Jurnal Pendidikan Akuntansi dan Keuangan

Journal homepage: https://ejournal.upi.edu/index.php/JPAK

Analysis of The Level of Cybersecurity Disclosure on Social Media on Bank Financial Performance (Case Study on Banks in Uzbekistan)

Shahzod Sherzod Norkulov [1], R Nelly Nur Apandi[2], Arim Nasim[3], Sardor Umarovich Kholdorov [4]*

[1]Double Degree Student of UPI-TSUE, Indonesia-Uzbekistan
[23]Faculty of Economics and Business Education,Universitas Pendidikan Indonesia, Indonesia
[4]Economics and Management Department, Tashkent State Economic University, Uzbekistan
Correspondence E-mail: nelly.nna@upi.edu

ABSTRACT

This study aims to determine the correlation between cybersecurity disclosure on social media and financial performance. This research uses a descriptive quantitative method using correlation analysis of 18 banks in Uzbekistan. This study cannot prove the correlation between cybersecurity disclosure and bank financial performance. This study has not been able to provide empirical evidence that the more information provided to customers about cybersecurity will increase customer trust in the security and convenience of transacting at the bank. This study has not been able to prove that non-financial bank information can be a signal for banks so that it can be responded to properly to assess bank performance. Empirically, this study can provide an overview of the existing conditions of cybersecurity disclosure that banks can improve. *Novelty* Researchers analyzed cybersecurity on social media carried out at banks in Uzbekistan.

ARTICLE INFO

Article History:
Submitted/Received 27 May 2025
First Revised 15 May 2025
Accepted 10 June 2025
First Available online 31 July 2025
Publication Date 31 July 2025

Keyword:
Disclosure, Cybersecurity, Social Media, Profit, Bank, Uzbekistan.

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print)

1. INTRODUCTION

The rapid advancement of technology has significantly transformed society, enhanced convenience, and streamlined business operations. Innovations such as artificial intelligence (AI), cloud computing, and data analytics have optimized efficiency and decision-making across various industries (Forman, 2024). However, this increasing reliance on digital solutions has also contributed to the rise of cybercrime, where criminals exploit vulnerabilities to manipulate and infiltrate confidential data, causing financial losses and reputational damage (Halal, 2023). The emergence of Cybercrime-as-a-Service (CaaS) has further exacerbated the situation, allowing individuals with limited technical expertise to carry out sophisticated attacks (HKCERT, 2023). In financial services, the balance between convenience and security remains challenging, as stringent security measures can deter users, while lax protocols expose them to cyber threats (Jara, 2022). As technology continues to evolve, understanding the interplay between digital convenience and cybercrime is crucial for developing effective security strategies in an increasingly digital world.

Economic globalization has intensified competition across all sectors, including banking. Banks must prioritize customer satisfaction in this highly competitive environment, as it significantly impacts their performance and profitability. High-quality banking services have been positively correlated with increased customer satisfaction, which fosters loyalty and enhances financial performance (Alallq, 2024). Furthermore, effective market segmentation strategies allow banks to meet the diverse needs of their clients better, improving satisfaction and competitive positioning (Osei et al., 2021). The development and diversification of banking products and services are crucial drivers of competitiveness, allowing banks to adapt to evolving customer preferences and maintain a strong market presence (Chocholáková et al., 2015). Therefore, securing customer satisfaction through service quality, targeted market strategies, and innovative offerings is essential for banks to enhance their performance and sustain a competitive edge.

Effective communication of a bank's cyber security measures is essential for building and maintaining customer trust. Transparent disclosure of strategies to mitigate cyber threats demonstrates a bank's commitment to safeguarding client assets and addresses growing customer concerns about data security. Research has shown that customer awareness of cyberattacks can negatively affect their trust and commitment to online banking services, highlighting the importance of proactive communication regarding cyber security initiatives (Bajwa et al., 2023). Studies also indicate that the specificity and verifiability of cybersecurity disclosures significantly influence stakeholder intentions, with detailed and credible information fostering greater trust (Bansal & Axelton, 2023). By openly sharing their cybersecurity practices, banks can enhance transparency, reduce information asymmetry, and strengthen customer confidence in their ability to protect sensitive data.

In the contemporary banking sector, institutions with robust cybersecurity capabilities often disclose their preventive measures to enhance customer trust. Transparent communication about cybersecurity practices can significantly bolster consumer confidence and loyalty (Panditharathna et al., 2024). Social media platforms have become effective

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print)

channels for such disclosures, enabling banks to reach a broad audience interactively. By leveraging these platforms, banks can disseminate information about their security protocols, educate customers on safe banking practices, and address concerns promptly, thereby strengthening customer relationships (Mgiba & Mxotwa, 2024).

Generation Z, typically born between 1997 and 2010, is characterized by its deep integration with digital technologies and social media. This cohort frequently uses social media for interaction and as a primary source of financial information, including banking content. Studies indicate that Millennials and Generation Z increasingly turn to social media for personal finance, such as making payments, crowdfunding, and shopping (Kansas City Federal Reserve, 2023). Moreover, these generations often rely on social media platforms for financial education and advice, underlining these digital channels' significant role in shaping their financial behaviors (Kansas City Federal Reserve, 2023). Consequently, social media has become a crucial platform for banks aiming to engage with Generation Z, disseminate information, and foster trust with this digitally native audience.

Social media platforms, such as Instagram, Facebook, and Telegram, play a pivotal role in information dissemination worldwide. In Uzbekistan, a developing country embracing public information flow, Telegram is the most popular platform, with approximately 18 million users. While less widely adopted, Instagram maintains a significant presence, with around 3.7 million users, offering unique advantages like a visually engaging interface and robust tools for brand promotion. Given the popularity of these platforms, especially Telegram, it is imperative to conduct comprehensive studies on cybersecurity disclosures within Uzbekistan’s social media landscape to protect user data and maintain public trust (Bright Uzbekistan, 2024).

The relationship between cybersecurity disclosure and performance can be interpreted from the signaling theory perspective. According to this theory, voluntary disclosure by firms, including financial institutions, about their cybersecurity measures and actions provides signals to the market about how organizations manage their cyber risks and how they engage in mitigating and detecting their security breaches (Berkman H, Jona J, Lee G, Soderstrom N 2018) These information or signals allow investors to assess the risk management and reduce the uncertainty regarding the organization’s future cash flow, encouraging investors to make informed investment decisions in these banks or firms, which consequently affect their performance (Khlif H, Hussainey K 2016) and valuation (Berkman H, Jona J, Lee G, Soderstrom N (2018), Gordon LA, Loeb MP, Sohail T 2010). In addition, more up-to-date information regarding cybersecurity procedures in which banks disclose can signal more security against cyber risks and crimes and a lower probability of the theft of confidential information. This helps to convey trust to stakeholders and thus enhances the bank’s performance.

Previous research has shown a significant negative impact of cyberattacks on bank profitability. Erkan-Barlow et al. (2023) analyzed 120 data breaches across U.S. commercial banks. They found that cyberattacks adversely affect profitability, with more pronounced effects over the 12 quarters following a breach, particularly from non-hack breaches. Larger

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print

and private banks experienced more substantial impacts than smaller and public banks, facing decreased deposits and loans, and increased liquidity, contributing to reduced profitability.

While much research has explored cybersecurity disclosures and their effect on bank performance in developed countries, there is a notable lack of studies focusing on developing nations like Uzbekistan, a former Soviet republic. For instance, research in Bangladesh indicates that board composition significantly influences voluntary cybersecurity disclosures within the banking sector (Mazumder & Hossain, 2023). Similarly, studies in the MENA region highlight the positive effect of cybersecurity disclosures on bank performance, with corporate governance mechanisms such as a Chief Risk Officer (CRO) moderating the relationship (Elsayed, Ismail, & Ahmed, 2024). However, research specific to Uzbekistan's banking sector remains limited. Bekbaev and Yalgasheva (2022) discussed information security within Uzbekistan's financial system but did not explore the impact of cybersecurity disclosures on bank performance. This study aims to bridge this gap by examining the relationship between cybersecurity disclosures and banking performance in Uzbekistan, considering its unique historical and socio-economic context.

2. METHODS

This research investigates the relationship between cybersecurity disclosure on social media and bank financial performance. Specifically, the study seeks to determine how banks' disclosures of cybersecurity events or security-related issues on social media platforms influence their economic outcomes, such as customer trust, reputation, market performance, and stock value. This research's independent variable (X) is cybersecurity disclosure on social media. This includes how banks communicate about cybersecurity issues such as data breaches, vulnerabilities, and security improvements through social media channels.

These disclosures can be public posts, statements, or responses to cybersecurity incidents. To describe cybersecurity disclosure on social media, the data will come from posts on the website, and Telegram in 2023. The dependent variable (Y) is bank financial performance. This refers to the economic indicators and outcomes that may be influenced by how cybersecurity issues are disclosed, such as Stock price changes, Customer retention, acquisition rates, Profit margins, Revenue, or loss linked to customer trust and behavior. The data will come from a financial report to describe the bank's financial performance.

Table 1. Operationalisation Variable

Variable	Indicators	Scale
Cybersecurity Disclosure on Social Media	Number of posting from Website and Telegram related to cybersecurity	Ratio
Financial Performance	Logaritma Natural Profit	Ratio

The population for this research consists of banks that have actively used social media platforms to disclose cybersecurity-related information. The sampling technique used in this research will be purposive sampling. The sample will be a subset of the population, consisting of 18 banks that have had cybersecurity incidents and have made disclosures on social media.

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print)

These banks will be selected based on their active social media presence, availability of data related to cybersecurity disclosures, and financial performance over the relevant period. This study uses a quantitative descriptive method. Data were analyzed using the Pearson correlation test.

3. RESULTS AND DISCUSSION

Descriptive Statistic

This study aims to determine the relationship between the level of disclosure regarding cybersecurity on social media and bank financial performance. This study was conducted on 18 banks in Uzbekistan. The samples are as follows:

Table 2.Sample Research

No	Bank	No	Bank
1	NBU	10	aloqa bank
2	SQB	11	davr bank
3	ANOR	12	ziraat bank
4	XALQ BANKI	13	asaka bank
5	SILK WAY BANK	14	universal bank
6	TBC BANK	15	mikrokredit bank
7	ASIA ALLIANCE	16	agrobank
8	TENGE BANK	17	orient finance bank
9	Hamkorbank	18	poytaxt bank

Of the 18 banks, nine are listed on the Tashkent Stock Exchange, and the remaining nine are not listed. Seven of the 18 banks are state-owned, while the remaining 11 are private banks.

Table 3.Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
CYBERSECURITY_DISC	18	2.00	40.00	13.4444	10.12988
FINANCIAL_PERFORMANCE	18	58336.00	471221414.00	45890348.0556	130061355.17811
Valid N (listwise)	18				

Based on Table 3, a general overview of the data is obtained. In the disclosure of cybersecurity on social media in the research sample, the smallest was two posts, and the largest was 40. The average post for the entire sample was 13 posts related to cybersecurity in this study. NBU Bank made most posts about cybersecurity. At the same time, the average profit generated by the Bank in the sample was 45890348 (in millions). The maximum profit amount was 471221414 generated by Microcredit Bank. The minimum profit amount was 58336. Various media are used to make disclosures on social media. In this study, two social media were used, namely those from the company website and Telegram. The use of social media is very high in Uzbekistan. Therefore, this study will explore further the disclosure of both. Based on Table 4, it is obtained that the number of disclosures on Telegram reached 152 posts during 2023, while there were fewer posts on the website, only 90. Based on this,

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print

it is proven that the delivery of public information carried out by banks is more updated on social media in the form of Telegram than on websites.

Table 4. Cybersecurity Disclosure

Website	Telegram
90	152

This study further explores keywords that are more frequently expressed on social media. The following are common topics used to express cybersecurity:

Figure 1. Cybersecurity Disclosure

Cybersecurity is a practice or action taken to protect systems, data, networks, programs, and devices from cyber attacks. These attacks usually aim to access, modify, steal sensitive information, extort money, and disrupt company operations. Based on the results of data analysis using word clouds, the themes depicted in Figure 1 were obtained. The themes that appeared more frequently were related to the command to check the official website regularly and change the PIN regularly. Another thing that was expressed was more about being careful not to provide bank identity and click the link shown without analysis first.

Table 5. Correlations

		CYBERSECURITY_DISC	FINANCIAL_PERFORMANCE
CYBERSECURITY_DISC	Pearson Correlation	1	-.028
	Sig. (2-tailed)		.911
	N	18	18
FINANCIAL_PERFORMANCE	Pearson Correlation	-.028	1
	Sig. (2-tailed)	.911	
	N	18	18

This study used 18 banks in Uzbekistan to examine the relationship between cybersecurity disclosure and financial performance. The results of the study showed that the sig value (2 2-tailed) reached 0.911, which is higher than the alpha value, so that the research hypothesis cannot prove the relationship between the two.

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print)

Level of Cybersecurity Disclosure on Social Media on Bank Financial Performance

Financial and non-financial information is important information as a process of corporate management accountability to the company owner. In the banking industry, digital security is a major issue that can drive customer loyalty levels. To increase this loyalty, the bank needs to provide information about company activities to prevent attacks in the digital world in banking. Based on cybersecurity disclosure data in social media collected from 18 Banks in Uzbekistan, it can be mapped that the disclosures include:

1. Always check the official page address; The bank provides information that customers must regularly check the banking applications they use. This is to anticipate the possibility that customers will not be aware of cybercrime if checks are not carried out regularly.Do not disclose bank card details.
2. Do not click on the link shown; Often, scammers do their actions by sending fake links that shorten URL services such as bit.ly or tinyurl to hide the actual link. Cybercriminals often do Account Login Phishing, which tries to steal login information by creating fake pages that look like popular sites.
3. Scammers By Doing Psychological Fraud, Cybercriminals use social engineering techniques to trick victims into clicking on certain seemingly trustworthy links. These links are often designed to steal personal information like login details, passwords, or even financial data. Therefore, people must recognize fake links and avoid potentially harmful traps.
4. Scammers are actively working, introducing themselves as system security officers. The large number of internet users has increased the number of targets for scamming. There are perpetrators who have targeted victims who are considered to have a lot of money, but there are also those who randomly choose victims to be deceived.
5. Our promotional posts involve posting logos to instill trust in Customers. They will also engage in Catfishing, Auction Fraud, and Donation scams.
6. Using special technology, fraudulently collecting customer data. Cybercriminals often engage in phishing, a scam that deceives victims by exploiting their data and information. This information can be obtained from email, text messages, telephone, or links.
7. If you find any suspicious activity on your bank account or card, please contact us immediately.
8. Temporarily disabled & preventive maintenance.Banking will carry out maintenance on an ongoing basis.
9. Bank Application & Teknologi SoftPOS. The bank will introduce new or additional applications to increase the added value of banking products.
10. 3d secure. 3DS stands for Three-Domain Secure. When someone wants to transact on an online shopping site and uses a credit/debit card, the system will ask for an OTP or one-time password. OTP is usually sent to the cardholder mobile phone number or via email. So that only the cardholder concerned can know the OTP code. Many hacking modes can be prevented when you use 3d Secure, especially online credit card data

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print

theft. The most common mode for hackers to steal this information is by phishing. This method is done by directing the victim to a link similar to a popular site.

After knowing the main themes on social media regarding cybersecurity, a correlation analysis was conducted between cybersecurity disclosures on social media and company performance in the same year. Table 5 shows that the Sig. (2-tailed) value is greater than the ά value (0.05), which is 0.911, meaning there is no correlation between the two variables. The higher level of disclosure regarding cybersecurity does not correlate with increased company profits due to increased customer loyalty. This is not in line with previous research, which has shown a significant negative impact of cyberattacks on bank profitability. Erkan-Barlow et al. (2023) analyzed 120 data breaches across U.S. commercial banks. They found that cyberattacks adversely affect profitability, with more pronounced effects over the 12 quarters following a breach, particularly from non-hack breaches. The lack of correlation can be attributed to the amount of bank information in social media that has not been widely used in Uzbekistan. This is evident from the fact that there are still not many financial publications on banking performance, let alone non-financial information such as cybersecurity disclosures, which are considered important additional information.

4. CONCLUSION

This study cannot prove the correlation between cybersecurity disclosure and bank financial performance. This study has not been able to provide empirical evidence that the more information provided to customers about cybersecurity will increase customer trust in the security and convenience of transacting at the bank. Therefore, this convenience will increase customer loyalty in transactions that benefit the bank. In the short term, it will increase bank profits. This study has limitations because it only looks at the impact of disclosure on profit achievement in the current year, even though this increase can begin to be achieved after information is submitted with a certain time lag. Another limitation is that the number of banks that provide complete information is still limited. Therefore, further researchers can use the value of performance achievement in the following year and data from several Central Asian countries to prevent data limitations.

5. REFERENCES

Forman, C. (2024). Research: Technology Is Changing How Companies Do Business. *Cornell SC Johnson College of Business*. Retrieved from https://business.cornell.edu/hub/2024/05/16/research-technology-is-changing-how-companies-do-business/

Halal, W. E. (2023). Forecasting the digital revolution and its impacts. *Technological Forecasting and Social Change*. Retrieved from https://en.wikipedia.org/wiki/William_Halal

HKCERT. (2023). Unmasking Cybercrime-as-a-Service: The Dark Side of Digital Convenience. *Hong Kong Computer Emergency Response Team*. Retrieved from

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print)

https://www.hkcert.org/blog/unmasking-cybercrime-as-a-service-the-dark-side-of-digital-convenience

Jara, A. (2022). Convenience or safety? The key to tackling financial cybercrime. *Iupana*. Retrieved from https://iupana.com/2022/04/11/convenience-or-safety-the-key-to-tackling-financial-cybercrime/?lang=en

Alallq, H. A. E. (2024). The Impact of Quality of Banking Services on Customer Satisfaction in Small and Medium Banks. *South Asian Journal of Social Sciences and Humanities*, 5(2), 39-55. https://doi.org/10.48165/sajssh.2024.5203

Osei, F., Ampomah, G., Kankam-Kwarteng, C., Bediako, D. O., & Mensah, R. (2021). Customer Satisfaction Analysis of Banks: The Role of Market Segmentation. *Science Journal of Business and Management*, 9(2), 126-138. https://doi.org/10.11648/j.sjbm.20210902.19

Chocholáková, A., Gabcová, L., Belás, J., & Sipko, J. (2015). Bank Customers' Satisfaction, Customers' Loyalty and Additional Purchases of Banking Products and Services. *Economics & Sociology*, 8(3), 82-94. https://doi.org/10.14254/2071-789X.2015/8-3/6

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. *Information and Computer Security*, 31(5), 635-654. https://doi.org/10.1108/ICS-11-2022-0179

Bansal, G., & Axelton, Z. (2023). Impact of Cybersecurity Disclosures on Stakeholder Intentions. *Journal of Computer Information Systems*, 64(1), 78-91. https://doi.org/10.1080/08874417.2023.2180785

Mgiba, N., & Mxotwa, N. (2024). Communicating Banking Cyber-security Measures, Customer Ethical Concerns, Experience, and Loyalty Intentions: A Developing Economy's Perspective. *International Review of Management and Marketing*, 14(3), 125-135.

Panditharathna, R., Liu, Y., de Macedo Bergamo, F. V., Appiah, D., Trim, P. R. J., & Lee, Y.-I. (2024). How Cyber Security Enhances Trust and Commitment to Customer Retention: The Mediating Role of Robotic Service Quality. *Big Data and Cognitive Computing*, 8(11), 165. https://doi.org/10.3390/bdcc8110165

Kansas City Federal Reserve. (2023). Social Media for Personal Finances: A New Trend for Millennials and Gen Z. *Kansas City Federal Reserve.*

Bright Uzbekistan. (2024). *Most prevalent social sites in Uzbekistan.* Retrieved from https://brightuzbekistan.uz/en/most-prevalent-social-sites-in-uzbekistan/

Erkan-Barlow, A., Ngo, T., Goel, R., & Streeter, D. W. (2023). An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States. *Journal of Global Business Insights*, 8(2), 120-135. https://doi.org/10.5038/2640-6489.8.2.1246

Bekbaev, G. A., & Yalgasheva, S. U. (2022). Information Security in the Financial and Banking System of the Republic of Uzbekistan. *Central Asian Journal of Mathematical Theory and Computer Sciences*, 3(2), 1-4. Retrieved from https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS/article/view/149

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, 10, 115. https://doi.org/10.1186/s43093-024-00402-9

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print

Mazumder, M., & Hossain, D. M. (2023). Voluntary cybersecurity disclosure in the banking industry of Bangladesh: Does board composition matter? *Journal of Accounting in Emerging Economies*, 13(2), 217-239. https://doi.org/10.1108/JAEE-07-2021-0237

Berkman H, Jona J, Lee G, Soderstrom N (2018) Cybersecurity awareness and market valuations. *J Account Public Policy* 37(6):508–526

Gordon LA, Loeb MP, Sohail T (2010) Market value of voluntary disclosures concerning information security. *Manag Inf Syst Q* 34(3):567–594

Khlif H, Hussainey K (2016) The association between risk disclosure and firm characteristics: a meta-analysis. *J Risk Res* 19(2):181–211. https://www.ibm.com/think/topics/cybersecurity

DOI: https://doi.org/10.17509/jpak.v13i2.84467
e-ISSN 2656-3266 and p-ISSN 2337-408X (Print)