The 3rd ASEAN School of Business Network International Conference 2026

www.aseansbn.org August 6-7, 2026 Pathum Thani, Thailand

Banking Governance in Digital Age: Does Cybersecurity Disclosure Matter to Improve Performance?

Khoirina Noor Anindya[1]*

[1]Universitas Islam Indonesia, Indonesia

*Corresponding Author: 24911078@students.uii.ac.id

ABSTRACT

The rapid digital transformation of the banking industry has increased exposure to digital and cyber risks, requiring stronger governance mechanisms to ensure effective digital risk management and transparency. This study examines the effect of banking governance mechanism namely 1) IT Committee; 2) Board Skill Index and 3) Board Gender Diversity on cybersecurity disclosure, then cybersecurity disclosure on bank performance. Using panel data from banking firms listed on the Indonesia Stock Exchange during 2016–2025, this research applies panel regression analysis to test the proposed relationships. Banking governance is measured by 1) IT Committee; 2) Board Skill Index and 3) Board Gender Diversity which reflecting digital-oriented governance characteristics, while cybersecurity disclosure is assessed using content analysis of annual reports. Bank performance is proxied by Return on Equity. The findings show mixed results between banking governance and cybersecurity disclosure. Cybersecurity disclosure has a positive effect on bank performance.

Keywords: Banking Governance; Cybersecurity Disclosure; Bank Performance.

DOI: https://doi.org/10.64458/asbnic.v3.167

Introduction

The banking industry was previously a physical storage entity, has now transformed into a data-based entity in the digital era and changed the company's business model (Figuigui & Machrouh, 2020). These developments are shifting banking services, bank-customer interactions, bank compliance with regulations, and the future of banking (Liu, 2021; Shehadeh, 2025). The existence of digital shock associated with the Covid-19 pandemic, where people have limitations in interacting physically, has increased digital transformation in all sectors, especially financial services and banking industry (Rahayu, et al., 2020). With this situation, banking industry faces several challenges, including 1) Digital revolution; 2) Changes in customer behaviour and expectations; and 3) New banking models (Figuigui & Machrouh, 2020; Asmar & Tuqan, 2024).

The banking industry's acceleration in the use of digital technologies such as cloud computing, artificial intelligence, and open banking has changed the definition of operational efficiency in banking. Open Banking is a condition where banks provide customer account access to third-party providers through open Application Program Interfaces (APIs), enabling third parties to build financial services on

top of the bank's data and infrastructure (Fischer-Hubner, et al., 2021). However, this innovation comes with the asymmetric and systemic cyber risks. Furthermore, data breaches, ransomware attacks, and sophisticated financial fraud become the real threats (Hassan, et al., 2024). The Indonesia National Cyber Security Operations Center stated that in 2020 there were 495 million cyber-attacks, an increase of 50% from the previous year (Rahayu, et al., 2020). Financial services and banking industry are increasingly subject to cyber incidents and attacks (Skinner, 2019).

Based on the digital treats, strengthening governance is necessary. As institutions that manage public funds and payment systems, banks are prime targets for cyber-attacks. In the Indonesian context, regulators emphasize oversight of risk management by strengthening risk management and information technology governance in the banking industry. However, changes in governance and the set of rules and principles that guide and oversee organizations sometimes leave companies at a crossroads (Malukani, Joshi, & Ubeja, 2024).

Facing various challenges, banks can no longer operate as business as usual. Corporate governance exists not only as a mechanism for monitoring business continuity, particularly the relationship between management and stakeholders. Banking governance required to mitigate technological risks, cybersecurity, customer data protection, and digital investment. Given the complexity of today's challenges, the establishment of an independent and dedicated IT committee is a bank's structural dedication to digital resilience.

Banking governance, which has discussed a lot about board size and board characteristics, is now developing in the technology area where the emergence of the IT committee or IT director and strengthening the position of Chief Risk Officer (CRO) in the organization has become very crucial (Elsayed, Ismail, & Ahmed, 2024). The IT committee or IT director plays an important role in banking governance because not all Board of Directors (BOD) have sufficient capabilities in handling and managing risks and preventing cyber-attacks.

Furthermore, the diversity skill of the Board of Directors (BOD) also influences technology decision-making. A diverse BOD enables banks to comprehensively identify risks and address regulatory changes. The board's ability to understand the digital threat landscape significantly impacts the quality of strategic decision-making. The board members with relevant expertise in finance, risk management, or governance domains are important factors that influence oversight quality and strategic agility (Mansour, Zureigat, Alkhlifhalsaeed, & Alkhatib, 2026).

The BOD structure with female leaders offers an advantage in cyber strategy. Women are inherently more cautious and sensitive to emerging issues, thus benefiting the BOD in decision-making, particularly in anticipating technological disruption and cyber-attacks. Banking companies are enhancing cybersecurity by providing cybersecurity disclosure. The significance of cybersecurity has escalated dramatically, becoming a pivotal aspect of organizational strategy and national security (Abrahams, Ewuga, Dawodu, Adegbite, & Hassan, 2024)

Board skill diversity is not just an oversight mechanism in banking industry, but also a strategic resource for the organization. Diverse competencies within the board, for example finance, information technology, risk management, law, and the banking industry enhance the organization's capacity to navigate environmental uncertainty. Based on Mansour, Zureigat, Alkhlifhalsaeed, & Alkhatib (2026), board with diverse competence has a positive effect on cybersecurity disclosure.

Board gender diversity as a mechanism of banking governance, has a benefit to make a good decision about strategic issue especially cybersecurity. Boards with three or more female directors show a strong positive influence on cybersecurity disclosure (Afroze, Gosh & Dey, 2025). The presence of women on bank boards is expected to balance digitalization ambitions with prudence in data protection. But, based on Alodat, et al., (2024), board gender diversity has no impact on cybersecurity disclosure.

Moreover, cybersecurity disclosure which is triggered by IT committee or IT director, board skill diversity and board gender diversity, also strengthen the bank performance. Regarding to Elsayed,

Ismail, & Ahmed (2024), cybersecurity disclosure has a positive and significant influence on bank performance. Cybersecurity policy which reflects in annual report has a statistically significant positive effect accounting performance (Bruno, Pistolesi, & Teti, 2025). But in the other hand, the existence of cybersecurity policies has a negative effect on bank performance because the costs of implementing cybersecurity exceed the benefits derived (Amani, Magnan, & Moldovan, 2025). With or without a cybersecurity-related committee, the presence of a board possessing IT expertise and female directors is associated with cybersecurity disclosure, particularly regarding cybersecurity mitigation. (Héroux & Fortin, 2024).

The priority of an IT committee and the diversity of abilities and gender of the BOD, it can improve cybersecurity disclosure carried out by banks (Shehadeh, 2025). The cybersecurity disclosure plays a crucial role in banking governance, improving performance, acting as a bridge. Companies can achieve high profits, a proxy for performance, because the IT committee produces transparent cyber reporting in their annual reports, providing investor confidence and driving stable, or even rising, stock prices. This aligns with signaling theory, which suggests that investors view the cybersecurity disclosure as positive information. Studying the sentiment of cyber disclosure has hence become essential, as it can affect the perceptions and decisions of stakeholders, including investors, regulators, and the public (Elnahass, Ahmed, & Trinh, 2025).

Literature Review

Digital Transformation in The Banking Industry

Digital transformation refers to changes occurring in activities, competencies, and business models due to the use of new digital technologies. Digital transformation in the banking industry involves two aspects: technology and services. Financial services include payments, credit, wealth management, investment banking, and communications. Technology includes cloud computing, AI, machine learning, big data, distributed ledgers, APIs, robo-advisors, and mobile technology (Liu, 2021).

Banking Governance

The corporate governance mechanism in banking in the digital era is carried out by maximizing the role of the BOD. The board of directors has two functions: monitoring managers (control role) and providing resources (service role). (Islam, Farah, & Stafford, 2026). Some of the banking governance mechanism are 1) IT Committee or IT Director; 2) Board Skill Diversity; and Board Gender Diversity.

1) IT Committee or IT Director

The IT Committee in the BOD or IT Director is responsible for overseeing the technology strategy within the company, as well as improving customer data security, thereby strengthening corporate governance (Firoozi & Mohsni, 2023).

2) Board Skill Diversity

The diversity of abilities or competencies of the BOD shows that the company's organizational structure has various competencies that can improve decision-making related to company strategy in the digital era (Firoozi & Mohsni, 2023).

3) Board Gender Diversity

Gender diversity on the Board of Directors (BOD) brings a different oversight perspective, with women in corporate leadership positions tending to be more cautious in decision-making. Boards with female representation appear more effective at changing board norms and can enhance corporate governance. (Srinidhi, Sun, Zhang, & Chen, 2020).

Cybersecurity Disclosure

Cybersecurity has now become a service in various fields, where cybersecurity is a necessity for organizations to protect large amounts of sensitive data and comply with regulatory standards. Based on

Hassan, et al., cybersecurity has become a major concern in the banking industry. Cybersecurity as an area of concern and governance has largely been addressed through multi-stakeholder governance (Eggenschwiler, 2018). Cybersecurity in banking also has become a paramount concern, requiring a proactive and adaptive approach to protect sensitive data, maintain trust, and ensure the resilience of financial systems (López, Jara-Sarrúa, Morales-Parada, & Palos-Sánchez, 2025).

Method

This research employs a quantitative approach using panel data analysis to examine the relationship between banking governance, cybersecurity disclosure, and firm performance. Secondary data are collected from annual reports of banking firms listed on the Indonesia Stock Exchange (IDX) during the observation period. The analytical tool used in this study is EViews with the Generalized Least Squares (GLS) method and a purposive sampling technique. The sample was determined using several criteria:

1) Banking companies listed on the Indonesia Stock Exchange
2) Banking companies that published annual reports consecutively between 2016 and 2025
3) Banking companies that presented the required variables

Table 1. Main Variables

Banking Governance				
Variable	**Label**	**Definition**	**Measurement**	**Source**
IT Committee	ITC	The presence of a dedicated committee within the bank's Board of Directors responsible for overseeing information technology strategy and cybersecurity.	Dummy variable which assigned a value of "1" IT committee if exists in BOD; and the value of "0" otherwise	(Jallali & Zoghlami, 2022)
Board Skill Index	BSkill	The level of skill diversity among members of the Board of Directors in domains relevant to digital risk management and corporate governance.	Percentage of board members with relevant expertise (finance, risk management, or governance domains).	(Firoozi & Mohsni, 2023)
Board Gender Diversity	BDiv	The level of gender diversity in the composition of the Board of Directors, reflecting the presence of female perspectives in strategic decision-making.	Percentage of Women on Board Directors	(Afroze, Ghosh, & Dey, 2025)
Cybersecurity Disclosure				
Variable	**Label**	**Definition**	**Measurement**	**Source**
Cybersecurity Disclosure	CSD	The level of transparency in a company's disclosure of information related to cybersecurity policies, strategies, and risk management in its annual reports.	The natural log of one plus total number of words related to cybersecurity (cybersecurity, security, cyber-attacks, data breach, IT, and related keywords) that appear in a company's report.	(Afroze, Gosh & Dey, 2025).

Performance				
Variable	**Label**	**Definition**	**Measurement**	**Source**
Return on Equity	ROE	Company's profitability by calculating how efficiently it generates profit from shareholders' equity.	Net Income divided by Total Equity	(Kumar, Gupta, & Das, 2022)

Table 2. Control Variables

Variables	Label	Definition	Measurement	Source
Bank Age	Age	The length of time a bank has been operating since its establishment, reflecting the bank's experience and reputation.	Natural logarithm of the number of years since the bank's founding	(Smaili, Radu, & Khalili, 2023) (Al-Sartawi, Sanad, Shehadeh, & Binsaddig, 2025)
Bank Size	Size	The size of the bank, reflecting the scale of its operations and business complexity.	Natural log value of one plus total asset	(Afroze, Ghosh, & Dey, 2025) (Al-Sartawi, Sanad, Shehadeh, & Binsaddig, 2025)
Leverage	Leverage	The level of debt usage in a bank's capital structure, reflecting its financial risk.	Ratio of total debt to total asset	(Afroze, Ghosh, & Dey, 2025) (Al-Sartawi, Sanad, Shehadeh, & Binsaddig, 2025)
Capital Adequacy Ratio	CAR	The capital adequacy ratio that measures a bank's ability to absorb losses and meet its obligations in accordance with Basel III regulations.	(Tier 1 Capital + Tier 2 Capital) divided by Risk weighted average assets	(Jallali & Zoghlami, 2022)

Results

Table 3. Descriptive Statistic

	IT Com	B Skill	B Div	CSD	Age	Leverage	CAR	Size	ROE
Mean	0.584615	70.16262	24.33108	3.226846	3.715000	77.52792	24.89085	17.12162	13.37523
Median	1.000000	75.00000	20.00000	3.430000	4.060000	83.26000	22.42500	18.58000	13.12500
Maximum	1.000000	100.0000	75.00000	5.300000	4.370000	91.07000	58.27000	21.76000	36.50000
Minimum	0.000000	12.50000	0.000000	0.000000	0.690000	0.000000	13.69000	11.16000	-3.79000
Std. Dev.	0.494695	21.73479	15.70130	1.174778	0.697616	19.04781	8.562508	3.215599	6.845320

Table 4. Regression Results (Banking Governance on Cybersecurity Disclosure)

	1)	2)	3)	4)
Constant	-4.057603***	-4.461991***	-4.417672***	-4.431272
IT Committee	0.233208			0.143061
Board Skill		0.012392***		0.008382*
Board Diverse			-0.018949***	-0.017214***
Firm Age	1.554508***	1.436634***	1.398867***	1.453748***
Leverage	-0.019677*	-0.018937*	-0.004435	-0.012871
Capital Adequacy Ratio	0.045629***	0.050377***	0.062481***	0.058931***
Bank Size	0.104514***	0.097348***	0.095984***	0.085743***

*Significant on 10%, **Significant on 5%, ***Significant on 1%

Table 5. Regression Results (Cybersecurity Disclosure on Performance)

	1)
Constant	42.98802***
CSD	1.167390***
Firm Age	-7.728178***
Leverage	0.085930
Capital Adequacy Ratio	-0.167189
Bank Size	-0.426005***

*Significant on 10%, **Significant on 5%, ***Significant on 1%

Discussion

Banking Governance on Cybersecurity Disclosure

1) IT Committee on Cybersecurity Disclosure

Based on Table 4, the IT Committee does not significantly influence Cybersecurity Disclosure (CSD) because the IT Committee in the banking governance system handles the technical aspects of IT maintenance and preventing cyberattacks, not the public disclosure of cybersecurity reflected in financial reports. If a successful cyberattack occurs, involving the loss of personal financial information and causing significant losses to shareholder wealth, it will be a major public concern (Kamiya, Kang, Kim, Milidonis, & Stulz, 2021). Public attention focused on management's inability to address cyber attacks will be the IT Committee's primary focus rather than increasing cybersecurity disclosure in financial reports.

The IT Committee's insignificant influence on cybersecurity disclosure in financial reports can be explained by the functional differences between technology oversight and public information disclosure policies. In general, the IT Committee plays a role in ensuring the effective implementation of information technology systems, digital infrastructure security, and technology-based operational risk management, but is not directly involved in determining the company's external reporting policies. Cyber risk disclosure in annual reports is typically part of a company's strategic policy, coordinated by the audit committee, risk management committee, or regulatory compliance function. Furthermore, disclosure of cybersecurity-related information is sensitive because it has the potential to expose company system vulnerabilities, so management tends to be cautious in determining the level of transparency to be disclosed to the public. In the highly regulated banking sector, cybersecurity disclosure practices are also more influenced by regulatory standards and company risk management policies than by the existence of a formal information technology committee. Therefore, the existence of

an IT Committee is not always a determining factor in increasing the level of cybersecurity disclosure in a banking company's financial reports.

This finding contrasts with the findings from (Haislip, Karim, Lin, & Pinsker, 2020) which state that CEOs with IT expertise and IT expertise on the board facilitate efficient IT utilization and are associated with timely information disclosure. This condition also contradicts with findings of (Ling, Liu, & Xia, 2025) and (Elmarzouky, Moussa, & Allam, 2025) which state that firms with a greater focus on cybersecurity governance at the board level (e.g., directors with IT expertise, the presence of IT committees and cybersecurity policies) demonstrate a higher commitment to managing and reporting cybersecurity risks and solutions.

In addition, with the current development of the financial landscape which is characterized by technological innovation and cybersecurity challenges, the banking sector also needs to understand the changes in leadership, in this case the change in the proportion of directors who include an IT Director or IT Committee in management (Moridu, Devi, Susanti, & Fatimah, 2023).

2) Board Skill on Cybersecurity Disclosure

Based on Table 4, board skill has a positive effect on cybersecurity disclosure. Board skills reflect the level of competence of board members, who come from backgrounds in finance, information technology, risk management, law, and the banking industry. In the era of digital transformation, cyber risk has become a complex strategic risk and requires multidisciplinary understanding at the board level. Boards with more diverse competencies are better able to understand digital risk exposures and evaluate management's technology security policies. This aligns with (Firoozi & Mohsni, 2023), which states that diversity in relevant expertise in finance, risk management, or governance domains can better monitor technology risks, leading to better disclosures related to information technology issues.

Based on the resource dependence theory proposed by Pfeffer and Salancik in 1978, the board serves as a provider of strategic resources in the form of expertise and experience that support the quality of organizational decision-making. This result also aligns with findings (Hillman, Withers, & Collins, 2009), which state that companies can reduce their dependence on the environment by having an effective board of directors, where the board of directors can make decisions for the company's future growth.

With diverse board skills and expertise, companies can improve the effectiveness of cyber risk oversight, thereby promoting transparency in the disclosure of digital security information. Furthermore, from the perspective of agency theory, as described by Jensen and Meckling in 1976, a competent board of directors can reduce information asymmetry between management and stakeholders by improving the quality of monitoring. Companies view cyber risks as technical and complex, so boards with diverse levels of competence tend to encourage more comprehensive cybersecurity disclosures, which are reflected in the company's annual report.

Resource dependency theory leads us to expect that director appointments depend in part on endogenous aspects such as the human capital (knowledge, skills, experience) and social capital (networks, social connections) they can bring to the firm (Haldar, Datta, & Shah, 2020). Proposed by Pfeffer and Salancik in 1978, the board serves as a provider of strategic resources in the form of expertise and experience that support the quality of organizational decision-making. This result also aligns with findings (Hillman, Withers, & Collins, 2009), which state that companies can reduce their dependence on the environment by having an effective board of directors, where the board of directors can make decisions for the company's future growth.

With diverse board skills and expertise, companies can improve the effectiveness of cyber risk oversight, thereby promoting transparency in the disclosure of digital security information. Furthermore, from the perspective of agency theory, as described by Jensen and Meckling in 1976, a competent board of directors can reduce information asymmetry between management and stakeholders by improving the quality of monitoring. Companies view cyber risks as technical and

complex, so boards with diverse levels of competence tend to encourage more comprehensive cybersecurity disclosures, which are reflected in the company's annual report.
Resource dependency theory leads us to expect that director appointments depend in part on endogenous aspects such as the human capital (knowledge, skills, experience) and social capital (networks, social connections) they can bring to the firm (Haldar, Datta, & Shah, 2020).

3) Board Diversity on Cybersecurity Disclosure

Based on Table 4, the percentage of female directors negatively impact cybersecurity disclosure in the banking sector can be explained by the specific characteristics of cyber risk disclosure, which differ from disclosure of other financial and non-financial information. In corporate governance literature, the presence of women on boards is often associated with a higher level of caution regarding strategic and reputational risks. In the banking sector, which relies heavily on public trust and the stability of information systems, cybersecurity disclosure serves not only as a means of transparency but also as part of the company's communication risk management strategy. Boards with higher levels of risk sensitivity tend to consider the potential negative consequences of overly broad cybersecurity disclosure, such as increased vulnerability to cyberattacks or the perception of greater risk among investors and customers. Therefore, the presence of female directors may encourage a more conservative approach to disclosure as a means of protecting the bank's operational stability and reputation.

In developing countries, women's representation on company boards of directors has not been regulated as in Europe, which has established quotas for female representation on publicly traded corporate and/or state-owned enterprise boards of directors, ranging from 33 to 50%, with various sanctions (Terjesen, Aguilera, & Lorenz, 2015). On the other hand, cybersecurity disclosure is a technical and sensitive type of disclosure, so it is more influenced by the board's digital competence, pressure from regulators such as the Financial Services Authority, and the company's risk management policies than by the demographic characteristics of board members. Therefore, the negative influence of female directors on cybersecurity disclosure can be understood as a reflection of the board's caution in maintaining a balance between information transparency and protecting the security of the banking system. These results contradict with the findings from (Seebeck & Vetter, 2022), which suggest that board gender diversity is positively related to corporate risk disclosure. One of the company risks is cyberattacks, and companies can also provide information to the public regarding IT system management to ward off such attacks.

Cybersecurity Disclosure on Performance

Based on Table 5, cybersecurity disclosure has a positive effect on bank performance. Broader cybersecurity disclosure reflects a company's ability to manage digital risks transparently and systematically, thereby increasing investor confidence in the quality of corporate governance. From a signalling theory perspective, cybersecurity disclosure serves as a signal that a company is prepared to face cyber threats that could potentially disrupt operations and financial stability. Investors view cybersecurity disclosure as positive information (Elnahass, Ahmed, & Trinh, 2025).

This aspect is worsened by the leakage of sensitive client data, which in most cases has magnified legal and regulatory consequences. In addition, most modern-day financial systems are so deeply embedded that the failure of one institution can ripple throughout the entire financial system (Al-Sartawi, Sanad, Shehadeh, & Binsaddig, 2025). Higher levels of transparency regarding information security policies, data protection, and technology risk management can reduce investor uncertainty and enhance perceptions of management credibility. This condition fosters shareholder confidence, ultimately contributing to increased efficiency in the use of a company's equity, as reflected in Return on Equity (ROE).

Furthermore, from an agency theory perspective, cybersecurity disclosure serves as a mechanism to reduce information asymmetry between management and investors regarding a

company's digital risk exposure. Transparency regarding cyber risk management demonstrates a company's robust internal control system and readiness to face technology-based operational disruptions. In the banking sector and companies dependent on digital infrastructure, the ability to maintain information system security is directly related to operational stability, reputation protection, and sustainable profitability. Therefore, companies with higher levels of cybersecurity disclosure tend to have better financial performance due to increased investor confidence and efficient capital management.

Conclusion

There are 2 findings in this research, that are 1) Banking Governance influences Cybersecurity Disclosure and 2) Cybersecurity Disclosure influences Performance

1) Banking governance regarding cybersecurity disclosure in the digital age, consisting of the IT Committee, Board Skill, and Board Diversity, yielded mixed findings. The IT Committee had no effect on cybersecurity disclosure because the IT Committee or IT Board within the company's board structure is defined as a part that provides technical IT services and does not directly influence cybersecurity disclosures written in the company's annual report. Board Skill has a positive effect on cybersecurity disclosure because the diversity of skills and expertise of the directors creates a management structure with strong cognitive collection that can encourage increased cybersecurity disclosure. In addition, decision-making can also be carried out carefully and consider various perspectives. Board diversity has a negative effect on cybersecurity disclosure. Board diversity is measured using the percentage of female directors on the board of directors in the banking sector. The results show that a higher number of female directors can weaken cybersecurity disclosure. This condition means that female directors who are cautious tend to avoid broad disclosures to the public related to the company's cybersecurity. Diversity in the board that can improve cybersecurity is not represented by the presence of female board members but by the diversity of skills and expertise they possess.
2) Cybersecurity disclosure has a positive impact on company performance. This is linked to signalling theory, which suggests that the public perceives companies that prioritize cybersecurity as well-managed, especially in today's digital age. Well-managed refers to the ability of directors to manage the company using IT systems and cyberattack mitigation. This translates into increased profits relative to the company's equity. Higher profits reflect a company's ability to effectively manage shareholder capital.

Recommendations

The results show that banking governance mechanisms have varying effects on cybersecurity disclosure, but cybersecurity disclosure has a positive effect on bank performance indicates that cybersecurity plays a strategic role in improving equity-based financial performance in the banking sector. Therefore, although not all components of banking governance directly drive cybersecurity disclosure, improving the quality of cyber risk disclosure remains an important mechanism strengthening the relationship between digital governance and bank financial performance in the era of digital transformation. The future research should incorporate other proxies to measure Cybersecurity Disclosure and extend the observation.

Acknowledgements

The researcher would like to express sincere appreciation to the Center of Management Development – Management Department – Universitas Islam Indonesia for the funding support provided in the completion of this research.

References

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity. *Computer Science & IT Research Journal, Volume 5, Issue 1, January 2024*, 1-25. https://doi.org/10.51594/csitrj.v5i1.699

Al-Sartawi, A. M., Sanad, Z., Shehadeh, M., & Binsaddig, R. (2025). Cybersecurity and Banks Performance: Evidence. *International Journal of Cyber Criminology Vol 19 Issue 1 January – June 2025*, 1 - 18.

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity Risks and Insidents Disclosure: A Literature Review. *Accounting Perspective, Vol.24, No. 3 (2025)*, 605-667. https://doi.org/10.1111/1911-3838.12411

Bruno, E., Pistolesi, F., & Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A Virtuous relationship to improve banks' performance. *International Review of Economics and Finance 99 (2025) 104053* , 1-13. https://doi.org/10.1016/j.iref.2025.104053

Eggenschwiler, J. (2018). A Typology of Cybersecuirty Governance Models. *St Antony's International Review, February 2018, Vol. 13, No. 2, International Relations in a Post-Factual World (February 2018)*, 67-78.

Elmarzouky, M., Moussa, T., & Allam, A. (2025). Cybersecurity disclosure: board commitment and regulatory impact in the UK. *The International Journal of Accounting, 31 Jul 2025*. https://doi.org/10.1142/S1094406025420053

Elnahass, M., Ahmed, Y., & Trinh, V. Q. (2025). Empowering Women to Lead Cybersecurity: The Effect of Female Executives on Disclosure Sentiment. *International Journal of Finance & Economics, 15 October 2025*, 1-27. https://doi.org/10.1002/ijfe.3067

Figuigui, B., & Machrouh, F. (2020). Banking Governance in The Era of Digital Transformation. *Journal of Research in Administrative Sciences, Vol.IX, Issue II, 2020*, 10-16.

Firoozi, M., & Mohsni, S. (2023). Cybersecurity disclosure in the banking industry: a comparative study . *International Journal of Disclosure and Governance, Palgrave Macmillan, Vol.20 (4)*, 451-477. https://doi.org/10.1057/s41310-023-00190-8

Fischer-Hubner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., . . . Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications 61 (2021) 102916*, 1-16. https://doi.org/10.1016/j.jisa.2021.102916

Haislip, J. Z., Karim, K. E., Lin, K. J., & Pinsker, R. E. (2020). The Influences of CEO IT Expertise and Board-Level Technology Committees on Form 8-K Disclosure Timeliness Available to Purchase. *Journal of Information Systems (2020) 34 (2)*, 167–185. https://doi.org/10.2308/isys-52530

Haldar, A., Datta, S., & Shah, S. (2020). Tokenism or realism? Gender inclusion in corporate boards. *Equality, Diversity and Inclusion: An International Journal Vol. 39 No. 6, 2020*, 707-725. https://doi.org/10.1108/EDI-04-2019-0126

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in Banking: A Global Perspective With a Focus Nigerian Banking. *Computer Science & IT Research Journal, Volume 5, Issue 1, January 2024*, 41-59.

Héroux, S., & Fortin, A. (2024). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance, Vol.28,* 359-404. https://doi.org/10.1007/s10997-022-09660-7

Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource Dependence Theory: A Review. *Southern Manahement Association (SMA) Volume 35, Issue 6,2009*, 1404–1427.

Islam, M. S., Farah, N., & Stafford, T. (2026). Do Women on the Board Mitigate Cybersecurity Risks? *Journal of Information Systems, Vol.XX, No.XX*, 1-33. http://dx.doi.org/10.2139/ssrn.5126335

Jallali, S., & Zoghlami, F. (2022). Does risk governance mediate the impact of governance and risk management on banks' performance? Evidence from a selected sample of Islamic banks. *Journal*

of Financial Regulation and Compliance (2022) 30 (4), 439–464. https://doi.org/10.1108/JFRC-04-2021-0037

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139 (2021)*, 719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kumar, A., Gupta, J., & Das, N. (2022). Revisiting the influence of corporate sustainability practices on corporate financial performance: An evidence from the global energy sector. *Business Strategy and the EnvironmentVolume 31, Issue 7, 2022*, 3231-3253. https://doi.org/10.1002/bse.3073

Ling, S., Liu, Z. (., & Xia, H. (2025). Code, control and cybersecurity: how board IT expertise shapes corporate risk management. *Journal of Accounting Literature, September 05, 2025*, 1-23. https://doi.org/10.1108/JAL-06-2025-0320

López, F. A., Jara-Sarrúa, L., Morales-Parada, F., & Palos-Sánchez, P. R. (2025). Cybersecurity disclosure in the financial sector: an examination of the influence of incident exposure, governance practices, and regulatory context. *Electronic Commerce Research, 31 December 2025*, 1-29. https://doi.org/10.1007/s10660-025-10081-5

Malukani, B., Joshi, A., & Ubeja, S. (2024). Corporate Governance in The Digital Age . *IUP Journal of Corporate Governance; Hyderabad Vol. 23, Iss. 3, (Jul 2024)*, 50-58.

Mansour, M., Zureigat, B. N., Alkhlifhalsaeed, A., & Alkhatib, A. (2026). Cybersecurity Disclosure, Board Oversight, and Financial Performance: Evidence from European Banking . *Corporate Board: Role, Duties and Composition, 22(1), 2026*, 8–22. https://doi.org/10.22495/cbv22i1art1

Moridu, I., Devi, E. K., Susanti, P., & Fatimah, S. (2023). Analysis of the Impact of Changes in Directors, IT Directors, and Risk Management of BSI (BRIS) on Information Technology Performance and Security and Risk Control at one of the BSI Bank Branches in Bandung City. *West Science Business and Management, Vol. 1, No. 04, September 2023*, 288~295.

Rahayu, I., Kurniawan, S., Imanullah, A., Maulana, Y., Kharisma, S., Afifah, & Dicky, F. (2020). *Profil Risiko Sektor Perbankan Tahun 2020 - Direkorat Identifikasi Kerenanan dan Penilaian Risiko Infrastruktur Kritikal Nasional.* Depok: Badan Siber dan Sandi Negara.

Seebeck, A., & Vetter, J. (2022). Not Just a Gender Numbers Game: How Board Gender Diversity Affects Corporate Risk Disclosure. *Journal of Business Ethics, Vol. 177, No. 2 (May 2022)*, 395-420. https://doi.org/10.1007/s10551-020-04690-3

Shehadeh, M. (2025). Disclosures on digital transformation strategy and financial technology in Jordanian banks: innovations, challenges and opportunities. *Journal of Financial Reporting and Accounting, 3 May 2025* , 1-29. https://doi.org/10.1108/JFRA-12-2024-0972

Skinner, C. P. (2019). Bank Disclosure of Cyber Exposure. *Iowa Law Review, Vol.105, 2019*, 239-281.

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management & Governance, Vol. 27(4), December, 2023*, 1049-1071. https://doi.org/10.1007/s10997-022-09637-6

Srinidhi, B., Sun, Y., Zhang, H., & Chen, S. (2020). How do female directors improve board governance? A mechanism based on norm changes. *Journal of Contemporary Accounting and Economics 16 (2020) 100181*, 1-18. https://doi.org/10.1016/j.jcae.2019.100181

Terjesen, S., Aguilera, R. V., & Lorenz, R. (2015). Legislating a Woman's Seat on the Board: Institutional Factors Driving Gender Quotas for Boards of Directors. *Journal of Business Ethics , May 2015, Vol. 128, No. 2 (May 2015)*, 233-251. https://doi.org/10.1007/s10551-014-2083-1