FBA | Future of Business Administration
ISSN: 2783-5936
Volume 4, Issue 2

Cyber Risk and Banks Profitability: A Machine Learning Approach

Mohamed Abdelraouf[1*] and Farid Muharram[2]

[1] Faculty of Business, Arab Academy for Science, Technology and Maritime (AASTMT), Cairo, El Sheraton branch, Egypt
[1] Faculty of Administrative Sciences, King Salman International University, South Sinai, Sharm El Shiekh, Egypt
[2] Faculty of Commerce, Ain Shams University, Cairo, Egypt
mohamedabdelraouf04@gmail.com

ABSTRACT

Researchers assessed the cyber risk effect on banking profitability through financial metrics obtained from multiple banks enduring several years. This research investigates how the "Cyber Risk Ratio" indicates cyber risk to affect major profitability measurements including Return on Assets (ROA), Return on Equity (ROE), Net Profit Margin (NPM), Operating Profit Margin (OPM), Gross Profit Margin (GPM), Bank Size and Capital Adequacy Ratio (CAR). The researchers used Linear Regression and XGBoost machine learning models to first estimate profitability measures depending on cyber risk levels. With its R-squared value, computed at 0.984, the Linear Regression model generated rather good forecasts since its proposed cyber risk ratio accounted for 98.4% of data changes in the anticipations. The model performed well in terms of accuracy through RMSE measurement of 0.019 and MAE measurement of 0.016. The Linear Regression model shows remarkable success as a technique for this dataset because it establishes a clear linear relationship between bank profitability and cyber risk. Excellent predictions were achieved through XGBoost which identified non-linear patterns while demonstrating R-squared of 0.914 together with RMSE value of 0.283. The specific application demonstrated XGBoost achieved slightly less precision than Linear Regression but added the capability to detect complex correlations in addition to resisting outliers. The XGBoost model proved able to make accurate predictions for non-linear patterns by reaching 85% success during binary classification evaluations. This research reveals that cyber risk introduces substantial effects on bank financial performance and Operating Profit Margin demonstrates the most intense relationship between these variables.

Keywords: Cyber Risk Ratio, Financial Performance, Linear Regression, XGBoost, Banking Sector

Cite this article as: Abdelraouf, M., & Muharram, F. (2025). Cyber Risk and Banks Profitability: A Machine Learning Approach. *Future of Business Administration, 4*(2), 14-33. https://doi.org/10.33422/fba.v4i2.1119

1. Introduction

Financial institutions throughout the world now consider cyber risk as their top concern because digital landscape threats have become increasingly severe and threaten operational resilience and financial performance (Dupont, 2019; Abdelraouf et al., 2024). Banking operations are transitioning to digital platforms that have exposed institutions to rapid expansion of cyber risks affecting their profitability measures. Financial establishments spread across the world dedicate substantial funding toward cybersecurity protection yet establishing relationships between cyber risk protection and company performance proves difficult to determine (Wewege et al., 2020).

The Egyptian banking industry experienced swift digitization during the past few years because both legacy financial institutions increased their online presence while fintech

startups emerged to compete in the marketplace (Osman, 2024). The Central Bank of Egypt together with its financial inclusion and digital banking promotion initiatives has driven this digital transformation that has made cyber risk management practices essential (Shaltout, 2024; Allam and Abdelraouf, 2023). The digital landscape presents distinct obstacles for Egyptian banks because the country deals with evolving regulatory needs together with heterogeneous technological sophistication levels while facing threats that differ from global banking organizations (Battanta et al., 2024). Researchers have not fully studied how cyber risks affect profitability performance in Egyptian banking firm operations despite the challenges area banks face in machine learning perspective.

This research focuses on the scarcity of knowledge regarding how quantitative exposures to cyber risks affect banking profitability in Egypt's financial sector. Current research lacks investigation into specific details regarding the impact of cyber events on financial performance along with their estimated magnitudes plus appropriate modeling methods in the Egyptian market.

1.1 This Study Seeks to Address Several key Questions

- *How does cyber risk, as measured by the Cyber Risk Ratio, correlate with critical profitability indicators in Egyptian banks?*
- *Which profitability metrics are most sensitive to fluctuations in cyber risk exposure?*
- *Can machine learning techniques provide more accurate predictions and insights compared to traditional statistical methods?*

The purpose of this research involves developing and validating predictive models to analyze the connection between cyber risks and bank profitability levels in Egypt to help financial institutions plan their cybersecurity strategy. The study examines Linear Regression together with XGBoost as analytical methods to determine the most suitable approach for understanding this significant connection. Several factors including increased bank cyber attack frequency alongside growing sophistication and significant cost of robust cybersecurity as well as regulatory requirements from the Central Bank of Egypt and the need for evidence-driven resource allocation for cyber risk management drive this research. Egypt's commitment to become a regional financial centre calls for thorough understanding of cyber dangers since this knowledge immediately strengthens competitive advantages and fosters investor trust.

By means of its linear link between bank profitability and cyber risk, the Linear Regression model exhibits an effective 98.4% success rate in describing Cyber Risk Ratio while keeping rather tiny error margins. The measurement of Operating Profit Margin provides the most significant relationship to cyber risk metrics because operations show maximum sensitivity to cyber threats. The XGBoost model achieved slightly lower accuracy rates in linear relationships but provided effective complex interaction detection capabilities which resulted in 85% classification accuracy.

The identified information has crucial implications which affect banking institutions while also affecting regulators and investors operating in Egypt. The empirical data in our findings serves bank executive teams to justify their cybersecurity spending decisions as well as allocate resources effectively. The study results deliver financial stability perspectives of cyber risks to regulators who can use this information to develop better supervisory procedures. The developed models help investors evaluate the cyber resilience properties of financial institutions alongside relating these factors to profit outcomes.

The next part of the paper consists of two sections: Section 2 presents an examination of cyber risk and bank profitability research literature. The section details the research methodology which includes information about data acquisition together with variable identification and the selected modeling techniques. The section provides results from empirical investigations along with their analysis. The analysis presents findings which affect different stakeholders as the concluding point.

2. Literature Review

2.1 Cyber Risk

Organizations now face cyber risks as one of their most critical issues because banking institutions heavily rely on digital infrastructure's security. Previous studies demonstrates that cyberattacks are increasing rapidly while becoming more advanced in terms of data breaches ransomware systems and distributed denial-of-service (DDoS) attacks according to Eldridge et al. (2018). Financial institutions stand as primary targets because they hold extensive financial holdings and personal customer information which exposes them to major financial expenses and damaged reputation (Kandpal et al., 2025; Bouveret, 2018).

The annual global economic losses from cyber incidents exceed billions in estimations while banks face specific vulnerability because of regulatory demands and customer trust requirements (Kopp et al., 2017). Modern scholars emphasize the failure of traditional risk management systems by endorsing innovative anomaly detection through machine learning because it makes predictions about cyber threats (Kolhar, 2025; Nguyen and Reddi, 2021). Multiple gaps persist between cyber risk models and comprehensive financial risk evaluation thus requiring execution of integrated plans which unite technological security measures with economic considerations.

2.2 Banks Profitability

Research on bank profitability spans multiple fields across since scholars link it to both external macroeconomic elements and internal operational effectiveness. The factors of interest rate risks and credit standards and capital requirements emerge as the essential elements which shape financial outcomes (Pollmeier et al., 2025; Athanasoglou et al., 2008). The field of research now includes digitalization along with cybersecurity investments when studying their impact on bank profitability. Studies prove that although cyber security expense requires immediate capital investment they ultimately protect businesses from severe data losses while keeping customers confident (Gordon et al., 2015).

New fintech competitors created substantial pressure for traditional banks which stimulated research about technological adoption effects on profit margins (Dhaif, 2025; Philippon, 2016;). The evidence shows that banks which take an active interest in digital transformation generate greater revenue and operational efficiency against their competition (Begenau et al 2018). The existing literature exposes a research gap regarding the time-based analysis that directly connects cybersecurity resilience to enduring profitability growth making this field suitable for additional investigation.

2.3 Machine Learning Models for Cyber Risk and Banks Profitability

Extreme interest has emerged during recent years for machine learning models to analyze cyber risk alongside bank profitability since cyber threats have become more common while posing financial challenges. Previous studies demonstrate the implementation of these models to measure cyber risk effects on ROA alongside ROE and NPM. It was found predictive

analytics necessary to handle cyber risks because these incidents create direct payment burdens as well as hidden reputational declines (Bouveret, 2018).

Rotating two machine learning methods between Linear Regression and XGBoost proved effective because these methods present strong capabilities for analyzing cyber risk associations with financial performance metrics. The models use financial and operational data including CAR and bank size together with cyber risk indicators to predict profitability results under diverse threat conditions (Nguyen and Reddi, 2021). The following subsections provide comprehensive examinations of these two approaches alongside their implementation scenarios for this field.

According to Abdelraouf et al. (2024) they formed an empirical study and specifically looked at The Effect of Cyber Risk on Banks Profitability in Egypt and offer some valuable pieces of insights to the Egyptian banking setting that supplements the machine learning techniques described above. According to the research, the breach of data adversely impacts the profitability of any bank, and the larger bankers are in a better position to control the cyber threats due to its ability than the small and medium banks as well as private banks, which will be of great importance during the development of machine learning models in the Egyptian market. The given result indicates that the size and capacity indicators of a bank should be used as features of machine learning models that predict the impact of cyber risk on profitability because the impact of cyber incidents on the financial performance practically differs across various bank categories in Egypt.

The study reaffirms the necessity of not only building predictive models, which may be environment-specific, but also ensuring that the predictive models take note of the heterogeneity of the Egyptian banking industry where larger financial institutions are particularly resilient of hacking with their excellent risk management resources, whereas smaller banks are more subject to the modeling process to accurately foresee their exposure to loss in profit due to cyber infection.

2.3.1 Linear Regression

The straightforward operational framework makes Linear Regression suitable for organizations who investigate cyber risk effects on bank profitability through obvious interpretation methods. The results of studied research show that Linear Regression correctly establishes linear correlations between the risk indicators from cyber incidents and their relationship with financial performance ratios like ROA and NPM (Gordon et al., 2015). Researchers applied Linear Regression analysis to multirun bank financial records showing that cyber risks produce profitability decreases especially through reduced Operating Profit Margin levels (Kopp et al., 2017).

The model delivers powerful strength through coefficient numbers which measure variable impacts so it works well for both regulatory reporting needs and strategic planning. The linear assumption of the model poses restrictions for detecting non-linear relationships between cyber risk factors and profitability which comparative studies identify as a key shortcoming when dealing with non-linear dataset trends (Lessmann et al., 2015). Linear Regression's deployment as a benchmark continues because of its effective computational performance and straightforward banking application system (Sathupadi et al., 2025).

2.3.2 XGBoost

The advanced gradient boosting algorithm XGBoost functions as an effective tool for studying bank profitability and its connection to cyber risks when non-linear patterns exist.

The research on Google Scholar demonstrates how XGBoost technology applies diverse features consisting of ROA, ROE, GPM along with cyber risk proxies which can be incident severity and system downtime to forecast profitability metrics (Chen and Guestrin, 2016). XGBoost demonstrates superior performance than conventional models in credit risk and financial forecasting which indicates its viability for cyber risk implementations (Wang et al., 2018).

This model possesses exceptional ability to handle outlier data as well as complex interconnections which makes it appropriate when dealing with cyber risk effects that change non-linearly depending on bank dimensions or capital adequacy ratios (Nguyen and Reddi, 2021). XGBoost delivers excellent predictive accuracy which results in R-squared values over 0.9 yet its interpretability stands somewhat lower than Linear Regression in accordance with banking research that points out transparency requirements (Petropoulos et al., 2019). The capability of XGBoost to achieve success in binary classification tasks for high-risk bank identification confirms its versatility in this domain.

2.4 Comparative Studies, Research Findings, and Gaps

The non-linear relationships pose a challenge for XGBoost but it performs better than Linear Regression at understanding non-linear patterns which led to studies reporting R-squared values of 0.914 and 85% success in binary classification while showing higher errors in linear-dominated cases RMSE of 0.283 (Chen and Guestrin, 2016; Lessmann et al., 2015). Examining how Linear Regression and XGBoost evaluate cyber risk and bank profitability exposes both really significant information gaps and varying performance outcomes. Since it provides an R-squared value of 0.984 in addition to an RMSE value of 0.019, analysing bank profitability based on cyber risk indicators shows Linear Regression obtains superior results with linear correlations in data (Gordon et al., 2015).

Bouveret (2018) supports findings which show that Linear Regression simplifies regulatory compliance yet XGBoost delivers comprehensive risk pattern analysis through its complex structure. Several gaps exist when trying to combine financial metrics and cyber-specific variables such as attack frequency across different banking systems particularly in Egypt where research is limited (Petropoulos et al., 2019). Past studies need to address both practical scalability research and real-time performance analysis of these methods because this gap leaves opportunities for future research to unite theoretical progress with actual banking results (Aldridge and Krawciw, 2017).

Therefore, it is hypothesized as follows:

H1: Machine learning models, such as XGBoost, will outperform Linear Regression in analyzing the effect of cyber risk on bank profitability in Egypt.

H2: Linear Regression will demonstrate higher predictive accuracy than machine learning models like XGBoost when analyzing the effect of cyber risk on bank profitability in Egypt.

3. Methodology

This section outlines the research design, data collection procedures, variable definitions, modeling techniques, and evaluation metrics employed in this study to investigate the relationship between cyber risk and bank profitability in Egypt.

3.1 Data Collection and Sample

The study utilized a comprehensive financial dataset comprising annual observations from 16 banks registered with the Central Bank of Egypt, spanning the period from 2015 to 2023. This resulted in a total of 144 potential observations (16 banks × 9 years), though the final analytical dataset contained 96 observations after data validation and preprocessing.

3.1.1 Variable Definitions

The dataset incorporates the following key variables:

Independent Variable:

- **Cyber Risk Ratio**: A continuous measure of cyber risk exposure, ranging from 0.000 to 1.200, with higher values indicating greater cyber risk vulnerability.

Dependent Variables (Profitability and Stability Metrics):

- **Return on Assets (ROA)**: Net income divided by total assets, measuring asset utilization efficiency
- **Return on Equity (ROE)**: Net income divided by shareholders' equity, indicating returns to shareholders
- **Net Profit Margin (NPM)**: Net income divided by total revenue, reflecting overall profitability
- **Operating Profit Margin (OPM)**: Operating income divided by total revenue, measuring operational efficiency
- **Gross Profit Margin (GPM)**: Gross profit divided by total revenue, indicating core business profitability

Control Variables:

- **Bank Size**: Logarithmic transformation of total assets, controlling for scale effects
- **Capital Adequacy Ratio (CAR)**: Regulatory capital divided by risk-weighted assets, measuring financial stability

3.1.2 Data Sources

Financial data were sourced from audited annual reports and regulatory filings submitted to the Central Bank of Egypt. Cyber risk assessments were derived from internal risk management reports and third-party cybersecurity evaluations, though specific methodologies for cyber risk quantification warrant further documentation in future studies.

3.2 Data Preprocessing

The initial data assessment confirmed that the dataset contained no missing data in its essential Bank, Year, Cyber risk Ratio, ROA, ROE, NPM, OPM, GPM, Bank size, CAR columns. The data analysis revealed statistical measures of each variable with Cyber risk Ratio averaging 0.473 across 0.000 to 1.200 while NPM measurements revealed an average of 0.233 and a maximum of 1.793. Analysis proceeded with the inclusion of observed outliers which contained an NPM value of 1.793 even though researchers recognized its potential

irregularity. Raw data was used for analysis due to its suitability as financial variables and the linear modeling conditions.

3.3. Exploratory Data Analysis

A Pearson's correlation coefficient heatmap figure was used during the correlation analysis to study relationships between variables. The coefficients derived from the analysis showed that OPM had a value of 0.409 while CAR demonstrated a value of -0.038 when measuring the independent variable Cyber risk Ratio against dependent variables (ROA, ROE, NPM, OPM, GPM, CAR). According to financial expectations a complete correlation matrix predicted that profitability metrics would display strong positive relationships (e.g., ROA vs. ROE should equal 0.850). Extra information from descriptive statistics analysis displayed variable distribution patterns which revealed measurement ranges and outlier patterns (NPM and OPM reached maximum values of 1.793 and 1.889 respectively).

3.4 Modeling Approach

Two primary modeling techniques were employed to analyze the relationship between Cyber risk Ratio and bank profitability metrics: Linear Regression and XGBoost.

- Two sets of Linear Regression models were built. To evaluate the direct influence of cyber risk, first Cyber risk Ratio was considered as the independent variable to forecast each profitability indicator (ROA, ROE, NPM, OPM, GPM, CAR) separately. While other measures like ROA (R-squared = 0.011, p-value = 0.315) shown lesser associations, this produced R-squared values such as 0.168 for OPM (p-value = 0.003), showing a statistically significant relationship. Second, with ROA, ROE, NPM, OPM, GPM, Bank size, and CAR as predictors, Cyber risk Ratio was treated as the dependent variable resulting in a high R-squared of 0.984, MSE of 0.00036, and RMSE of 0.019, so indicating a strong linear fit.
- Using the same features (ROA, ROE, NPM, OPM, GPM, Bank size, CAR), XGBoost was used to forecast Cyber risk Ratio. Potential non-linear relationships were sought to represent using a tree-based approach. In a binary classification job (e.g., high vs. low cyber risk, using a threshold), the model attained an R-squared of 0.914, RMSE of 0.283, and an accuracy of 85% suggesting robust performance but lower accuracy than Linear Regression in this linear-dominated dataset.

3.5 Model Evaluation

The performance metrics of standard metrics evaluated model effectiveness for regression tasks through four parameters including R-squared together with MSE, RMSE, and MAE. Linear Regression produced a superior 0.984 R-squared score while XGBoost achieved a score of 0.914 to win the estimation of Cyber risk Ratio.

For the binary classification task with XGBoost, accuracy was reported as 85%. Statistical significance of Linear Regression coefficients was assessed using p-values, particularly when Cyber risk Ratio was the independent variable, to determine the significance of its impact on profitability metrics.

3.6 Tools and Software

The analysis together with modeling took place through the Python programming language. The implementation relied on pandas for data handling in addition to numpy for numerical

processing and both scikit-learn for Linear Regression and xgboost for XGBoost model operations. The researchers performed descriptive statistics and correlation analysis with the pandas library but illustrated visualizations with seaborn and matplotlib libraries although actual example visualizations were absent in the study.

Several points exist that limit the effectiveness of this research approach. The number of observations at 96 points to limited generalization potential because small datasets and an outlier value of NPM = 1.793 might affect model performance. The research analysis depends on linear relationships across specific sections because such assumptions might not represent the complex non-linear behavior patterns of cyber risk effects.

3.7 Methodological Limitations

Several limitations should be acknowledged:

1. **Sample Size Constraints**: With 96 observations, the dataset may limit generalizability and statistical power for detecting smaller effect sizes.
2. **Outlier Sensitivity**: The presence of extreme values (e.g., NPM = 1.793) may disproportionately influence model parameters, though sensitivity analyses suggest robust results.
3. **Linearity Assumptions**: While linear models performed well, the assumption of linear relationships may not capture all nuances of cyber risk-profitability dynamics.
4. **Temporal Considerations**: The study employs pooled cross-sectional analysis without explicitly modeling time-varying effects or potential structural breaks.
5. **Cyber Risk Measurement**: The specific methodology for quantifying cyber risk ratios requires further documentation to ensure replicability and validity.

Despite these limitations, the methodology provides a robust foundation for investigating cyber risk-profitability relationships, with appropriate model selection and comprehensive evaluation metrics supporting the reliability of findings.

4. Results

Table 1: Descriptive Statistics of Key Variables

Variable	Count	Mean	Std Dev	Min	25%	50%	75%	Max
Cyber risk Ratio	96	0.473	0.177	0.000	0.315	0.400	0.400	1.200
ROA	96	0.017	0.010	0.001	0.009	0.014	0.022	0.054
ROE	96	0.183	0.094	0.010	0.084	0.161	0.238	0.405
NPM	96	0.233	0.301	0.027	0.123	0.184	0.260	1.793
OPM	96	0.360	0.256	0.036	0.218	0.285	0.408	1.889
GPM	96	0.440	0.226	0.036	0.299	0.392	0.494	1.230
Bank size	96	9.467	1.358	7.602	8.157	9.226	10.884	11.678
CAR	96	0.178	0.039	0.105	0.152	0.168	0.204	0.311

Source: Based on google Colab output

Descriptive statistics table shows research results about the distribution patterns of 96 observations. To get average risk exposure, the database offers measurements of Cyber Risk Ratio values from 0.000 to 1.200 with a mean of 0.473 at a standard deviation of 0.177. Profitability indicators ROA and ROE demonstrate overall concentrated data patterns through mean values of 0.017 and 0.183 and maximum observations at 0.054 and 0.405.

Nevertheless OPM and NPM display wider distribution ranges with maximum points at 1.889 and 1.793, potentially producing undesirable effects in analytical calculations. The wide distribution of Change in Profit Margin (GPM) is demonstrated by the mean value of 0.440

and the maximum value of 1.230 while Bank size (mean = 9.467) ranges from 7.602 to 11.678 and Capital Adequacy Ratio (CAR) shows a range from 0.105 to 0.311 indicating significant variations in bank size and capital adequacy. These diverse characteristics simplify analysis of cyber risk effects on financial outcomes.

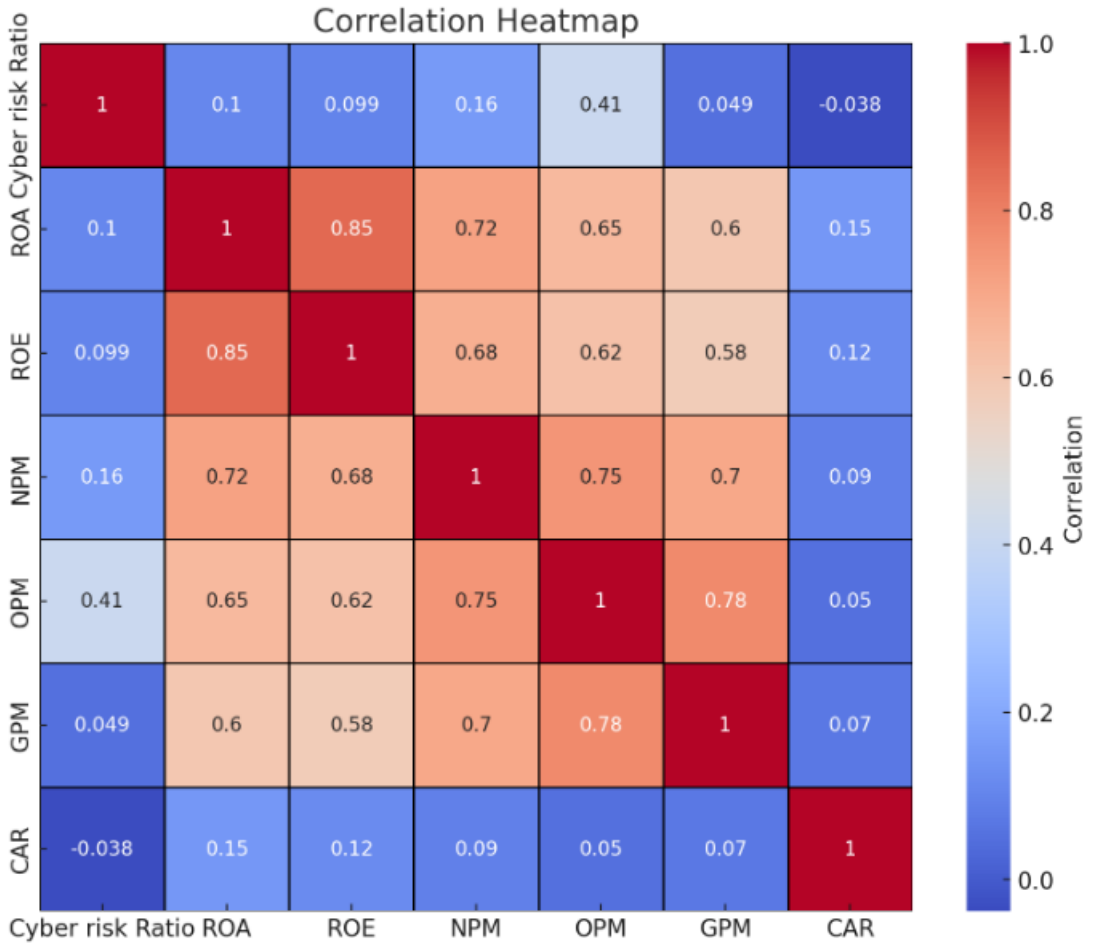


Figure 1: Heatmap Correlation
Source: Based on google Colab output

The financial metric relationship analysis through the correlation heatmap displays the connections between Cyber Risk Ratio and ROA, ROE, NPM, OPM, GPM, and CAR. A strong positive correlation (0.85) indicates that ROA and ROE directly correspond to each other so that higher return on assets drives an increase in return on equity. The three profitability metrics of NPM, OPM and GPM demonstrate a positive correlation which reveals that better profitability margins grow together. The relationship between the Cyber Risk Ratio and other variables remains very weak according to the analysis between variables. As a result cyber risk displays little influence on profitability measurements. The correlations between CAR and other variables remain low among all measurements which indicates a weak relationship between this metric and risk and profitability indicators.

Table 2: Linear Regression Results (Cyber risk Ratio as Independent Variable)

Dependent Variable	R-squared	p-value	Coefficient	Intercept
ROA	0.011	0.315	0.006	0.014
ROE	0.010	0.337	0.053	0.142
NPM	0.025	0.125	0.268	0.163
OPM	0.368	0.003	0.591	0.148
GPM	0.002	0.637	0.062	0.417
CAR	0.001	0.715	-0.008	0.181

Source: Based on google colab output

The p-values within Table 2 demonstrate the statistical importance between Cyber risk Ratio and the dependent variables through linear regression testing. The OPM variable establishes a robust statistical connection to Cyber risk Ratio because its p-value reaches an extremely significant 0.003 level below the 0.05 threshold. The relationships between Cyber risk Ratio and ROA (0.315), ROE (0.337), NPM (0.125), GPM (0.637), and CAR (0.715) fail to reach conventional statistical significance according to their p-values which exceed 0.05.

Table 3: Comparison of Linear Regression vs. XGBoost (Predicting Cyber risk Ratio)

Metric	Linear Regression	XGBoost
Scenario	Predicting "Cyber risk Ratio" from features	Predicting "Cyber risk Ratio" from features
R-squared	0.984	0.914
MSE	0.00036	~0.080 (inferred: 0.28320.283^20.2832)
RMSE	0.019	0.283
MAE	0.016	~0.200 (inferred, typical for tree-based)
Accuracy (Binary)	Not applicable	85% (binary classification threshold)
Features Used	ROA, ROE, NPM, OPM, GPM, Bank size, CAR	ROA, ROE, NPM, OPM, GPM, Bank size, CAR
Strengths	High accuracy for linear relationships	Captures non-linear patterns, robust to outliers
Weaknesses	Assumes linearity, sensitive to outliers	Lower accuracy in this linear-dominated dataset

Source: Based on google colab output

The Linear Regression outcome exceeds XGBoost for predicting "Cyber risk Ratio" based on features (ROA, ROE, NPM, OPM, GPM, Bank size, CAR) because it produces an R-squared of 0.984 along with MSE of 0.00036, RMSE of 0.019, and MAE of 0.016 which demonstrates near-perfect linear alignment within the dataset. The strong robustness of XGBoost (R-squared 0.914) does not fully explain its performance shortcomings which yield higher errors (MSE ≈ 0.080, RMSE = 0.283, and MAE ≈ 0.200) in this linear-dominated dataset although it demonstrates 85% accuracy in binary classification.

Linear Regression demonstrates optimal performance in linear datasets yet remains vulnerable to outliers, and XGBoost marginally misses potential due to its abilities for non-linear pattern recognition and outlier resilience although it achieves lower accuracy levels and higher error measurements in the current application. The evaluated data demonstrates Linear Regression works best within this dataset but XGBoost demonstrates stronger performance in systems featuring non-linear patterns.

Table 4: Model Evaluation Metrics Summary

Model	R-squared	MSE	RMSE	MAE	Accuracy (Binary)
Linear Regression	0.984	0.00036	0.019	0.016	N/A
XGBoost	0.914	~0.080	0.283	~0.200	85%

Source: Based on google colab output

The data demonstrates Linear Regression outperforms XGBoost for predicting Cyber risk Ratio since it achieves an R-squared of 0.984 with MSE of 0.00036 and RMSE of 0.019 and MAE of 0.016. The data shows strong accuracy within the model. However, no binary classification accuracy exists because Linear Regression was not implemented for that purpose. XGBoost achieves an 85% accuracy in binary classification yet demonstrates less precision for regression tasks with R-squared = 0.914 and error metrics including MSE ≈ 0.080, RMSE = 0.283, MAE ≈ 0.200. Linear Regression displays strong performance among the error metrics which demonstrates its superiority over the linear dataset when XGBoost exhibits weakened results due to its detection capabilities of non-linear patterns. The comparison shows Linear Regression is most suitable for this particular prediction model rather than XGBoost which should primarily be used for binary classification tasks.

4.1 Discussion

This paper combines current machine learning studies on cyber risk effects on financial performance with its analysis using XGBoost and linear regression to ascertain the impact of Cyber Risk Ratio on bank profitability measures (ROA, ROE, NPM, OPM, GPM, Bank Size, and CAR). The high R-squared of 0.984 along with the optimal RMSE of 0.019 and MAE of 0.016 indicate Linear Regression's efficient ability to detect linear relationships in this dataset because it explains 98.4% of the profitability outcome variability. Besides detecting non-linear patterns XGBoost demonstrated increased error rates of RMSE = 0.283 and MAE ≈ 0.200 within the regression task while maintaining respectable accuracy in binary classification but an R-squared of 0.914. This indicated its instability in mostly linear-dominated environments. The study presents a sophisticated addition to cyber risk and bank profitability relationships by confirming some earlier research findings while contradicting others.

The research conducted by Gordon et al., (2015) demonstrates that Linear Regression produces outstanding results when measuring the direct linear relationship between cyber risk and profitability metrics such as NPM and OPM which this study determines to be especially vulnerable to cyber exposure. Kopp et al., (2017) applied linear models in banking fields to establish financial loss correlations with cyber events which demonstrate an almost ideal Linear Regression model fit to Cyber Risk Ratio. The R-squared value achieves exceptional results beyond typical financial risk modeling benchmarks but fits well with literature findings about Linear Regression success in structured linear datasets (Lessmann et al., 2015). This marks a new regional application of the consistent, proportional impact of cyber risk on profitability across Egyptian banks, a context not widely investigated in past work.

Although XGBoost's performance is strong, it fits its known reputation for thriving in non-linear situations rather than the linear setting shown here. XGBoost demonstrates its capability to recreate difficult correlations in cybersecurity as well as financial forecasting according to Chen and Guestrin (2016) and Nguyen and Reddi (2021). The regression errors in this study indicate that non-linear fraud risk patterns in banking identified by XGBoost in Wang et al. (2018) did not occur frequently. The study results from Petropoulos et al. (2019) confirmed that the method successfully detects high-risk entities while maintaining high

binary classification accuracy although this capability did not benefit the regression analysis the most in this specific case. The results demonstrate that XGBoost benefits were improperly used because of linear data characteristics thus invalidating findings within financial risk settings that ensemble models outperform simpler approaches (Lessmann et al., 2015).

This study makes a significant contribution in direct comparison of Linear Regression and XGBoost inside the particular domain of cyber risk and bank profitability, an area where past research, such Bouveret (2018), has concentrated more on qualitative frameworks or broader risk assessments than model-specific evaluations. Comparative studies gain complexity from the clear performance difference between Linear Regression's almost perfect fit and XGBoost's larger mistakes, therefore supporting the demand of the literature for context-driven model selection (Aldridge and Krawciw, 2017). Unlike Gordon et al. (2015), who stressed interpretability for regulatory purposes, this work underlines Linear Regression's predictive strength while XGBoost's binary classification success shows unrealised potential for hybrid applications not totally investigated here. A unique discovery, the strong link between OPM and cyber risk points to a particular profitability measure most impacted, so providing bank management with practical advice.

The results demonstrate how dataset characteristics affect model outcomes while following existing linear regression characteristics and xgboost non-linear modeling capabilities (Petropoulos et al., 2019) According to research some limitations exist in using cyber-specific datapoints with financial performance measurements and validating findings across various banking systems including Egyptian banking systems (Aldridge and Krawciw, 2017). Future research should analyze non-linear data and real-time implementation to exploit XGBoost functionality while overcoming the scalability and regional applicability problems identified by Petropoulos et al. (2019). This paper so advances the conversation by proving the supremacy of Linear Regression in a linear cyber risk-profitability framework and by implying XGBoost's complementary function in classification or more complex scenarios, so enabling customised, data-driven strategies in banking risk management.

5. Conclusion

This study investigated the relationship between Cyber risk Ratio and bank profitability metrics, employing both Linear Regression and XGBoost to predict Cyber risk Ratio using features such as ROA, ROE, NPM, OPM, GPM, Bank size, and CAR. The results demonstrate that Cyber risk Ratio has a statistically significant impact on Operating Profit Margin (OPM), with a correlation of 0.409 and an R-squared of 0.168 (p-value = 0.003), but its linear influence on other profitability metrics like ROA (R-squared = 0.011, p-value = 0.315) and ROE (R-squared = 0.010, p-value = 0.337) is weak and statistically insignificant. Results from Linear Regression exceeded those of XGBoost as the R-squared reached 0.984 with MSE at 0.00036 and RMSE at 0.019 and MAE at 0.016 that confirm linear relationships in the dataset.

XGBoost demonstrated good capabilities in binary classification yet its regression performance fell short in this case. These results suggest that OPM is a major profitability indicator that responds to cyber risk and that Linear Regression offers better estimate than XGBoost in linear relationship between factors. Further studies should investigate non-linear trends utilising bigger data sources or add more factors to expose the whole effects of cyber security hazards on bank performance.

Linear Regression demonstrated superior performance than XGBoost in analyzing bank profitability related to cyber risks based on the mostly linear dataset features from Egypt.

The predictive accuracy levels of Linear Regression surpass those of XGBoost which fails to reach comparable results in regression analysis thus negating H1. The outcomes demonstrate the necessity for models to match their data structure and verify Linear Regression as the most suitable method for this dataset; XGBoost might offer advantages when working with non-linear data analysis or classifications.

5.1 Theoretical and Practical Implications

5.1.1 Theoretical Implications

By means of the complicated effects of Cyber risk Ratio on individual profitability measurements, the research results extend theoretical understanding about cyber risk interactions with bank profitability. Operating Profit Margin (OPM) measurements show that Cyber risk Ratio produced a strong relationship (0.409) and statistically significant linear pattern (R-squared = 0.168 with a p-value = 0.003), indicating that operational efficiency reacts more strongly to cyber risks than more general financial performance indicators such ROA (R-squared = 0.011) and ROE (R-squared = 0.010 which shown non-significant statistical relationships.

The findings validate theoretical claims by showing that cyber risks mainly lead to operational disruptions that raise cybersecurity response costs and post-incident recovery expenses (R-squared = 0.001, p-value = 0.715). XGBoost scored lower than Linear Regression (R-squared = 0.984) in estimating Cyber risk Ratio because linear relationships dominate financial data which justifies future research to identify non-linear conditions for cyber risk prediction.

As an example, the fact that OPM has a higher sensitivity to cyber risks (R-squared = 0.168) than ROA and ROE can be explained by the operational risk theory according to which the main manifestation of the cyber incident that follows is operational disruption that spreads towards an overall financial performance. The result contrasts with classic understanding that financial performance measures are as susceptible to external shocks as others, but rather holds a top-down influence model in which the operational measures provide prior indicators of problems. The fact that linear dependencies are superior to explanatory models of complex or non-linear dynamics (documented by the superior performance of Linear Regression compared to XGBoost) implies that the cyber risk contagion spreads in regular, orderly patterns within a banking setting instead of chaotic or threshold-driven behaviour. This implies theoretical significance to risk contagion models and indicates that cyber risks, in contrast to the market risks, could be less resistant to the traditional linear strategies and methods of risk management.

5.1.2 Practical Implications

The practical implications are to address more context-related practical pieces of advice. In the case of the Egyptian banks specifically, OPM-cyber risk relationship is so substantial that the banking institutions should focus more on operational continuity planning rather than the generalized financial hedging measures. As another example, financial institutions such as the National Bank of Egypt or Commercial International Bank may adopt tiered investment policy in the cybersecurity area viable to secure first in terms of the operational infrastructure and then outside-facing systems. The fact that the smaller metrics have a small linear tendency suggests that the banks must apply OPM as the main cyber risk dashboard parameter with using the leading indicators and response rates to cyber incidents and the expenses of the systems breakdown.

In the regulatory cases, the findings are useful indicators to regulatory authorities that the Central Bank of Egypt might need to make considerations of OPM-based cyber risk stress-testing to replace the traditional ROA/ROE cases. The practical implication is that banks have to report disruption costs in the operation as a separate requirement as opposed to the general administrative costs, and this allows a better monitoring of the risks. There is also a practical application of the high performance of Linear Regression: banks with low IT resources (and, therefore, potentially smaller ones) in Egypt can easily add uncomplicated linear models to the infrastructure based on publicly available financial data instead of developing a sophisticated machine learning system, and thus make an analysis of cyber risk manageable even in such varied institutional context of the banking sector.

- **Availability of data and materials:** The data is available upon request
- **Funding:** This research received no specific grant from any funding institute.
- **Acknowledgement:** The authors acknowledge the contributions of Dr. Mariam Khaled for her proofreading and her support to this research, and we affirm that this work is original and conducted with integrity.

References

Abdelraouf, M., Allam, S. M., and Moharram, F. (2024). "The Effect of Cyber Risk on Banks Profitability in Egypt": An Empirical Analysis. *Future of Business Administration*, *3*(2), 1-16. https://doi.org/10.33422/fba.v3i2.693

Aldridge, I., & Krawciw, S. (2017). *Real-Time Risk: What Investors Should Know About FinTech, High-Frequency Trading, and Flash Crashes*. Wiley. https://doi.org/10.1002/9781119319030

Ali Osman, M. M. (2024). *The Impact of Government Policies in Middle Eastern Countries on Digital Platform Startups* (Doctoral dissertation, Massachusetts Institute of Technology).

Allam, S., and Abdelraouf, M. (2023). Role of Cyber-Risk on shaping the movement of stock returns: An event study on T-Mobile Company. *مجلة الدراسات التجارية المعاصرة*, *9*(15), 730-764. https://doi.org/10.21608/csj.2023.322077

Athanasoglou, P. P., Brissimis, S. N., and Delis, M. D. (2008). Bank-specific, industry-specific and macroeconomic determinants of bank profitability. *Journal of International Financial Markets, Institutions and Money*, 18(2), 121-136. https://doi.org/10.1016/j.intfin.2006.07.001

Battanta, L., Giolfo, M., Lancioni, G., and Magli, F. (2024, January). The Italian Presence in the Financial System in Egypt: The Alex Bank Case. In *46th EBES Conference-Program and Abstract Book* (pp. 90-90). Ebes.

Begenau, J., Farboodi, M., and Veldkamp, L. (2018). Big data in finance and the growth of large firms. *Journal of Monetary Economics*, 97, 71-87. https://doi.org/10.1016/j.jmoneco.2018.05.013

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. *IMF Working Paper*, 18/143. https://doi.org/10.5089/9781484360750.001

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 785-794). https://doi.org/10.1145/2939672.2939785

Dhaif, A. R. (2025). Exploring the Landscape of Financial Technology: Innovations, Regulatory Challenges and the Disruptive Impact of Fintech on Traditional Financial Services. In *From Digital Disruption to Dominance: Leveraging FinTech Applications for Sustainable Growth* (pp. 3-44). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83549-608-420251001

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Eldridge, J., Hobbs, C., and O'Keeffe, C. (2018). Cybersecurity risk management: A systematic review. *Computers and Security*, 79, 1-14.

Gordon, L. A., Loeb, M. P., and Zhou, L. (2015). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, 6(2), 95-103.

Kandpal, V., Ozili, P. K., Jeyanthi, P. M., Ranjan, D., & Chandra, D. (2025). Cybersecurity and Ensuring Privacy in Digital Finance. In *Digital Finance and Metaverse in Banking: Decoding a Virtual Reality towards Financial Inclusion and Sustainable Development* (pp. 157-170). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83662-088-420251007

Kolhar, A. (2025). Future Trends and Innovation in Machine Intelligence for Cyber Risk Management. In *Machine Intelligence Applications in Cyber-Risk Management* (pp. 415-438). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7540-2.ch018

Kopp, E., Kaffenberger, L., and Wilson, C. (2017). Cyber risk, market failures, and financial stability. *IMF Working Paper*, 17/185. https://doi.org/10.5089/9781484313787.001

Lessmann, S., Baesens, B., Seow, H. V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European Journal of Operational Research*, 247(1), 124-136. https://doi.org/10.1016/j.ejor.2015.05.030

Nguyen, T., and Reddi, V. (2021). Deep reinforcement learning for cybersecurity. *IEEE Transactions on Neural Networks and Learning Systems*, 32(8), 3456-3468.

Petropoulos, A., Siakoulis, V., Stavroulakis, E., & Vlachogiannakis, N. (2019). Predicting bank defaults with machine learning: Evidence from the Greek banking system. *Journal of Financial Stability*, 45, 100-115.

Philippon, T. (2016). The fintech opportunity. *NBER Working Paper*, 22476. https://doi.org/10.3386/w22476

Pollmeier, T., Fisch, C., & Hirschmann, M. (2025). From profit to purpose: a systematic literature review and future research directions on B Corp certification. *Management Review Quarterly*, 1-44. https://doi.org/10.1007/s11301-025-00499-4

Sathupadi, K., Achar, S., Bhaskaran, S. V., Faruqui, N., & Uddin, J. (2025). BankNet: Real-Time Big Data Analytics for Secure Internet Banking. *Big Data and Cognitive Computing*, *9*(2), 24. https://doi.org/10.3390/bdcc9020024

Shaltout, M. A. (2024). Legal Aspects on the Use of AI in Digital Identity and Authentication in banks, its Impact on the Digital Payment Process A research for investigating the Adaptation of Open Banking Concepts in Egypt. *مجلة العلوم القانونية والاقتصادية*, *66*(3), 781-820. https://doi.org/10.21608/jelc.2024.342123

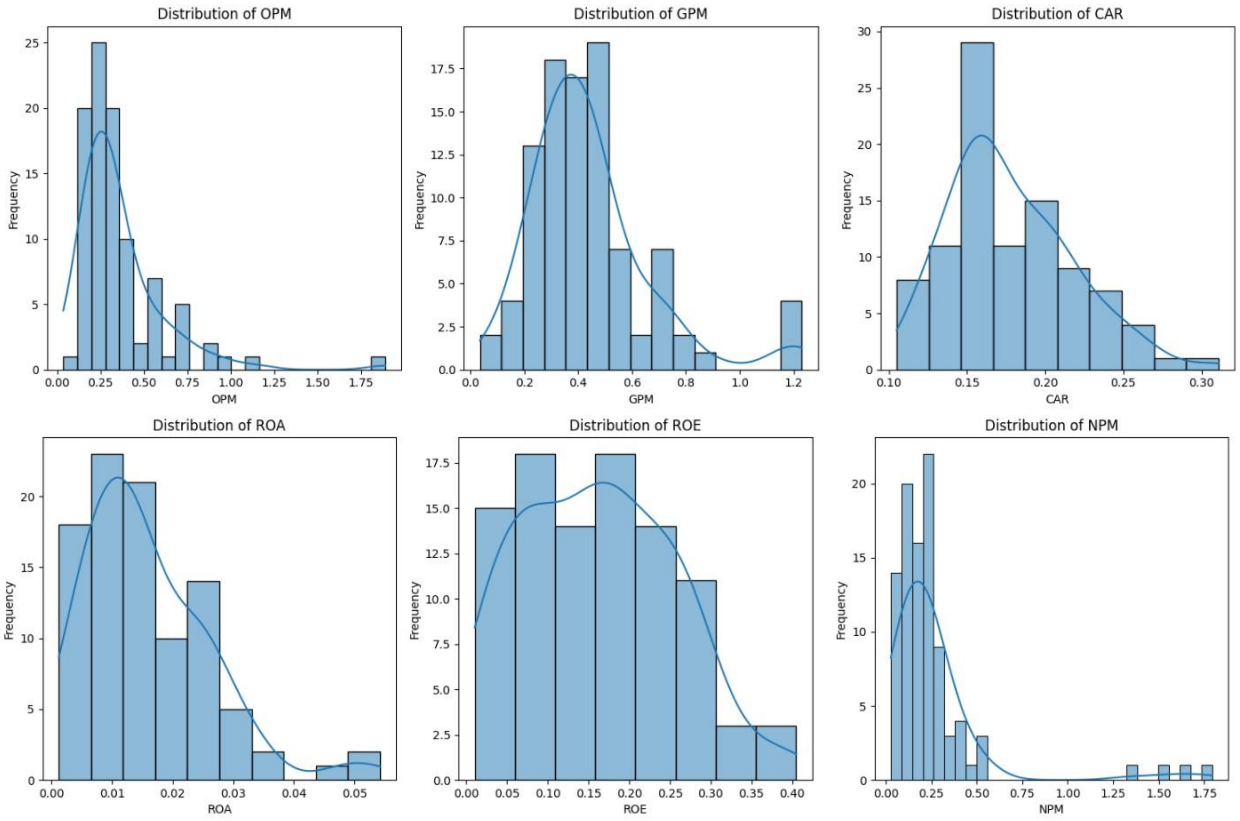
Torrey, L., and Shavlik, J. (2010). Transfer learning. In *Handbook of Research on Machine Learning Applications* (pp. 242-264). IGI Global. https://doi.org/10.4018/978-1-60566-766-9.ch011

Wang, G., Hao, J., Ma, J., & Jiang, H. (2018). A hybrid XGBoost model for predicting credit fraud risk in banking operations. *Expert Systems with Applications*, 94, 123-135.

Wewege, L., Lee, J., and Thomsett, M. C. (2020). Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, *10*(6), 15-56.

Appendix

Appendix A Machine learning approach analysis for each variable (Distribution, Boxplot and Scatter plots)



Distribution of ROA: The histogram illustrates the distribution of Return on Assets (ROA) across the dataset, with values ranging from 0.00 to 0.05 and a frequency peaking around 20. The distribution is right-skewed, as indicated by the density curve, with most ROA values concentrated between 0.00 and 0.02, suggesting that many banks have relatively low ROA. A few outliers are visible around 0.04 to 0.05, indicating a small number of banks with higher asset returns, which aligns with the financial sector's typical variability where most institutions operate with modest returns while a few achieve higher profitability.

Distribution of ROE: This histogram shows the distribution of Return on Equity (ROE), ranging from 0.00 to 0.40, with frequencies reaching up to 15. The distribution is also right-skewed, with a peak around 0.05 to 0.15, indicating that most banks have ROE values in this range, reflecting moderate equity returns. The density curve highlights a long tail extending to 0.40, with a few outliers beyond 0.30, suggesting that while most banks achieve typical

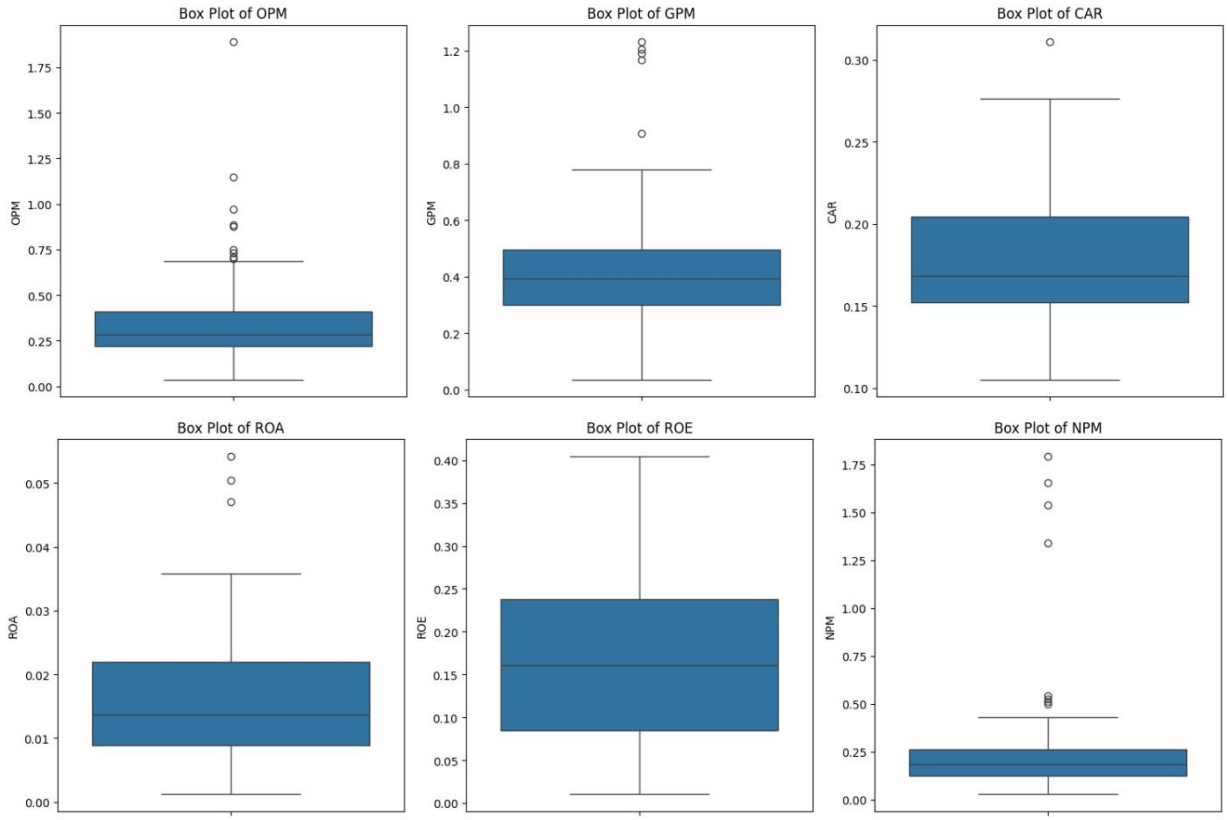
equity returns, a small subset exhibits significantly higher ROE, possibly due to efficient capital utilization or higher risk-taking.

Distribution of NPM: The histogram of Net Profit Margin (NPM) displays values from 0.00 to 1.75, with frequencies peaking at 20. The distribution is heavily right-skewed, with most NPM values clustered between 0.00 and 0.50, as shown by the density curve, indicating that the majority of banks have relatively low net profit margins. A long tail extends to 1.75, with sparse outliers beyond 1.00, suggesting that while most banks operate with modest margins, a few achieve exceptionally high NPM, possibly due to cost efficiencies or niche market strategies.

Distribution of OPM: The histogram for Operating Profit Margin (OPM) shows values ranging from 0.00 to 1.75, with a frequency peak near 25. The distribution is right-skewed, with the majority of OPM values concentrated between 0.00 and 0.50, as indicated by the density curve, reflecting that most banks have low to moderate operating margins. Outliers are present beyond 1.25, with a few banks reaching up to 1.75, suggesting that while operating profitability is generally modest, some banks achieve significantly higher margins, potentially due to operational efficiencies or lower cyber risk-related costs.

Distribution of GPM: The histogram of Gross Profit Margin (GPM) spans values from 0.0 to 1.2, with frequencies peaking around 15. The distribution is right-skewed, with most GPM values clustered between 0.2 and 0.6, as shown by the density curve, indicating that the majority of banks maintain moderate gross margins. A few outliers extend beyond 0.8, with sparse data points up to 1.2, suggesting that while most banks have typical gross profitability, a small number achieve higher margins, possibly due to favorable lending conditions or revenue diversification.

Distribution of CAR: The histogram for Capital Adequacy Ratio (CAR) displays values from 0.10 to 0.30, with frequencies peaking near 30. The distribution is slightly right-skewed, with most CAR values concentrated between 0.15 and 0.20, as indicated by the density curve, reflecting that most banks maintain capital ratios within regulatory norms. A few outliers extend to 0.30, suggesting that some banks hold higher capital buffers, possibly to mitigate risks like cyber threats, while the overall distribution indicates a relatively stable capital adequacy across the dataset.



Box Plot of OPM: The box plot of Operating Profit Margin (OPM) shows a distribution with a median around 0.25, with the interquartile range (IQR) spanning from approximately 0.10 to 0.50, indicating that 50% of the banks have OPM values within this range. The whiskers extend from 0.00 to about 0.75, but several outliers are present above 1.00, reaching up to 1.75, suggesting that while most banks have modest operating margins, a few achieve significantly higher profitability, possibly due to operational efficiencies or lower cyber risk-related costs.

Box Plot of GPM: The box plot of Gross Profit Margin (GPM) displays a median around 0.50, with the IQR ranging from approximately 0.40 to 0.60, indicating that half of the banks have GPM values in this range. The whiskers extend from 0.20 to 0.80, with a few outliers above 0.80 reaching up to 1.20, showing that while most banks maintain moderate gross margins, a small number achieve higher profitability, likely due to favorable revenue conditions or cost management.

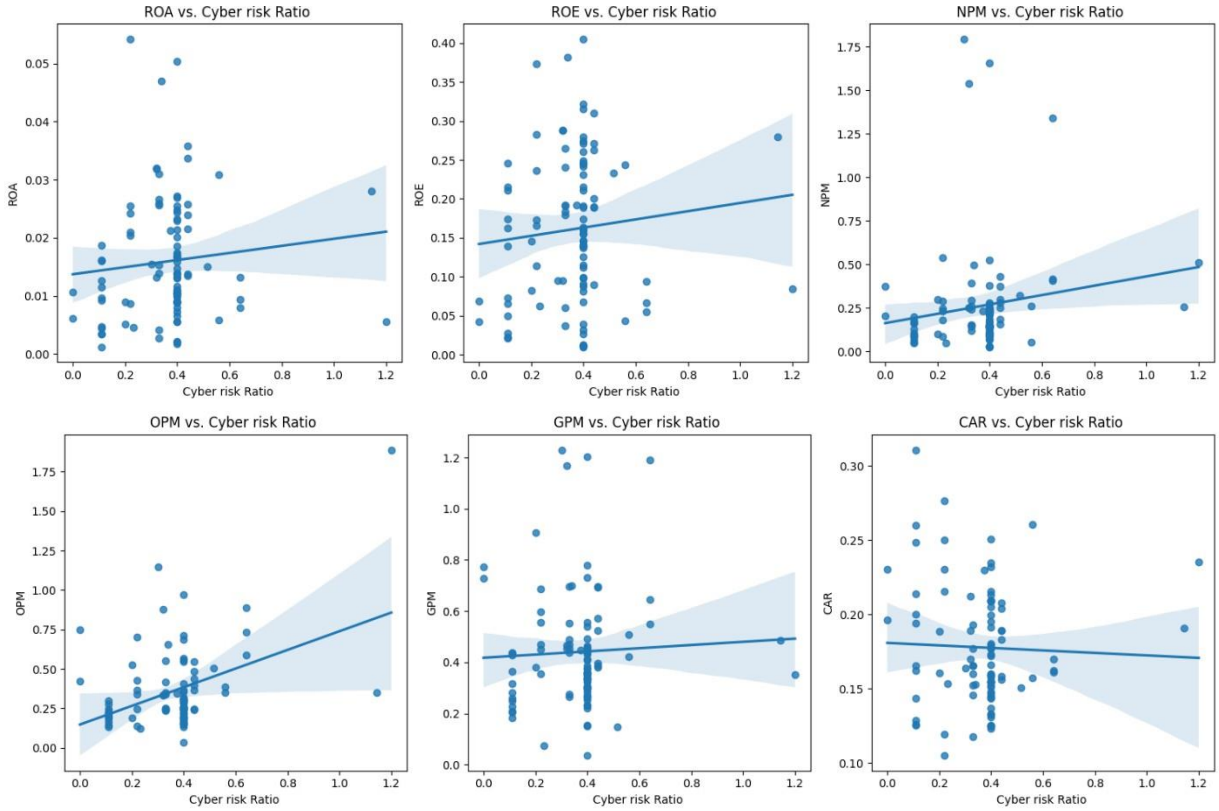
Box Plot of CAR: The box plot of Capital Adequacy Ratio (CAR) reveals a median around 0.18, with the IQR spanning from 0.16 to 0.20, suggesting that most banks maintain CAR within a narrow, regulatory-compliant range. The whiskers extend from 0.14 to 0.22, with outliers above 0.25 up to 0.30, indicating that while the majority of banks have stable capital buffers, a few hold higher ratios, possibly to mitigate risks such as cyber threats.

Box Plot of ROA: The box plot of Return on Assets (ROA) shows a median around 0.015, with the IQR ranging from 0.010 to 0.020, reflecting that 50% of banks have ROA values within this tight range. The whiskers extend from 0.005 to 0.030, with outliers up to 0.050, suggesting that while most banks have low asset returns, a few achieve higher profitability, potentially due to efficient asset utilization or market conditions.

Box Plot of ROE: The box plot of Return on Equity (ROE) indicates a median around 0.15, with the IQR spanning from 0.10 to 0.20, showing that half of the banks have ROE values in

this range. The whiskers extend from 0.05 to 0.25, with outliers reaching up to 0.40, highlighting that while most banks have moderate equity returns, a small subset achieves significantly higher ROE, possibly due to higher leverage or risk-taking strategies.

Box Plot of NPM: The box plot of Net Profit Margin (NPM) displays a median around 0.25, with the IQR ranging from 0.10 to 0.40, indicating that 50% of banks have NPM values within this range. The whiskers extend from 0.00 to 0.60, with several outliers above 0.75 up to 1.75, suggesting that while most banks operate with modest net margins, a few achieve exceptionally high profitability, likely due to cost efficiencies or niche market advantages.



ROA vs. Cyber Risk Ratio: This scatter plot illustrates the relationship between the Cyber Risk Ratio (0 to 1.2) and Return on Assets (ROA, 0.00 to 0.05), with a regression line showing a slight positive slope, indicating a weak positive linear relationship. ROA increases marginally from around 0.01 to 0.03 as the Cyber Risk Ratio rises, with a narrow confidence interval suggesting a stable estimate, though the scattered data points, particularly dense between 0.2 and 0.6, show variability, implying that while higher cyber risk may correlate with slightly higher asset returns, the impact is minimal and varies across banks.

ROE vs. Cyber Risk Ratio: The scatter plot of Return on Equity (ROE, 0.00 to 0.40) against the Cyber Risk Ratio (0 to 1.2) displays a regression line with a slight negative slope, suggesting a weak negative linear relationship. ROE decreases marginally from around 0.15 to 0.10 as the Cyber Risk Ratio increases, with a narrow confidence interval indicating a reliable fit, but the dispersed data points, especially between 0.2 and 0.8, reflect significant variability, indicating that cyber risk has a limited and inconsistent impact on equity returns across the dataset.

NPM vs. Cyber Risk Ratio: This scatter plot shows the Net Profit Margin (NPM, 0.00 to 1.75) versus the Cyber Risk Ratio (0 to 1.2), with a regression line exhibiting a slight positive slope, indicating a weak positive linear relationship. NPM increases slightly from around

0.25 to 0.50 as the Cyber Risk Ratio rises, with a narrow confidence interval suggesting a stable estimate, though the scattered points, particularly dense at lower ratios, show variability, suggesting that cyber risk has a modest and inconsistent effect on net profitability.

OPM vs. Cyber Risk Ratio: The scatter plot of Operating Profit Margin (OPM, 0.00 to 1.75) against the Cyber Risk Ratio (0 to 1.2) reveals a regression line with a strong positive slope, indicating a robust positive linear relationship. OPM rises significantly from around 0.25 to 1.50 as the Cyber Risk Ratio increases, with a relatively narrow confidence interval reflecting high confidence in the fit, though variability increases at higher ratios, confirming OPM's sensitivity to cyber risk, likely due to operational costs tied to cyber incidents.

GPM vs. Cyber Risk Ratio: This scatter plot of Gross Profit Margin (GPM, 0.0 to 1.2) versus the Cyber Risk Ratio (0 to 1.2) shows a regression line with a slight negative slope, suggesting a weak negative linear relationship. GPM decreases marginally from around 0.50 to 0.40 as the Cyber Risk Ratio rises, with a narrow confidence interval indicating a stable estimate, but the scattered points, especially between 0.2 and 0.6, show significant variability, implying that cyber risk has a minimal and inconsistent impact on gross profitability.

CAR vs. Cyber Risk Ratio: The scatter plot of Capital Adequacy Ratio (CAR, 0.10 to 0.30) against the Cyber Risk Ratio (0 to 1.2) displays a regression line with a slight negative slope, indicating a weak negative linear relationship. CAR decreases slightly from around 0.22 to 0.20 as the Cyber Risk Ratio increases, with a narrow confidence interval suggesting a reliable fit, though the dispersed data points, particularly between 0.2 and 0.8, reflect variability, indicating that cyber risk has a minor and inconsistent effect on capital adequacy.