engine capable of producing organization specific ALE and ROSI values, with the aim of enabling Nigerian fintech firms to measure and prioritise cyber threats using numerical risk scoring.

Conceptual Clarifications

Several constructs underpin the proposed framework and are defined here for clarity. The Exposure Factor (EF) is the proportion of an asset's value expected to be lost in a single successful cyber incident; in this study it is set at the verified 2.1% fraud to transaction ratio. Asset Valuation (AV) refers to the monetary value of the information or transaction asset placed at risk. The Annualized Rate of Occurrence (ARO) is the expected frequency, per year, with which a given threat vector is expected to materialise against that asset. Single Loss Expectancy (SLE) is the monetary loss expected from one occurrence of a threat, computed as the Asset Value multiplied by the Exposure Factor: $SLE = AV \times EF$. Annualized Loss Expectancy (ALE) extends SLE across a year by multiplying it by the Annualized Rate of Occurrence: $ALE = SLE \times ARO$, which expands to $ALE = AV \times EF \times ARO$. Return on Security Investment (ROSI) expresses the financial value of a proposed control as a percentage, computed as Risk Reduction minus the Cost of Security, divided by the Cost of Security. An automated rating algorithm classifies exposure using these outputs, assigning Critical when ALE is at least 15% of Asset Value, High at 8%, Medium at 3%, and Low below 3%. These thresholds allow the numerical ALE figure to be mapped back onto familiar qualitative categories without losing its underlying financial precision.

Literature Review

Anthony and Jesudarasimi (2025) analysed a decade of NIBSS transaction data and established a statistically verifiable 2.1% fraud to transaction ratio ($p = 0.029$), demonstrating that fraud incidence measurably inhibits fintech adoption among Nigerian consumers; their contribution was, however, descriptive, offering a validated ratio without translating it into an organisation level financial model or computational tool. Pubtexto Journals (2025) designed an adaptive, explainable AI framework that achieved high threat detection accuracy for resource constrained fintech SMEs, addressing the operational challenge of identifying attacks in low resource environments; the framework's focus, however, was detection and classification rather than estimating the monetary loss a detected threat would impose, leaving the financial dimension of risk unaddressed. Enigbokan et al. (2024) examined the mathematical properties of ordinal risk heat maps and demonstrated that qualitative High, Medium, Low scales introduce distortion into corporate budgeting decisions because ordinal categories lack the linearity required for meaningful arithmetic comparison; their critique motivates the case for quantitative alternatives but does not itself propose or implement one.

Olowu and Chima (2025) applied predictive modelling techniques to forecast cyber risk trends in Nigerian fintech, contributing a forward looking risk estimation approach; the model, however, produced probabilistic risk scores rather than Naira denominated loss figures, and was not embedded in a decision support tool usable

by practitioners. Adewale (2025) evaluated the applicability of global frameworks such as NIST CSF 2.0 to West African fintech startups and found that these frameworks remain abstract and difficult to operationalise without local calibration, reinforcing the need for parameters, such as exposure factors, drawn from Nigerian data rather than imported benchmarks. Young (2025) analysed digital switching network data and showed that a small volume of severe exploits, rather than high frequency, low impact attacks, accounts for most capital flight in Nigerian settlement systems, indicating that severity weighted, rather than frequency only, risk measures better reflect actual financial exposure.

Collectively, these studies establish that a statistically sound Nigerian fraud ratio exists (Anthony & Jesudarasimi, 2025), that detection focused AI tools are maturing (Pubtexto Journals, 2025), that qualitative heat maps are mathematically unsuited to budgeting (Enigbokan et al., 2024), that imported frameworks require local calibration (Adewale, 2025), and that severity rather than volume drives financial loss (Young, 2025). None of the reviewed studies, however, combines a locally calibrated exposure factor with an automated, code based Decision Support System capable of producing organisation specific, Naira denominated ALE and ROSI figures. This absence of a computational bridge between validated local statistics and actionable financial output constitutes the gap addressed by the present study.

Methodology

This study adopted a quantitative design science research approach combining mathematical modelling with prototype development. The Exposure Factor (EF) used the 2.1% fraud to transaction ratio established by Anthony and Jesudarasimi (2025); the Annualized Rate of Occurrence (ARO) was drawn from the 2024 NIBSS Fraud Landscape report and 2025 FITC quarterly reports; and Asset Valuation (AV) was modelled on transaction benchmarks for Nigerian fintech SMEs as categorised by the CBN (2024). The Decision Support System was implemented as a three-layer web application using React on Next.js, with TypeScript for type safety in monetary computations. The Input Layer captures annual asset value, threat vector, security implementation cost, and control effectiveness. The Processing Layer applies the Exposure Factor to compute SLE and ALE. The Output Layer presents results on a dashboard featuring a financial impact comparison chart and an automated PDF export function. A controlled simulation was designed around a hypothetical mid sized Nigerian fintech organisation, Fintech-X, with an Annual Asset Value of ₦3,000,000,000, exposed to a Social Engineering/Phishing threat vector with an Annualized Rate of Occurrence of 6.2, and a proposed Email Security Gateway and staff training control costing ₦50,000,000 at 85% effectiveness.

Results

The framework was built using React operating within Next.js, with TypeScript ensuring type safety for large Naira values and custom SVG charts providing real time visual comparison of financial impact before and after proposed security investments. Applying the simulation inputs, the engine returned a Single Loss Expectancy of ₦63,000,000 per breach and an unmitigated Annualized Loss Expectancy of ₦390,600,000, automatically classified as Critical Risk. After applying 85% control effectiveness, the mitigated ALE fell to ₦58,590,000, an annual risk reduction of ₦332,010,000. Subtracting the ₦50,000,000 implementation cost produced a Return on Security Investment of 564.02%. Exercising the engine against the remaining threat vectors, holding Asset Value and Exposure Factor constant, produced an unmitigated ALE of approximately ₦283,500,000 for Web/API Compromise (ARO 4.5), ₦132,300,000 for System/Network Breach (ARO 2.1), and ₦113,400,000 for Insider Threat (ARO 1.8).

Table 1: Comparison of the Proposed Framework with the Base Study

Evaluation Metric	Base Paper (Anthony & Jesudarasimi, 2025)	Proposed Framework (Next.js DSS)
Primary Output	Descriptive statistics (2.1% fraud ratio, $p = 0.029$)	Naira denominated ALE, SLE, and ROSI
Risk Measurement	Static historical percentage	Dynamic engine applying the ratio to varying asset values
Organisational Utility	Academic and regulatory awareness	Practical budgeting and ROI tool for CTOs and CFOs
Decision Support	Identifies that fraud deters adoption	Tests control cost against financial viability

Discussion

This shows that expressing risk as a function of both severity and frequency, rather than severity alone, allows management to correctly prioritise Social Engineering and Phishing as the vector warranting the most urgent investment, consistent with FITC (2025) findings that social engineering remains the leading threat category across Nigerian financial institutions. As shown in Table 1, the proposed dashboard advances the descriptive contribution of Anthony and Jesudarasimi (2025) into an operational tool capable of quantifying and testing the financial viability of specific security controls. Under a conventional High, Medium, Low matrix, the Social Engineering threat facing Fintech-X would simply be labelled High Risk, offering no financial context. The framework resolves this by converting the 2.1% fraud ratio into a live calculation, ranking threats by actual monetary damage.

The results also support compliance with the CBN Risk Based Cybersecurity Framework (2024), which requires a documented, defensible risk methodology, since the dashboard produces an auditable Naira figure that can be regenerated as transaction volumes or threat frequencies change. The framework's generalisability is bounded by the accuracy of the Exposure Factor and Annualized Rate of Occurrence supplied; where an organisation's fraud experience diverges from the 2.1% national average, parameters should be recalibrated using the organisation's own historical data.

Evaluation

The framework was considered validated if it produced realistic estimates, supported cost benefit analysis, and improved on qualitative methods. Against these criteria, the simulated Fintech-X scenario produced Naira figures consistent with the scale of a mid sized fintech organisation's transaction exposure; the computed Return on Security Investment of 564.02% demonstrates that the engine supports direct cost benefit analysis of a proposed control before it is purchased; and, as set out in Table 1, the dashboard's dynamic, monetary output represents a measurable improvement over the static, qualitative High, Medium, Low matrix used in comparable prior work. The framework is therefore judged to satisfy its stated validation criteria.

Conclusion

This study developed and validated a localized Quantitative Cyber Risk Assessment Framework for Nigerian fintech organisations, demonstrating that cyber risk can be expressed in concrete financial terms rather than subjective qualitative labels. By embedding the 2.1% fraud to transaction ratio into an automated Next.js based Decision Support System, the framework computed SLE, ALE, and ROSI for a simulated organisation, projecting an annual exposure of ₦390,600,000 that was reduced to ₦58,590,000 through a cost justified security control, yielding a 564.02% Return on Security Investment. The study was limited by its reliance on a simulated rather than live scenario and on publicly available NIBSS and FITC statistics rather than proprietary incident data.

Recommendations

Future work should incorporate machine learning based predictive threat modelling, real time threat intelligence, non financial impact measures, and validation using real organisational datasets. Nigerian fintech organisations and regulators are encouraged to adopt quantitative, rather than purely qualitative, cyber risk assessment as a standard component of security governance.

Acknowledgments

The author thanks the project supervisor, Dr Fatima Adamu-Fika, and co-supervisor, Mr Tunde A. Alabelewe, for their guidance, and the Department of Cyber Security, Air Force Institute of Technology, Kaduna, for the academic support provided throughout this research.

References

- Adewale, O. (2025). Localized exposure calibration for fintech platforms: Evaluating global risk frameworks in West African startups (Undergraduate project report). Air Force Institute of Technology.
- Anthony, C., & Jesudarasimi, E. (2025). The impact of cybersecurity risks in fintech and mobile banking adoption in Nigeria. *Nigerian Journal of Financial Technology*, 4(1), 1–18.
- Central Bank of Nigeria. (2024). Risk-based cybersecurity framework and guidelines for Deposit Money Banks and Payment Service Banks. <https://www.cbn.gov.ng>
- Enigbokan, T., Okafor, C., & Bello, R. (2024). The quantitative veneer: Limitations of ordinal risk heat maps in financial systems. *Journal of Information Security and Applications*, 78, 103–119.
- Financial Institutions Training Centre. (2025). Quarterly report on fraud and forgery in Nigerian financial institutions: 2024 annual summary. <https://fitc-ng.com/reports>
- IBM Security. (2023). Cost of a data breach report 2023. <https://www.ibm.com/reports/data-breach>
- National Institute of Standards and Technology. (2018). Cybersecurity framework (CSF) version 1.1. <https://www.nist.gov/cyberframework>
- Nigeria Inter-Bank Settlement System. (2024). The Nigerian financial services industry fraud landscape. <https://nibss-plc.com.ng/insights>
- Olowu, D., & Chima, P. (2025). Predictive modeling of cyber risk in Nigerian fintech: A quantitative approach. *Nigerian Journal of Technology and Security*, 7(2), 14–29.
- Pubtexto Journals. (2025). An adaptive explainable AI framework for threat detection in resource-constrained fintech SMEs. *Pubtexto Journal of Computer Science*, 3(2), 45–61.
- Verizon. (2024). Data breach investigations report (DBIR). <https://www.verizon.com/business/resources/reports/dbir>
- Young, K. (2025). The multi-channel severity disconnection: Attack volume versus capital flight in digital switching networks (Master's thesis). University of Lagos.