The Impact of Cybersecurity on Bank Performance

[Blank line]

Alex Brown

Old Dominion University

CYSE201S: **Cybersecurity and the Social Sciences**

Diwakar Yalpi

2/24/26

The Impact of Cybersecurity on Bank Performance

In today's increasingly digital world, cybersecurity has become more important than ever. Therefore, cybersecurity has evolved from just protection from viruses to issues that delve into the realm of social sciences. The relationship between cybersecurity and bank performance helps illuminate how institutions manage risk factors, uphold, and maintain public trust. And finally, help ensure and stabilize the ever-evolving economy within the rapidly changing global environment. By reading and reviewing the article, we examine how security measures influence financial outcomes, how they affect marginalized groups, and the challenges alongside them, as this study connects technological protection with broader social, economic, and institutional principles that shape modern society.

Connection to the principles.

The topic of cybersecurity and bank performance relates closely to core principles of the social sciences, particularly economics, sociology, criminology, and political science. This interdisciplinary connection highlights the complex interplay between technological advancements, financial stability, and societal well-being. The economic perspective focuses on the costs and benefits of cybersecurity investments for banks, including the potential for financial losses due to breaches and the returns on investment in security measures. More specially from an economic perspective for any organization its best if they weigh and consider the different options of cybersecurity investments, as it can be the factor between a safe and secure system or potential financial losses associated with cyber breaches and reputational damage (Gordon, Loeb, & Zhou, 2011). The sociological aspect examines how these security measures impact customer trust and the broader societal acceptance of digital banking. Criminology contributes by analyzing the motivations and methods of cybercriminals, informing the development of

preventative strategies. And political science offers insights into the regulatory frameworks and international cooperation necessary to combat cyber threats effectively.

Study Overview: Research Question, Variables, and Methods

The article titled Cybersecurity and Banks Performance: Evidence from Gulf Cooperation Council Countries" takes and examines whether cybersecurity performances influence bank operations within the GCC or *Gulf Cooperation Council. * With the main research question being about investigating the bond between cybersecurity and bank performance and they affect each other. This question in turn preposes the hypothesis that if stronger and more reliable cybersecurity systems and performance positively effects bank performance? Within this study, the Dependent variable recognized would be the bank's financial performance. Therefore, the independent variable in this study is cybersecurity performance. The methodology used in this study is a quantitative approach, employing panel data regression analysis along with detailed statistics. The data collected spans from 2010 to 2020, covering 10 years of financial and cybersecurity metrics for banks across the GCC region. This is used to more accurately collect and track the performance of both while controlling other influencing factors.

Impact on Marginalized and Vulnerable Populations

The topic and relation between cybersecurity and bank performance relates to the challenges, concerns, and contributions of marginalized groups in several important ways. Firstly, cybersecurity threats disproportionately affect these communities. The lack of access to resources and education makes them more vulnerable (Leukfeldt & Yar, 2016). This can lead to greater financial losses and reputational damage for banks that serve them. Furthermore, the

underrepresentation of marginalized groups in the cybersecurity field means that their unique perspectives and experiences are often overlooked when developing security protocols and strategies. This can lead to solutions that aren't inclusive or effective for everyone. Secondly, concerns of the lack of security for marginalized groups can also lead to a lack of trust in financial institutions. This can impact customer retention and acquisition of banks. This lack of inclusion can also hinder innovation within the cybersecurity sector itself. When diverse voices are not part of the conversation, new ideas and approaches may be missed. This can lead to a narrower perspective and potentially less innovative solutions. Therefore, researching and examining the relationship between cybersecurity and bank performance is crucial for understanding the full impact of these digital transformations. As it also highlights the social impact it has on communities along with how institutional cybersecurity efforts can protect vulnerable populations while also strengthening overall financial stability.

Course Concepts that relate to the Article

Concepts from the PowerPoint presentation that relate to the article are the concept of empiricism and the scientific method. Empiricism is the idea that knowledge comes from sensory experience, and the scientific method is a systematic approach to acquiring knowledge through observation and experimentation. Therefore, as we see that data is based on observed and measured data, rather than theory which lines up with empirical research study methods. In addition, the use of the methods used to gather data on banks' annual reports, financial statements, and cybersecurity disclosures also describes the concept of Archival research. This research type would provide the utmost accurate data for the research.

Conclusion

In conclusion, this article demonstrates how robust cybersecurity measures are essential for maintaining strong bank performance, safeguarding both financial interests, and fulfilling social responsibilities. Detailing with various research methods such as empirical data and archival data. Or with social sciences such as economics, sociology, criminology, and political science. Through these artifacts, we see how the study demonstrates the direct impact value that cybersecurity has on banks in the GCC region. Not only does the study highlight the value and effectiveness of the relation between the two, but it also highlights the social implications it has on marginalized groups. As they offer a large voice, which should be considered and heard, as the security of their data, especially when it comes to banks, should never be overlooked.

Additionally, as said before, the study analyzes and illustrates the application of core principles. Therefore, it helps connect to real-life practices that numerous organizations use. As the banking sector continues to evolve in a digital era, the integration of effective cybersecurity practices will remain a cornerstone of trust and success. Banks that proactively invest in cybersecurity not only protect their assets and customers but also build a reputation for reliability and resilience. Ultimately, prioritizing cybersecurity is not just a technical necessity but a strategic imperative that empowers banks to thrive amid emerging challenges and future opportunities.

References

Al-Sartawi, A. (2025). ***Cybersecurity and banks performance: Evidence from Gulf Cooperation Council. Cybercrime Journal, Volume ?,*** **Article 444/132.** **https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/444/132**

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Toahchoodee, M., & Ray, I. (2011). On the formalization and analysis of a spatio-temporal role-based access control model. *Journal of Computer Security*, *19*(3), 399–452. https://doi.org/10.3233/jcs-2010-0418