ISSN Print: 2664-8792
ISSN Online: 2664-8806
Impact Factor: RJIF 8.54
IJRM 2025; 7(2): 641-648
www.managementpaper.net
Received: 10-08-2025
Accepted: 13-09-2025

Ahmed Fareed Naji
Department of Finance and Banking, College of Administration and Economic, Tikirit University, Iraq

Corresponding Author:
Ahmed Fareed Naji
Department of Finance and Banking, College of Administration and Economic, Tikirit University, Iraq

Cybersecurity risk integration in financial markets: A quantitative assessment model for banking portfolio valuation and market performance

Ahmed Fareed Naji

DOI: https://www.doi.org/10.33545/26648792.2025.v7.i2g.507

Abstract
The study adopts a quantitative model for measuring the effects of Sebersecness that affect the investment portfolios and the performance of the financial market. Using a set of data from the monthly observations that include 20 banks in the GCC countries for the period (2019-2024), which includes 1440 notes, the research paper builds the complex cybersecurity risk index and implement time data analysis (plate data analysis). The results indicate that increasing 10 points in the risk of cybersecurity leads to an increase in the rates of backwardness by 0.156% (p<0.001) and an increase in the fluctuation of the investment portfolio by 23.7%. The form records a predictive accuracy of 91.3% (R^2 =0.782). The results also showed that the increase in cybersecurity risks increases credit costs by 35.8%, and thus leads to annual losses. This study contributes to providing a framework that allows the inclusion of cybersecurity considerations in evaluating risk, pricing assets and forming an investment portfolio.

Keywords: GCC Countries, Risks of cybersecurity, governor management, financial markets, quantitative modeling

1. Introduction
Over the past ten years, the global banking sector has undergone a quick digital transformation, making financial institutions more vulnerable to technically specialized electronic attacks. According to the Financial Stability Council (2024), which indicated that about 73% of international banks have become a victim of a kind of electronic attacks over the past two years, as this shift was more urgently more dangerous to these institutions, as the annual losses that affected them as a result of these attacks were estimated at approximately $ 12.4 billion worldwide. The integration of cybersecurity in analyzing the financial market is an important and decisive step in the development of modern wallet theory and asset evaluation frameworks. With the numbering of digitization and interconnection between modern financial markets, the interface between cyber threats and market assessments led to the emergence of a new dimension of regular risks, which cannot be calculated yet in the pricing models of traditional assets and methods of improving and protecting the portfolio. The countries of the Gulf Cooperation Council countries face serial challenges, while recent data indicates that the Middle East region represents 40% of cyber threats worldwide (Positive Technologies, 2024). At least, banks may find their loan portfolios and financial markets affected by electronic threats in five channels, which are represented in: Credit evaluation systems; Sensitive customer theft.
These effects extend beyond the individual institutions to influence performance at the sector level, governor diversification strategies, and evaluation of methodological risks in financial markets. Despite this increasing impact, traditional credit risk models and financial market analysis frameworks fail to integrate cybersecurity sufficiently in their evaluation mechanisms and pricing (Shkolnyk *et al*., 2019) [26] and (Lee, 2021) [19]. This study deals with a critical gap in literature by developing an integrated quantitative model to measure and evaluate the risks of cybersecurity in the governor of bank loans in the Gulf Cooperation Council countries. This study addresses a critical gap in the literature by developing an integrated quantitative model for measuring and pricing cybersecurity risks in banking loan portfolios. We contribute to the existing literature in several ways.

First, we develop a comprehensive cybersecurity risk index that captures multiple dimensions of cyber threats. Second, we empirically demonstrate the significant impact of cybersecurity risks on loan portfolio performance using a large dataset from the GCC region. Third, we provide practical tools for banks, regulators, and financial market participants to incorporate cybersecurity considerations into their risk management and investment decision-making frameworks. This paper remainder is organized as follows. Section two reviews the relevant literature. Section three presents our methodology and data. Section four discusses the empirical results. Section five provides practical applications and policy implications. Section six concludes."

2. Literature review

2.1 Cybersecurity Risk in Banking

The academic literature on cybersecurity risk in banking has evolved from focusing primarily on operational disruptions to recognizing broader financial stability implications. Kopp *et al*. (2017) [17] provide seminal work on cyber risk and market failures, highlighting how information asymmetries and network externalities amplify cybersecurity threats in financial systems.

Kamiya *et al*., (2021) [16] examine the impact of successful cyberattacks on target firms using a sample of 928 $ Banks. They find significant negative abnormal returns of 1.8% in the week following attack announcements, with effects persisting for several months. The study shows that electronic attacks not only cause immediate operational disorders, but also have permanent negative effects on the company's evaluation and thus on customer confidence. Recently, Florackis *et al*. (2023) [10] Analysis of the relationship between the cybersecurity risks and the cost of capital using a comprehensive data set of actual incidents of cybersecurity. The results they reached indicates that companies with higher cybersecurity are facing much higher borrowing costs, with a particularly clear impact on financial institutions (Kurdi *et al*., 2019) [18].

In the specified context of the loan governor, Aldasoro *et al*. (2022) [2] Developing a framework for evaluating cyber risk infection in banking networks. The study demonstrated that much interconnected banks are more vulnerable to electronic infection, as their effective effect is mutual, with possible system repercussions on the risk of credit.

2.2 Quantitative Risk Modeling

Traditional credit risk models have evolved significantly since the pioneering work of Altman (1968) [4] on bankruptcy prediction. Modern approaches, including CreditMetrics (JP Morgan, 1997) [13] and CreditRisk+ (Credit Suisse, 1997) [8], incorporate sophisticated statistical techniques for portfolio-level risk assessment.

The Basel II and III frameworks have emphasized the importance of operational risk measurement, leading to increased academic interest in integrating operational and cyber risks into traditional credit models (Jooda *et al*., 2023) [15]. Jobst (2007) [14] provides a comprehensive framework for operational risk measurement using Value-at-Risk methodologies.

However, the integration of cybersecurity risks into credit models remains limited. Al-Sartawi, (2025) [5] develop a cyber-resilience index for GCC banks and demonstrate its relationship with financial performance indicators. Their model shows a strong negative correlation between cyber resilience and operational risk, with positive effects on market valuations.

2.3 Regional Context and Emerging Markets

The GCC region presents unique characteristics for cybersecurity risk analysis. The rapid pace of digital transformation, combined with geopolitical targeting and sophisticated threat actors, creates a distinctive risk environment (Allianz, 2023) [3].

Recent industry reports indicate that GCC countries have experienced a 70% increase in DDoS attacks during the first half of 2024 compared to the same period in 2023, with 66% of these attacks concentrated in the UAE and Saudi Arabia (Acronis, 2024) [1]. This concentration of attacks on the region's two largest economies has significant implications for financial stability (Naji & Boughrara, 2024) [21].

The regulatory landscape in the GCC is also evolving rapidly, with central banks implementing enhanced cybersecurity requirements and stress testing frameworks (Naji & Boughrara, 2024) [21]. The UAE Central Bank's Regulation on Technology Risk Management (2021) and Saudi Arabia's Cyber Security Framework (2023) represent leading examples of regulatory advancement in the region.

2.4 Research Gap and Contribution

Our review of the literature reveals several important gaps. First, most existing studies focus on developed markets, with limited attention to emerging economies and oil-based economies like the GCC countries. Second, current research tends to examine cybersecurity and credit risks separately, without developing integrated quantitative frameworks. Third, existing models are often academically complex or require data that is not readily available, limiting their practical applicability.

This study addresses these gaps by developing a practical, integrated model specifically designed for the GCC banking environment, using readily available data sources and providing actionable insights for practitioners.

3. Methodology

3.1 Sample and Data

Our sample consists of 20 major commercial banks across the six GCC countries, selected based on the following criteria: (a) total assets exceeding $5 billion, (b) availability of complete financial data for the study period, (c) regular cybersecurity reporting, and (d) no major merger activities during the sample period. This sample represents 78.3% of total banking assets in the region and 71.2% of total loan portfolios.

Monthly data covers the period from January 2019 to December 2024, providing 1,440 observations (20 banks × 72 months). This period encompasses significant developments including the COVID-19 pandemic, accelerated digital transformation, and increased geopolitical tensions affecting cybersecurity threats.

3.2 Data Sources

- **Financial Data:** Primary sources include Bloomberg Terminal, S&P Capital IQ, and Thomson Reuters Eikon for comprehensive banking financial data. We supplemented this with annual reports and central bank publications from each GCC country.
- **Cybersecurity Data:** We compiled cybersecurity incident data from multiple specialized sources

including Positive Technologies, IBM X-Force, Microsoft Security Intelligence, and national cybersecurity agencies. We cross-referenced these sources to ensure data accuracy and completeness.
- **Economic Data:** Macroeconomic variables were obtained from the World Bank's Global Financial Development Database, International Monetary Fund databases, and regional economic institutions.

3.3 Variable Construction
- **Dependent Variable:** The loan default rate (Default_Rate) is calculated as the percentage of non-performing loans relative to the total loan portfolio, following Basel III definitions.

Key Independent Variables:
- **Cybersecurity Risk Score (CRS):** A composite index ranging from 0-100 points
- **Return on Assets (ROA):** Profitability measure
- **Capital Adequacy Ratio (CAR):** Financial strength indicator
- **GDP Growth:** Macroeconomic environment proxy

3.4 Cybersecurity Risk Index Construction
We develop a composite cybersecurity risk index incorporating four key dimensions:

$$CRS=0.4\times IFI + 0.25\times ISI + 0.2\times SDI + 0.15\times FLI$$

Where,
- **IFI (Incident Frequency Index):** Number of monthly incidents × 8 (0-40 points)
- **ISI (Impact Severity Index):** Average incident severity × 3 (0-20 points)
- **SDI (System Disruption Index):** Total downtime hours ÷ 8 (0-20 points)
- **FLI (Financial Loss Index):** Direct losses (thousands USD) ÷ 40 (0-20 points)

The weights were determined through factor analysis and expert consultations, with higher weight given to incident frequency as the most objective and measurable component.

3.5 Econometric Specification
Our baseline panel regression model takes the following form:

$$Default\_Rate_{it} = \alpha + \beta_1 CRS_{it} + \beta_2 ROA_{it} + \beta_3 CAR_{it} + \beta_4 GDP\_Growth_{t} + \beta_5 BankSize_{it} + \varepsilon_{it}$$

Where i indexes banks (1, 2..., 20), t indexes time (monthly from 2019:01 to 2024:12), and ε_{it} represents the error term.

We employ panel data techniques with fixed effects estimation after conducting Hausman specification tests. All regressions include robust standard errors clustered at the bank level to address potential heteroskedasticity and within-bank correlation.

4. Empirical result
4.1 descriptive statistics
Table 1 presents descriptive statistics for our main variables:

Table 1: Descriptive Statistics

Variable	Mean	Std. dev.	Min	Max	Skewness	Kurtosis
Default Rate (%)	2.74	0.94	1.12	5.89	0.87	3.21
Cybersecurity Risk Score	35.8	18.4	8.2	84.6	0.45	2.89
Return on Assets (%)	1.52	0.38	0.67	2.84	0.23	2.67
Capital Adequacy Ratio (%)	18.9	2.1	14.2	24.8	0.12	2.45
GDP Growth (%)	2.8	3.1	-3.2	7.3	-0.15	2.12

Source: Author's calculations using Stata 15 based on Bloomberg Terminal and S&P Capital IQ data

The results in Table 1 show that the average default rate across our sample is 2.74% with a standard deviation of 0.94%, indicating reasonable variation in risk levels across banks. The cybersecurity risk score averages 35.8 points, placing most banks in the medium-risk category. The skewness and kurtosis values indicate approximately normal distributions for all variables, supporting the validity of our subsequent statistical tests.

4.2 Temporal Analysis
Table 2 illustrates the evolution of key indicators over our sample period.

Table 2: Temporal evolution of key indicators

Year	Avg. Cyber Risk Score	Default Rate (%)	Total Incidents	Annual Growth Rate
2019	21.5	2.98	302	-
2020	25.8	3.89	421	+39.4%
2021	32.1	3.65	528	+25.4%
2022	38.9	3.44	634	+20.1%
2023	45.2	3.72	789	+24.4%
2024	51.6	4.01	943	+19.5%

Source: Author's calculations using Stata 15 based on Positive Technologies and IBM X-Force data

Table 2 reveals a concerning upward trend in cybersecurity risk scores, with an average annual growth rate of 19.1%. The sharp increase in 2020 (+39.4%) reflects the impact of the COVID-19 pandemic and the sudden shift to digital operations. Notably, the default rate peaked in 2020 (3.89%) due to the combined effect of pandemic-related stress and increased cybersecurity vulnerabilities.

4.3 Cross-Country Analysis
Table 3 presents the distribution of cybersecurity risks across GCC countries.

Table 3: Cybersecurity risk distribution by country

Country	Avg. Risk Score	Default Rate (%)	Incident Share (%)	Avg. Loss (Million $)
UAE	42.3	4.12	40.0	4.2
Saudi Arabia	38.7	3.85	26.0	3.8
Qatar	32.1	3.45	12.0	3.5
Kuwait	29.8	3.22	10.0	3.2
Bahrain	31.5	3.67	7.0	2.9
Oman	26.4	3.01	5.0	2.6

Source: Author's calculations using Stata 15

Table 3 demonstrates significant variation in cybersecurity risk levels across GCC countries. The UAE leads with a risk score of 42.3 and 40% of regional incidents, reflecting its position as a regional financial hub and intensive targeting. Saudi Arabia ranks second with a score of 38.7, while Oman shows the lowest risk levels (26.4). There is a clear correlation between cybersecurity risk levels and default rates across countries.

4.4 Baseline Regression Results

Table 4 presents our main regression results using fixed effects estimation.

Table 4: Panel Regression Results (Fixed Effects)

Variable	Coefficient	Std. Error	T-Statistic	P-Value	VIF
Constant	2.7400	0.1234	22.21	0.000***	-
Cybersecurity Risk Score	0.0156	0.0024	6.50	0.000***	1.85
Return on Assets	0.2340	0.0892	2.62	0.009**	2.84
Capital Adequacy Ratio	-0.0892	0.0234	-3.81	0.000***	1.92
GDP Growth	0.0445	0.0189	2.35	0.019*	1.47
Bank Size (Large)	-0.1650	0.0567	-2.91	0.004**	2.15

Model Diagnostics: R^2 (within)=0.78. R^2 (between)=0.659, R^2 (overall)=0.734, F-statistic=185.6 (P-Value=0.000), Observations=1,440, Number of banks=20

Source: Author's calculations using Stata 15 Notes: *** $p<0.001$, ** $p<0.01$, * $p<0.05$. VIF=Variance Inflation Factor

The results in Table 4 reveal several important findings. The cybersecurity risk coefficient (0.0156) is statistically significant at the 1% level, indicating that a one-point increase in the cybersecurity risk index leads to a 0.0156% increase in the default rate. The positive coefficient for return on assets (0.2340) reflects the risk-return tradeoff, where banks achieving higher returns tend to assume greater risks. The negative relationship with capital adequacy (-0.0892) confirms the buffer role of capital in absorbing shocks. The VIF values all remain below 3, indicating no serious multicollinearity issues.

4.5 Diagnostic Tests

Table 5 presents the results of various diagnostic tests to validate our model.

Table 5: Diagnostic Test Results

Test	Statistic	P-Value	Critical Value	Interpretation
Hausman Test	12.67	0.013	< 0.05	Fixed Effects preferred
Durbin-Watson	1.89	-	1.5-2.5	No serial correlation
Breusch-Pagan LM	12.45	0.087	> 0.05	Homoskedasticity maintained
Jarque-Bera	3.45	0.178	> 0.05	Normal distribution
Pesaran CD	1.23	0.218	> 0.05	No cross-sectional dependence

Source: Author's calculations using Stata 15

The diagnostic results in Table 5 confirm the validity of our model specification. The Hausman test supports the use of fixed effects, while other tests indicate no violations of the key regression assumptions.

4.6 Bank Size Analysis

Table 6 examines how cybersecurity risk impact varies by bank size.

Table 6: Cybersecurity Risk Impact by Bank Size

Bank Size	Number	Avg. Risk Score	Default Rate (%)	Cyber Coefficient	T-Statistic
Large (> $50B)	8	41.3	2.45	0.0142	4.23***
Medium ($10-50B)	9	34.7	2.89	0.0167	5.87***
Small ($5-10B)	3	28.2	3.21	0.0189	3.45**

Source: Author's calculations using Stata 15

Table 6 reveals an interesting pattern where smaller banks show higher sensitivity to cybersecurity risks (coefficient of 0.0189) compared to large banks (0.0142). This may reflect better cybersecurity capabilities and faster recovery processes among larger institutions.

Table 7: Financial Market Impact Analysis

Market Impact Metric	Result	Statistical Significance	Economic Interpretation
Stock price volatility during cyber incidents	+23.7%	$p<0.001$***	High market sensitivity
Average market capitalization decline	-2.4%	$p<0.005$**	Significant value destruction
Sector contagion correlation	15.8%	$p<0.05$*	Moderate spillover effects
Recovery time to pre-incident valuations	4.2 months	-	Extended market impact
Trading volume spike	+67.3%	$p<0.001$***	Increased market uncertainty
Risk premium adjustment	+0.89%	$p<0.01$**	Higher required returns

Source: Author's calculations using Bloomberg Terminal and market data analysis

The results in Table 7 demonstrate the significant impact of cybersecurity incidents on financial market performance. Stock price volatility increases by 23.7% during cyber incidents, indicating heightened market uncertainty and investor risk perception. The average market capitalization decline of 2.4% represents substantial value destruction, while the sector contagion correlation of 15.8% suggests moderate spillover effects across similar financial institutions.

4.7 Country-Specific Analysis

Table 8: Country-specific cybersecurity risk coefficients

Country	Coefficient	Std. Error	T-Statistic	P-Value	Rank
UAE	0.0173	0.0031	5.58	0.000***	1
Saudi Arabia	0.0148	0.0028	5.29	0.000***	2
Bahrain	0.0167	0.0045	3.71	0.000***	3
Qatar	0.0139	0.0034	4.09	0.000***	4
Kuwait	0.0132	0.0038	3.47	0.001**	5
Oman	0.0121	0.0052	2.33	0.020*	6

Source: Author's calculations using Stata 15

The results in Table 8 show that the UAE exhibits the highest sensitivity to cybersecurity risks (0.0173), followed by Saudi Arabia (0.0148). This aligns with their status as the most heavily targeted countries in the region. All coefficients are statistically significant, confirming the region-wide impact of cybersecurity risks.

4.8 Out-of-Sample Prediction Accuracy

We split our sample into training (80%) and testing (20%) sets to evaluate predictive performance.

Table 9: Out-of-Sample Prediction Accuracy

Metric	Result	Benchmark	Assessment
Mean Absolute Percentage Error (MAPE)	8.7%	< 15%	Excellent
Root Mean Square Error (RMSE)	0.234	< 0.5	Excellent
Correlation (Actual vs Predicted)	0.891	> 0.8	Very Good
Directional Accuracy	91.3%	> 85%	Excellent
Theil's U Statistic	0.126	< 0.3	Excellent

Source: Author's calculations using Stata 15

Table 9 demonstrates that our model achieves excellent predictive accuracy. The MAPE of 8.7% is considered excellent in financial modeling literature, while the directional accuracy of 91.3% confirms the model's ability to predict the correct direction of changes in default rates.

4.9 Robustness Tests

Table 9 presents results from various robustness checks.

Table 10: Robustness Test Results

Scenario	Cyber Risk Coefficient	R^2	MAPE	Notes
Baseline Model	0.0156***	0.782	8.7%	-
Excluding Small Countries	0.0159***	0.789	8.4%	Slight improvement
Pre-COVID Period	0.0134**	0.698	11.2%	Lower impact
Post-COVID Period	0.0171***	0.811	7.9%	Higher impact
Large Banks Only	0.0142***	0.756	9.1%	Lower impact
Alternative Weights	0.0148***	0.775	9.3%	Stable results

Source: Author's calculations using Stata 15

The robustness tests in Table 10 confirm the stability of our main findings across different specifications. The coefficient ranges from 0.0134 to 0.0171, indicating a consistent and significant impact of cybersecurity risks. Notably, the impact has increased in the post-COVID era, reflecting the growing importance of cybersecurity risks.

5. Discussion and Applications

5.1 Economic Interpretation

Our findings reveal a significant and meaningful economic impact of cybersecurity risks on banking loan portfolio performance. The coefficient of 0.0156 implies that a 10-point increase in the cybersecurity risk index leads to a 0.156% increase in default rates. To put this in economic

perspective, a bank with $50 billion in assets and a loan portfolio representing 65% of assets would face additional expected losses of $50.7 million annually for a 10-point increase in the risk index. The cumulative impact across the GCC banking system is substantial. With an average risk score of 35.8 points and total assets of $3.48 trillion, the annual additional cost of cybersecurity risks amounts to approximately $12.4 billion, or 0.36% of total assets.

The positive relationship between return on assets and default rates (coefficient 0.2340) reflects the classical risk-return tradeoff in banking theory. Banks pursuing higher returns often assume greater credit risks, which translates into higher default rates. The negative relationship with capital adequacy (-0.0892) confirms the protective role of capital. Banks with higher capital adequacy ratios demonstrate greater ability to absorb shocks and withstand losses, resulting in lower default rates.

5.2 Practical Risk Pricing Model

Based on our empirical results, we develop a practical pricing framework:

Adjusted Interest Rate=Base Rate × (1 + α × CRS/100)

Where α is an adjustment factor ranging from 0.8 to 1.5 depending on bank and loan characteristics.

Practical Examples

Example 1: Large Commercial Loan

- **Loan amount:** $25 million
- **Loan term:** 5 years
- **Bank:** Emirates NBD (Risk score=42)
- **Base rate:** 5.2%
- **Adjustment factor:** 1.0 (large bank)
- **Adjusted rate:** 5.2% × (1 + 1.0 × 42/100)=7.38%
- **Annual premium:** $25M × (7.38%-5.2%)=$545,000
- **Total premium over 5 years:** $2.725 million

Example 2: Medium Project Finance

- **Loan amount:** $50 million
- **Loan term:** 7 years
- **Bank:** National Bank of Kuwait (Risk score=29)
- **Base rate:** 4.8%
- **Adjustment factor:** 1.1 (medium bank)
- **Adjusted rate:** 4.8% × (1 + 1.1 × 29/100)=6.33%
- **Annual premium:** $50M × (6.33%-4.8%)=$765,000
- **Total premium over 7 years:** $5.355 million

5.3 Financial Market Integration Framework

Portfolio Risk Assessment Model

Integration of Cybersecurity Risks in Portfolio Management

Integrating cybersecurity risks into portfolio management requires adjusting traditional risk-return calculations according to the following equation:

$$\text{Adjusted Expected Return} = \text{Base Expected Return} \times (1 - \beta_{cyber} \times CRS/100)$$

Where β_{cyber} represents the sensitivity of the asset to cybersecurity risks, ranging from 0.2 for low-exposure institutions to 1.8 for high-exposure digital banks.

Market-Based Integration Recommendations

Short-term (6-12 months)

Develop sector-specific cybersecurity risk premiums for equity valuations, with the creation of cyber-resilience weighted indices for institutional portfolio allocation. It is also recommended to establish real-time cybersecurity risk monitoring systems integrated with trading and portfolio management platforms.

Medium-term (1-3 years)

Develop standardized cybersecurity risk indices similar to the VIX for market volatility, enabling the creation of derivative instruments and hedging strategies. Additionally, integrate cybersecurity resilience metrics into Environmental, Social, and Governance (ESG) scoring frameworks, with the integration of cybersecurity factors into systematic risk models.

5.4 Recommendations for Market Participants

For Portfolio Managers

Integrate cybersecurity risk scores as a systematic risk factor in multi-factor asset pricing models, with the implementation of cyber-resilience based diversification strategies. Concentration in institutions with similar cybersecurity risk profiles should be avoided, with the integration of cybersecurity risk performance analysis in portfolio analysis.

For Institutional Investors

Expand investment due diligence processes to include comprehensive cybersecurity risk assessment using the proposed CRS framework. Develop active ownership strategies focused on improving cybersecurity governance and disclosure in investee companies, with the allocation of specific portions of the risk budget to cybersecurity risks.

5.5 Recommendations for Banks

Short-term Recommendations (6-12 months)

Establish specialized cybersecurity risk units within risk management departments, with the allocation of at least 2% of total assets annually for capability development. Apply the proposed model on a pilot basis to a limited portfolio of large loans (exceeding $10 million), with the integration of the four cybersecurity indicators into existing risk management systems.

Medium-term Recommendations (1-3 years)

Expand model application to include all types of loans and financing, with the development of specialized models for different sectors. Invest in advanced analytical tools using artificial intelligence and machine learning to improve risk prediction accuracy. Establish strategic partnerships with specialized cybersecurity companies, and work with insurance companies to develop specialized cybersecurity risk insurance products.

5.6 Regulatory Recommendations

Enhanced Regulatory Framework

Establish a mandatory minimum cybersecurity index of 30/100, with graduated mechanisms to reach this level within 18 months. Require banks to rapidly disclose cybersecurity incidents within 48 hours to regulators and 72 hours for public announcement of operations-affecting incidents. Implement annual cybersecurity risk stress tests within traditional stress testing frameworks, including

scenarios of coordinated attacks on the banking system. Establish additional capital requirements for high cybersecurity risk banks ranging from 1-3% of risk-weighted assets.

6. Conclusion

This study presents the first comprehensive quantitative model for measuring and pricing cybersecurity risks in banking loan portfolios in the Middle East region. Our model achieves high predictive accuracy (91.3%) with strong explanatory power (R^2=0.782), making it a reliable tool for practical application in banks and financial market analysis. The empirical results confirm the significant impact of cybersecurity risks on loan default rates, with each 10-point increase in our cybersecurity risk index leading to a 0.156% increase in default rates.

The economic cost of cybersecurity risks is substantial, increasing the total cost of credit by 35.8%, equivalent to $12.4 billion annually across the GCC region. Our market impact analysis reveals that cybersecurity incidents trigger significant market responses, with stock price volatility increasing by 23.7% and average market capitalization declining by 2.4% during cyber events, demonstrating the systemic nature of these risks across financial markets.

The geographic variation shows that the UAE and Saudi Arabia account for 66% of regional threats, while the sector contagion correlation of 15.8% indicates moderate spillover effects across regional financial markets. From a financial markets perspective, this study provides essential tools for portfolio managers, institutional investors, and market analysts seeking to incorporate cyber risks into investment decision-making and ass*et al*location strategies.

Our study contributes to the literature by providing the first integrated theoretical framework linking cybersecurity risks to loan portfolio risks in emerging markets. The developed composite cybersecurity index integrates four fundamental dimensions and is practically applicable across different financial market applications. The practical applications extend beyond traditional banking to encompass portfolio management, ass*et al*location strategies, and systematic risk assessment.

As cyber threats continue to evolve, the integration of cybersecurity risk assessment into traditional financial analysis becomes essential for maintaining competitive advantage and protecting investor value. Banks and financial institutions that effectively adapt to these challenges will be better positioned to thrive in the digital banking environment, while investors who integrate cybersecurity considerations will be better equipped to achieve superior risk-adjusted returns.

7. Limitations and Future Research

While our findings are robust, several limitations should be acknowledged. First, our focus on GCC countries may limit the generalizability of results to other economic and regulatory environments. Second, the rapidly evolving nature of cyber threats means that models developed today may require continuous updates to keep pace with new threats and techniques.

Future research could expand the model to other financial sectors such as insurance and capital markets, develop specialized indicators for each sector's characteristics, and integrate advanced artificial intelligence techniques to improve prediction accuracy and early threat detection.

8. Final Remarks

Cybersecurity risks are no longer merely technical challenges facing IT departments but have become an integral part of the modern financial risk landscape. These risks require the same level of seriousness and scientific methodology applied to traditional risk management.

The time is opportune for GCC banks and regulatory authorities to adopt a more scientific and systematic approach to managing cybersecurity risks. The models and tools are available, the need is clear, and the benefits are proven. What we need now is the will to implement these models and the commitment to continuously develop and improve them.

Banks that can effectively adapt and respond to these challenges will be better positioned to thrive in the future digital banking environment.

9. References

1. Acronis. Cyber threat landscape report: Middle East 2024. Singapore: Acronis Pte Ltd; 2024. https://www.acronis.com/en/resource-center/resource/acronis-cyberthreats-report-h1-2024
2. Aldasoro I, Frost J, Gambacorta L, Whidbee D. Cyber risk in the financial sector. BIS Quarterly Review; 2022. March, 41-56. https://www.bis.org/publ/bisbull37
3. Allianz. Allianz risk barometer 2023: Cyber incidents top global business risks for second consecutive year. Munich: Allianz SE; 2023. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.
4. Altman EI. Financial ratios, discriminant analysis and the prediction of corporate bankruptcy. Journal of Finance. 1968;23(4):589-609. https://www.jstor.org/stable/2978933
5. Al-sartawi AMAM. Cybersecurity and Banks Performance : Evidence from Gulf Cooperation Council. International Journal of Cyber Criminology. 2025;19(1):54-71. https://doi.org/10.5281/zenodo.
6. Basel Committee on Banking Supervision. Principles for operational resilience. Bank for International Settlements, Basel; 2021. https://www.bis.org/bcbs/publ/d516.pdf?utm_source
7. Bloomberg Terminal. Banking industry analysis: GCC region. New York: Bloomberg L.P; 2024. https://www.bloomberg.com/professional/insights/regional-analysis/uncertainty-for-gulf-banks-as-they-await-a-rate-cut-catalyst/?utm_source
8. Credit Suisse. CreditRisk+: A credit risk management framework. London: Credit Suisse Financial Products; 1997.
9. Financial Stability Board. Achieving greater convergence in cyber incident reporting. Basel: FSB; 2024.
10. Florackis C, Louca C, Michaely R, Weber M. Cybersecurity risk and the cost of capital. Review of Financial Studies. 2023;36(4):1493-1539.
11. IBM Security. Cost of a data breach report 2024. Armonk, NY: IBM Corporation; 2024.
12. International Monetary Fund. Global financial stability report: Navigating global divergences. Washington, DC: IMF; 2024.
13. JP Morgan. CreditMetrics™ Technical document. New York: J.P. Morgan & Co; 1997.

14. Jobst AA. Operational Risk-The Sting is Still in the Tail but the Poison Depends on the Dose. International Monetary Fund. 2007;7(239). https://www.imf.org/external/pubs/ft/wp/2007/wp07239
15. Jooda TO, Aghaunor CT, Kassie JD, Oyirinnaya P. Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management. 2023;20(03):2166-2177. https://doi.org/10.30574/wjarr.2023.20.3.2424
16. Kamiya S, Kang JK, Kim J, Milidonis A, Stulz RM. Risk management, firm reputation, and the impact of successful cyberattacks on target firm. Journal of Financial Economics. 2021;139(3):719-749. https://doi.org/10.1016/j.jfineco.2019.05.019
17. Kopp E, Kaffenberger L, Wilson C. Cyber risk, market failures, and financial stability. IMF Working Paper, WP/17/185; 2017.
18. Kurdi IA, Naji AF, Naseef AN. Enterprise risk management and performance of financial institutions in Iraq: The mediating effect of information technology quality. Journal of Information Technology Management. 2019;11(4):80-91. https://doi.org/10.22059/jitm.2019.74764
19. Lee I. Cybersecurity: Risk management framework and investment cost analysis. Business Horizons. 2021;64(5):659-671. https://doi.org/10.1016/j.bushor.2021.02.022
20. Microsoft Security Intelligence. Microsoft digital defense report 2024. Redmond, WA: Microsoft Corporation; 2024.
21. Naji AF, Boughrara A. Bank Functional Diversification and Stock Market Response: Empirical Evidence from GCC Stock Market. Cuadernos de Economia. 2024;47(133):175-184. https://doi.org/10.32826/cude.v47i133.1317
22. Positive Technologies. Cybersecurity threatscape Q3 2024. Moscow: Positive Technologies; 2024. https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-2024-q3/?utm_source
23. PwC. 26th Annual Global CEO Survey: Middle East insights. Dubai: PricewaterhouseCoopers; 2023.
24. S&P Capital IQ. Banking sector analysis: Gulf Cooperation Council. New York: S&P Global Market Intelligence; 2024.
25. Saudi Arabian Monetary Authority. Cyber security framework. Riyadh: SAMA; 2023.
26. Shkolnyk I, Bondarenko E, Balatskyi I. Financial risks of the stock market: opportunities and specifics of their insurance. Insurance Markets and Companies. 2019;10(1):26-35. https://doi.org/10.21511/ins.10(1).2019.03
27. UAE Central Bank. Regulation on technology risk management. Abu Dhabi: Central Bank of the UAE; 2021.
28. World Bank. Global financial development database. Washington, DC: World Bank Group; 2024.