Rieco Hellams

October 5, 2025

Article Review 1

**Impact of Cybersecurity and Bank Performance:**

## Intro

In today's society, the strength of security can help determine the future and current outcomes of an organization. Credibility and dependability are major morals in life, but they are also major in the technology world. Businesses that cannot provide a secure cybersecurity system can record low numbers of clients due to other organizations having a more superior protection system in place. Al-Sartawi talk about cybersecurity and bank performance giving us a view at the possible outcomes of both lack of security and superior security. Sartawi and his article focuses on the period during the pandemic also known as COVID-19.

This journal reflects the core social science principles by analyzing the interaction between human behavior, institutions, and technology. It examines how cybersecurity influence trust within organizations and its customers, governance, and financial stability in banks. The author states that "The research revealed that the banks in the GCC achieved a medium level of cybersecurity during the COVID-19 pandemic and that this level has a positive impact on financial performance, specifically Return on Assets (ROA)."

This quote helps to show the interaction between human behavior, institutions, and technology.

The research question of this journal seemed to be, what level of cybersecurity did GCC-listed banks achieve during COVID-19, and how did it affect their financial performance? The study implies two key hypotheses: first, that higher levels of cybersecurity practices lead to improved financial performance—measured through indicators such as Return on Assets (ROA); and second, that weak or inconsistent cybersecurity mechanisms can negatively affect financial stability, particularly in times of crisis like the pandemic. In this study, the independent variable (IV) is the level of cybersecurity adoption and governance practices implemented by banks, while the dependent variable (DV) is financial performance, measured through metrics such as ROA, profitability, and investor confidence.

The research types used in this journal is empirical method with a literature analysis included as well. The empirical method was used when the researchers collected the ROA or return of assets and the ROE/ return of equity from bank reports and then compared the two against each bank's level of cybersecurity principles and governance mechanisms. The empirical method allowed the researchers to test the relationship between cybersecurity strength and the relationship it has to financial performance. The literature review portion of the study referenced prior research linking cybersecurity governance and regulatory compliance to improved financial resilience, providing a theoretical framework for interpreting the empirical findings.

Next, is the types of data and analysis done within the journal. Multiple types of data were collected, for example the cybersecurity scores/levels from the GCC-listed banks. The data included cybersecurity scores and levels reported by these banks, financial performance indicators such as Return on Assets (ROA) and profitability, and secondary data drawn from international sources like the ITU Global Cybersecurity Index and EY's cybersecurity reports. For analysis, the researchers applied methods like regression analysis to locate correlations between cybersecurity adoption and bank performance. Additionally, they conducted content analysis of global studies on regulation, governance, and cyber risk to provide broader context and reinforce the empirical findings.

This article relates back to the importance of the cybersecurity skills we discussed in our recent PowerPoint. When we look at the skills needed, some of them could help the banks have a stronger cybersecurity system with these skills installed and immediately enforced. Things such as cloud security, network security, and access management all play major roles in cybersecurity and roles in what makes a great company. Based on our PowerPoints and the article/journal we can see the importance of a strong cybersecurity implementation and how it will help banks make more money/ gain more.

Cybersecurity in banking can affect marginalized groups because low-income individuals are more vulnerable to fraud or identity theft because they have fewer resources for recovery of such valuable assets lost. Also, small businesses can suffer because they rely heavily on banks and can lack protection when major breaches occur. Lastly, the elderly was affected. They faced increased cyber fraud during the pandemic,

showing that vulnerable groups suffer heavier consequences of weak cybersecurity systems.

## Conclusion

The study makes significant contributions to society by showing that cybersecurity is not merely a technical issue but also an economic and social concern. It provides evidence that strong cybersecurity practices enhance financial stability, supporting regulatory bodies in developing unified governance frameworks. The research highlights the systemic risks cyberattacks pose to entire economies, particularly during global crises such as COVID-19. Moreover, it encourages banks to invest in resilience, protecting institutions as well as citizens and marginalized groups who rely on stable financial systems, while offering policymakers valuable insights into the need for international collaboration and standardized reporting frameworks.

Reference:

Al-Sartawi, A. M. A. M., Sanad, Z., Shehadeh, M., & Binsaddig, R. (2023). *Cybersecurity and banks performance: Evidence from Gulf Cooperation Council*. *Journal of Financial and Economic Studies, 12*(3), 101–120.