CYBERSECURITY DISCLOSURE, BOARD OVERSIGHT, AND FINANCIAL PERFORMANCE: EVIDENCE FROM EUROPEAN BANKING

Marwan Mansour *, Bilal Nayef Zureigat **, Abdulaziz Alkhlifhalsaeed ***, Ahmed Alkhatib ***

* *Corresponding author,* Amman Arab University, Amman, Jordan
Contact details: Amman Arab University, Jordan Street — Mubis, P. O. Box 2234, Amman 11953, Jordan
** Amman Arab University, Amman, Jordan
*** King Faisal University, Al-Ahsa, Saudi Arabia

How to cite this paper: 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), 8–22.
https://doi.org/10.22495/cbv22i1art1

ISSN Online: 2312-2722
ISSN Print: 1810-8601

Received: 19.09.2025
Revised: 09.12.2025; 24.12.2025
Accepted: 29.12.2025

JEL Classification: G21, G32, G34, K22, M41
DOI: 10.22495/cbv22i1art1

Abstract

This study investigates whether voluntary cybersecurity disclosure (CSD) operates as a value-relevant governance mechanism in European banking. Drawing on stakeholder, agency, and signaling theories, we argue that credible cyber transparency reduces information asymmetry, strengthens legitimacy, and signals operational resilience to investors and regulators (Berkman et al., 2018; Alsadoun & Albaz, 2025). Using an unbalanced panel of 5,742 bank-year observations from 638 banks across 25 European countries (2014–2022), we construct a binary CSD indicator based on manual content analysis of annual reports and estimate pooled ordinary least squares (OLS), fixed-effects (FE), and two-step system generalized method of moments (GMM) models. The results show that CSD is positively associated with both accounting performance (return on equity, ROE) and market valuation (Tobin's Q). These effects are stronger in banks with higher leverage and stronger board oversight, including greater audit committee expertise, board gender diversity, independence, and board skills. Our findings suggest that CSD is not merely a compliance exercise but a board-level governance tool that enhances financial outcomes and supports emerging regulatory initiatives such as the Digital Operational Resilience Act (DORA). The study offers policy-relevant insights for regulators, investors, and bank executives seeking to align digital resilience with sustainable financial performance.

Keywords: Cybersecurity Disclosure, Corporate Governance, Board Oversight, Corporate Reporting, Bank Performance, Europe

Authors' individual contribution: Conceptualization — M.M.; Methodology — M.M.; Software — M.M. and B.N.Z.; Validation — B.N.Z.; Formal Analysis — M.M. and B.N.Z.; Investigation — Ab.A.; Resources — Ab.A.; Data Curation — B.N.Z.; Writing — Original Draft — M.M.; Writing — Review & Editing — B.N.Z., Ab.A., and Ah.A.; Visualization — M.M. and B.N.Z.; Supervision — M.M.; Project Administration — Ah.A.; Funding Acquisition — Ah.A.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: The Authors gratefully acknowledge the support provided by Amman Arab University and King Faisal University, whose academic environments and research facilities played a vital role in enabling the development and completion of this study. This work was funded by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU254502].

1. INTRODUCTION

The intensifying digitization of financial systems has substantially increased the exposure of banks to cybersecurity threats, heightening the operational and financial vulnerabilities of institutions across global markets. Cyberattacks have evolved in scale, sophistication, and strategic intent, generating severe consequences for organizational resilience and stakeholder trust. As a result, cybersecurity has moved beyond the realm of technical risk to become a core component of corporate governance and enterprise risk management frameworks. In this context, cybersecurity disclosure (CSD) has emerged as a voluntary transparency mechanism with growing relevance, signaling institutional competence, regulatory readiness, and environmental, social, and governance (ESG) alignment.

Banks, as critical nodes in the digital economy, face disproportionate risk due to their complex technological infrastructures, sensitive data holdings, and systemic importance. In Europe, financial institutions are increasingly pressured by regulators, investors, and ESG rating agencies to strengthen cyber governance and provide clear, consistent disclosures of cybersecurity risks and mitigation strategies. These demands have intensified in the aftermath of notable incidents and regulatory shifts, pushing CSD into the strategic foreground of bank governance.

While studies from emerging markets and non-European contexts — such as Karyani et al. (2024) and Matemane et al. (2024) — demonstrate that cybersecurity transparency enhances financial resilience and investor confidence, the European context remains empirically underexplored. Existing research has often focused on broader ESG disclosures or lacked methodological rigor in isolating the unique financial implications of CSD within the European Union (EU) banking landscape. Moreover, most studies fail to account for the distinct supervisory environment shaped by the European Central Bank (ECB), the Single Supervisory Mechanism, and emerging policy frameworks such as the Digital Operational Resilience Act (DORA).

Although DORA was formally adopted in 2023, its regulatory momentum — fueled by prior policy drafts, consultation papers, and market expectations — likely influenced disclosure behavior well before its official implementation. Evidence from institutional data supports this trajectory: in 2023, over 4,600 cyber incidents were reported in the EU financial sector, yet only 38% of banks disclosed cybersecurity risks in their ESG filings (European Union Agency for Cybersecurity [ENISA], 2024; European Banking Authority [EBA], 2022). This discrepancy underscores the persistence of voluntary gaps and strategic discretion in cybersecurity reporting, particularly in the pre-DORA period (2014–2022).

Theoretically, this study integrates stakeholder theory, which posits that CSD serves as a legitimacy mechanism to reduce uncertainty and align with stakeholder expectations; agency theory, which views transparency as a tool to mitigate information asymmetries and enhance managerial accountability; and signaling theory, which frames CSD as a strategic signal of institutional reliability and operational robustness. These complementary frameworks allow for a multifaceted interpretation of how and why CSD may influence firm performance.

Despite growing regulatory and academic attention, few empirical studies have rigorously evaluated the performance implications of voluntary CSD in European banking. The conflation of cybersecurity with general ESG reporting, limited cross-country coverage, and insufficient handling of endogeneity weaken existing evidence. This study addresses these gaps by constructing a novel binary measure of CSD based on manual content analysis of annual reports from 638 European banks across 25 countries over the period 2014–2022.

We employ a robust empirical strategy combining pooled ordinary least squares (OLS), fixed-effects (FE) models, and system generalized method of moments (GMM) to account for unobserved heterogeneity, reverse causality, and dynamic relationships. Furthermore, we conduct a heterogeneous effect analysis based on bank risk profile (leverage levels) to explore whether transparency yields differential benefits in high-risk environments.

This paper makes three key contributions. First, it provides the first large-scale, causal analysis of the financial consequences of voluntary CSD within the European banking sector. Second, it situates CSD within a theoretical and institutional governance framework, demonstrating how cybersecurity transparency functions as a value-relevant signal in an evolving regulatory landscape. Third, it offers policy-relevant insights for regulators, investors, and banking executives seeking to align digital resilience with financial outcomes in the pre-DORA period.

The remainder of this paper is structured as follows. Section 2 develops the theoretical framework and reviews prior research on CSD, board oversight, and bank performance. Section 3 describes the research design, sample selection, variable measurement, and econometric methods. Section 4 presents the empirical results, including baseline models, robustness tests, and heterogeneous effects by bank risk profile. Section 5 discusses the findings in light of stakeholder, agency, and signaling theories and situates them within the evolving European regulatory context. Section 6 concludes with key implications for regulators, boards, and investors, outlines policy recommendations, and suggests avenues for future research.

2. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

2.1. Theoretical framework

This research uses an integrated theoretical method to analyse how CSD affects EU bank financial performance. It uses stakeholder theory, agency theory, and signalling theory to describe how corporations manage risk, develop legitimacy, and share private information with external stakeholders. CSD may affect firm-level outcomes in a high-risk, regulated environment like the European banking industry via each theory's unique but complementary perspective (Alsadoun & Albaz, 2025; Kanyongo & Wadesango, 2025).

According to stakeholder theory, the company is immersed in social, regulatory, and economic connections. According to this approach, banks must retain legitimacy with shareholders, regulators, customers, staff, and the public (Alshdaifat et al., 2024; Hasani et al., 2023). Cybersecurity transparency addresses expanding social and regulatory demands for digital responsibility, especially in light of financial system cyber risks. Voluntary CSD boosts stakeholder trust and reputational certainty, improving the firm's social licence (Khan et al., 2025; Alodat et al., 2025).

However, agency theory emphasises managers' principal-agent conflict with shareholders, especially in opaque or high-risk fields like cybersecurity. Disclosures minimise information asymmetry, align management incentives, and strengthen board supervision (Radu & Smaili, 2022; Kiesow Cortez & Dekker, 2022; Xing et al., 2025). In cybersecurity, where performance measurements are sometimes unstandardised, CSD signals management responsibility and internal risk controls. This reduces moral hazard and protects long-term value in banks when shareholders have little information and communications technology (ICT) risk awareness.

Signalling theory views voluntary disclosures like CSD as strategic communications that explain the firm's unobservable strengths to the market. Since cyber resilience and digital preparation are intangible, organisations use disclosure to demonstrate good governance, technical maturity, and forward-thinking risk management. CSD improves investor views and may boost business value when signals are reliable, consistent, and entrenched in ESG narratives (Vo & Pham, 2025; Guohong et al., 2025).

These theoretical viewpoints agree that CSD is a strategic governance instrument, not just compliance. CSD boosts stakeholder legitimacy, reduces agency risks, and shows institutional digital threat expertise. This multi-theoretical basis supports the study's key hypothesis: that European banks with more voluntary cybersecurity openness have better accounting performance (return on equity, ROE) and market value (Tobin's Q).

Figure 1. Integrated theoretical framework linking stakeholder, agency, and signaling theories to CSD and bank performance

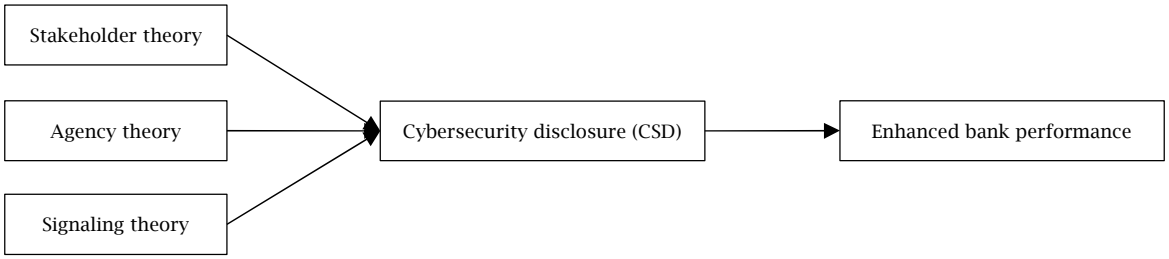

Figure 1 shows the theoretical framework based on stakeholder, agency, and signaling theories, viewing CSD as a strategic governance tool. Stakeholder theory emphasizes trust and legitimacy; agency theory focuses on reducing information gaps and increasing accountability; signaling theory pertains to external communication of cyber readiness. These mechanisms explain how CSD improves performance by strengthening stakeholder relations, governance, and market perceptions.

2.2. Hypothesis development

The digital transformation of banking has provided customers with unprecedented access to online and mobile services, but it has also intensified exposure to cyber threats. The increasing sophistication of attacks — exacerbated by cloud adoption, artificial intelligence, and fintech integrations — has placed mounting pressure on financial institutions to strengthen cyber resilience and disclose these practices transparently (ENISA, 2024; Cele & Kwenda, 2025; Kaur & Ramkumar, 2022).

Within this environment, CSD emerges as a governance mechanism that extends beyond regulatory compliance to address rising stakeholder demands for accountability. Recent evidence shows that disclosure levels often increase following high-profile breaches, suggesting firms strategically recalibrate risk communication in response to scrutiny. Importantly, voluntary disclosure — whether or not prompted by incidents — has been shown to improve market valuation and profitability (Chen et al., 2023; Elsayed et al., 2024), underscoring its role as a value-relevant signal.

Conversely, inconsistent or symbolic disclosure can erode trust, heighten reputational risk, and undermine credibility with regulators and investors (Tosun, 2021; Radu & Smaili, 2022). In a sector where digitalization is integral to operations, the absence of a credible CSD may weaken both governance structures and capital market confidence (Wang et al., 2024).

Theoretical perspectives converge in explaining why CSD matters:

- Stakeholder theory frames CSD as a legitimacy-enhancing tool that strengthens institutional credibility and aligns behavior with societal and regulatory expectations (Hasani et al., 2023; Alodat et al., 2025). Consistency and credibility are critical; without them, disclosure fails to generate sustainable trust (Ramírez et al., 2022; Thanasas et al., 2023; Yip et al., 2025).
- Agency theory emphasizes CSD's role in mitigating information asymmetry between managers and shareholders. Transparent cyber reporting signals managerial accountability and enables effective investor oversight in inherently opaque digital environments (Kiesow Cortez & Dekker, 2022; Alrfai et al., 2023).
- Signaling theory interprets voluntary disclosure as a reputational mechanism. By proactively communicating cyber strategies — even in the absence of crises — banks convey preparedness,

competence, and foresight, positively shaping investor sentiment and valuation (Gordon et al., 2010; Arroyabe et al., 2024).

Empirical studies validate these theoretical claims. CSD enhances performance in the Middle East and North Africa (MENA) banks (Elsayed et al., 2024), supports SME competitiveness in the United Kingdom (Hasani et al., 2023), and generates positive market reactions in China (Barry et al., 2022). Yet, evidence from European banking remains limited, despite heightened regulatory focus and the adoption of the DORA in 2023. The pre-DORA period (2014–2022), when disclosure was voluntary, presents a unique setting to assess whether CSD generates tangible financial value absent regulatory compulsion.

Building on this integrated theoretical foundation and addressing gaps in the literature, we propose the following hypothesis:

H1: Voluntary cybersecurity disclosure is positively associated with financial performance in the European banking sector.

3. RESEARCH METHODOLOGY

3.1. Research design

This study employs a longitudinal panel data design to explore the relationship between voluntary CSD and financial performance among European banks (Tabash et al., 2024). The use of panel econometrics allows us to control for unobserved heterogeneity across banks and to capture temporal dynamics over a nine-year period (2014–2022). We begin with pooled OLS and FE estimators and further address potential endogeneity and reverse causality by employing dynamic panel models, including two-step system GMM. These techniques are well-suited to correct for simultaneity bias and omitted variable bias, enhancing the robustness and validity of our empirical findings.

3.2. Sample and data description

The empirical analysis is based on an unbalanced panel of 5,742 bank-year observations drawn from 638 listed and unlisted banks operating across 25 European countries. The sample includes both large and small financial systems, capturing diverse institutional, regulatory, and digital maturity contexts. Table 1 presents the distribution of banks and observations by country. Countries with the largest representation include the Netherlands (43 banks), Sweden (39), France (38), and Switzerland (38), while the smallest samples are from Luxembourg and the Czech Republic (13 each), and Iceland (15). The dataset excludes Latvia, Cyprus, Slovakia, Malta, and Serbia due to missing or insufficient disclosure data in the Refinitiv database. Nonetheless, the sample covers over 90% of the EU banking sector by total assets and market capitalization, ensuring strong external validity.

Table 1. Distribution of European banks

No.	*Country*	*No. of bank*	*Obs.*	*No.*	*Country*	*No. of bank*	*Obs.*
1	Spain	24	216	14	Norway	24	216
2	Belgium	21	189	15	Finland	29	261
3	France	38	342	16	Austria	19	171
4	Germany	35	315	17	Poland	16	144
5	Italy	21	189	18	Czech Republic	13	117
6	Netherlands	43	387	19	Greece	31	279
7	Sweden	39	351	20	Romania	18	162
8	Switzerland	38	342	21	Slovenia	22	198
9	United Kingdom	36	324	22	Iceland	15	135
10	Ireland	34	306	23	Luxembourg	13	117
11	Portugal	14	126	24	Hungary	19	171
12	Denmark	34	306	25	Croatia	22	198
13	Estonia	20	180	Total		638	5742

CSD data, governance attributes, and financial metrics were extracted from the Refinitiv (Thomson Reuters) Eikon database, following methodologies similar to Alodat et al. (2025). The dependent variables are ROE and Tobin's Q, representing accounting-based and market-based performance measures, respectively. Independent variables include a binary indicator for CSD and a range of control variables covering size, leverage, profitability, capital adequacy, and macroeconomic factors. The data structure supports the use of advanced panel estimation methods to identify causality and evaluate robustness across multiple model specifications.

3.3. Contextual justification and relevance

Increasing cyber dangers and voluntary disclosure procedures in the absence of a disclosure obligation characterised the pre-regulatory European banking industry (2014–2022). The Tesco Bank hack in 2016, the ECB website penetration in 2019, ING and Dutch bank DDoS assaults in 2020, and the Revolut breach in 2022 were significant occurrences. These attacks highlighted systemic weaknesses and triggered cybersecurity governance reforms.

In 2023 (effective 2025), the European Commission established the DORA, requiring institutions to notify ICT events, undertake resilience testing, and monitor third-party ICT risks. DORA was outside the research window, but its policy evolution over time indicated institutional pressure and may have affected voluntary disclosures before legislation (Clausmeier, 2023; European Commission, 2022; ENISA, 2024).

Cyber threats have also evolved rapidly — from malware and phishing to complex ransomware campaigns, data theft, and attacks on critical financial infrastructure. The ENISA and the ECB have issued frequent warnings on the sophistication of threat actors, including state-sponsored cyber operations. These dynamics highlight the relevance of cybersecurity governance and make the analysis of voluntary CSD during this transitional regulatory phase especially timely and policy-relevant.

3.4. Variable measurement and definitions

This section outlines the construction and operationalization of the key variables used in this study, including the dependent, independent, and control variables. All data were sourced from the Refinitiv DataStream database and structured into a panel format for robust econometric analysis.

3.4.1. Dependent variables

To assess both accounting-based and market-based financial performance, we use two widely accepted metrics: return on equity (*ROE*) and Tobin's Q (*TobinQ*). ROE reflects a bank's internal efficiency and its ability to generate profits relative to shareholder equity (Alhasnawi et al., 2025). It is a major banking profitability statistic and widely used in performance benchmarking (Héroux & Fortin, 2020). Tobin's Q, the ratio of a bank's market value to its book value, measures investor confidence and market valuation (Gordon et al., 2010). A greater Tobin's Q signifies market optimism for growth and wealth development. Elsayed et al. (2024) show that merging accounting and market indicators provides a complete assessment of business performance in response to governance initiatives like CSD.

3.4.2. Independent variable

The key independent variable — *CSD* — is operationalized as a binary variable:

- *CSD* = 1 if a bank explicitly discloses cybersecurity-related risks, practices, or governance information in its annual report;
- *CSD* = 0 otherwise.

This binary measurement approach follows prior research (Mazumder & Hossain, 2023; Alodat et al., 2025), which highlights its reliability and practicality, especially in cross-country, large-sample studies where subjective scoring may introduce inconsistency.

Although simplistic, binary disclosure indicators are effective in signaling firm responsiveness to stakeholder expectations and regulatory pressures. Given the pre-DORA context of the study (2014–2022), when disclosures were voluntary, the presence of CSD is a strong indicator of strategic transparency. Scholars such as Gordon et al. (2010) and Cele and Kwenda (2025) affirm that binary proxies capture meaningful distinctions in disclosure behavior, especially when policy frameworks are evolving.

To enhance validity, we applied a manual content analysis approach to screen each annual report for the presence of keywords and narrative elements relating to:

- ICT risk and cybersecurity;
- cyber governance structures;
- resilience frameworks;
- and disclosure of past cyber incidents.

This binary coding was reviewed by two independent coders to ensure inter-rater reliability and reduce subjectivity.

3.4.3. Control variables

To ensure robust estimation and reduce omitted variable bias, we incorporate a comprehensive set of control variables informed by prior governance and finance literature (Kiesow Cortez & Dekker, 2022; Elsayed et al., 2024). These include corporate governance attributes, bank-specific financial characteristics, and macroeconomic indicators.

Governance variables comprise *AC_Expertise* (measured as the proportion of members with financial or information technology (IT) qualifications), *BGD* (percentage of female directors), *B_Independent* (board independence, proportion of non-executive directors), and *B_Skills* (a composite board skills index capturing competencies in finance, risk, and technology) — all recognized factors that influence oversight quality and strategic agility (Alodat et al., 2025; Al-Tahat et al., 2025; Firoozi & Mohsni, 2023).

Bank-specific controls include bank size *B_SIZE* (log of total assets), bank age *B_AGE* (years since incorporation), and financial leverage *B_LEV* (ratio of total liabilities to assets) (Smaili et al., 2023; Shubita et al., 2024; Berkman et al., 2018).

In addition, macroeconomic variables such as annual gross domestic product (*GDP*) growth and inflation (*INF*) are included at the country level to capture broad economic conditions that shape credit demand, interest margins, and profitability. To further account for structural and temporal heterogeneity, we introduce FE for country and year in all regression models. This allows us to isolate the effect of *CSD* from time-specific shocks and regulatory idiosyncrasies. Variable definitions and sources are presented in Table 2.

Table 2. Variables description and definitions (Part 1)

Variable type	*Variable name*	*Label*	*Definition*	*Reference*
Dependent variables	Return on equity	*ROE*	Ratio of net income to total shareholders' equity; reflects internal financial performance and profitability.	Héroux and Fortin (2020)
	Tobin's Q	*TobinQ*	Market value of the firm divided by the book value of its total assets; serves as a proxy for market valuation and investor perception.	Gordon et al. (2010)
Independent variables	Cybersecurity disclosure	*CSD*	Binary variable equal to 1 if the bank discloses any cybersecurity-related information in its annual report; 0 otherwise.	Mazumder and Hossain (2023)
	Cybersecurity disclosure (robustness)	*CSD**	Refined binary indicator based on the presence of narrative elements on ICT risk, cyber governance, resilience frameworks, and incident disclosures.	Cele and Kwenda (2025)
Control variables	Audit committee expertise	*AC_Expertise*	Dummy variable equal to 1 if the audit committee has at least three members, including one with financial or IT expertise; 0 otherwise.	Alshdaifat et al. (2024)
	Board gender diversity	*BGD*	Percentage of female directors on the board; a proxy for diversity in governance.	Alodat et al. (2025)

Table 2. Variables description and definitions (Part 2)

Variable type	*Variable name*	*Label*	*Definition*	*Reference*
Control variables	Board independence	*B_Independent*	Share of independent, non-executive directors on the board; reflects the strength of monitoring mechanisms.	Elsayed et al. (2024)
	Board skills index	*B_Skills*	Percentage of board members with relevant expertise in finance, risk management, or governance domains.	Firoozi and Mohsni (2023)
	Bank size	*B_SIZE*	Natural logarithm of total bank assets; reflects institutional scale and market position.	Berkman et al. (2018)
	Bank age	*B_AGE*	Natural logarithm of the number of years since the bank's founding; proxies organizational maturity and stability.	Smaili et al. (2023)
	Leverage	*B_LEV*	Ratio of total liabilities to total shareholders' equity; an indicator of financial risk.	Standard financial ratio
	GDP growth	*GDP*	Annual GDP growth rate (%) of the bank's country of operation; captures macroeconomic conditions.	World Bank Data
	Inflation rate	*INF*	Annual inflation rate (%) of the bank's country; reflects the monetary environment affecting real returns and pricing.	World Bank Data

3.5. Statistical model specification

The following model examines how *CSD* and governance factors influence the difference between ROE and Tobin's Q in European banks:

$$PERFORMANCE_{i,t} = \beta_0 + \beta_1 CSD_{i,t} + \beta_2 AC\_Expertise_{i,t} + \beta_3 BGD_{i,t} + \beta_4 B\_Independent_{i,t} + \beta_5 B\_Skills_{i,t} + \beta_6 B\_SIZE_{i,t} + \beta_7 B\_AGE_{i,t} + \beta_8 B\_LEV_{i,t} + \beta_9 GDP_{i,t} + \beta_{10} INF_{i,t} + \varepsilon_{i,t} \quad (1)$$

where, *PERFORMANCE* is the dependent variable that represents European banks' performance, evaluated using the ROE and Tobin's Q models. β_0 represents the constant, while β_{1-10} represent the slopes of the independent and control variables. $\varepsilon_{i,t}$ is the error term. The independent variable is the *CSD* of the bank (*i*) during the period (*t*).

The primary explanatory variable, *CSD*, is a binary variable coded as 1 if a bank discloses cybersecurity-related information in its annual report, and 0 otherwise. This qualitative scoring method, consistent with prior literature (Mazumder & Hossain, 2023; Saleh & Mansour, 2024), facilitates comparability across banks and jurisdictions that lack standardized disclosure regimes. Although binary scoring may lack granularity, it is particularly effective in cross-national panel designs, ensuring interpretive consistency without compromising analytical rigor (Gordon et al., 2010).

The model includes governance attributes such as *AC_Expertise, BGD, B_Independent*, and *B_Skills* — all shown to influence strategic oversight and disclosure practices. Bank-specific characteristics like *B_SIZE, B_AGE*, and *B_LEV* control for structural and financial heterogeneity. Country-level macroeconomic indicators — *GDP* and *INF* — are also included to account for external operating conditions.

To control for unobserved time-invariant country characteristics and period-specific shocks (e.g., regulatory developments, economic crises), the model incorporates country-FE and year-FE. This approach enhances internal validity by isolating within-bank variation over time from broader contextual fluctuations.

All variable definitions, coding procedures, and sources are detailed in Table 2. This specification serves as the foundation for further robustness checks and endogeneity-corrected estimations (e.g., system GMM) in subsequent sections.

3.6. Estimation techniques and robustness checks

To strengthen the internal validity of our findings and account for endogeneity concerns — including reverse causality, omitted variable bias, and unobserved heterogeneity — we employed two complementary econometric approaches: the system GMM and independent variable estimation.

System GMM is well-suited for dynamic panel data involving endogenous regressors and lagged dependent variables. It uses internal instruments derived from the lagged levels and first differences of the variables, helping to address simultaneity bias and dynamic endogeneity (Saleh et al., 2025). In our implementation, we applied the two-step system GMM estimator with Windmeijer's finite-sample correction to obtain robust standard errors and improve efficiency.

As a complementary approach, we applied independent variable regression to further address potential endogeneity in *CSD*. Here, we used exogenous regulatory events — such as the phased implementation of national cybersecurity frameworks and pre-DORA supervisory guidance — as instruments. These regulatory events influenced banks' voluntary disclosures but were not directly tied to their financial performance during the study period, satisfying both relevance and exclusion criteria. To assess the robustness of our results, we conducted multiple diagnostic checks:

- Variance inflation factors (VIFs): to detect and mitigate multicollinearity among regressors.
- Hansen J-test: to assess the validity of the over-identifying restrictions and instrument strength in the GMM specification.
- Arellano-Bond AR(2) test: to examine autocorrelation in the second-differenced residuals, ensuring that the instruments are not correlated with error terms.

By employing both static and dynamic estimation strategies and subjecting them to rigorous robustness tests, we ensure that our conclusions regarding the financial implications of *CSD* are credible, consistent, and resilient across specifications. This multifaceted methodology strengthens the causal interpretation of the observed relationships in the European banking context.

Beyond the baseline specifications employed in this study — pooled OLS, FE, and two-step

system GMM — several alternative empirical strategies would also be suitable for examining the CSD-performance nexus. For instance, panel quantile regressions could capture distributional heterogeneity in how *CSD* affects low- versus high-performing banks. At the same time, propensity score matching or difference-in-differences designs could further mitigate selection bias concerns related to voluntary disclosure. Shock-based identification strategies exploiting major cyber incidents or staggered regulatory reforms would enable stronger causal interpretation of *CSD* effects. Although these approaches lie beyond the scope of the present paper, they represent promising avenues for future research and complement the dynamic panel strategy adopted here.

4. RESEARCH RESULTS

4.1. Descriptive statistics

Table 3 summarizes the descriptive statistics of the study variables. The mean *ROE* is 8.7% (standard deviation (SD) = 4.5%), indicating moderate profitability with a slight left-skew. *TobinQ* averages 0.55, reflecting a moderate market valuation with mild skewness and kurtosis. *CSD* is reported by about 63% of banks, consistent with prior studies, though disclosure remains uneven.

Governance indicators show strong institutional structures: *AC_Expertise* is almost universal (mean = 0.84), *BGD* averages 32.8%, *B_Independent* 64%, and *B_Skills* 42.6%. *B_SIZE* size (mean log assets = 25.2) and *B_AGE* (mean = 34 years) vary widely, while *B_LEV* averages 1.66 but with high dispersion, indicating heterogeneity in financial risk.

Macroeconomic indicators exhibit substantial cross-country variation during the sample period. Average *GDP* growth is 1.9%, ranging from -4.2% to 6.8%, while inflation (*INF*) averages 2.3%, with values between 0.3% and 5.9%. This dispersion reflects the heterogeneous economic conditions across the 25 European countries included in the sample. The magnitude and variability of these macroeconomic controls are consistent with prior European panel studies, such as Chebbi (2025) and Clausmeier (2023), which similarly account for macroeconomic heterogeneity in cross-country financial analyses. Overall, all variables display acceptable distributional properties, supporting their suitability for regression analysis.

Table 3. Descriptive statistics

Variables	*Obs.*	*Mean*	*SD*	*Min*	*Max*	*Skew.*	*Kurt.*
ROE	5742	0.087	0.045	-0.15	0.23	-0.20	2.60
TobinQ	5742	0.548	0.893	0.028	2.834	-0.166	3.949
CSD	5742	0.628	0.488	0	1	-0.58	1.269
AC_Expertise	5742	0.835	0.342	0	1	-2.133	5.574
BGD	5742	32.801	10.853	14.287	51	-0.2133	2.042
B_Independent	5742	64.011	19.521	31	99	-0.071	2.266
B_Skills	5742	42.627	19.555	10.525	73.335	0.031	1.861
B_SIZE	5742	25.171	2.266	20.1	27.7	-0.157	2.201
B_AGE	5742	34.135	32.731	3	179	1.785	6.666
B_LEV	5742	1.663	1.943	0.0667	4.841	1.08	2.34
GDP	5742	1.900	1.200	-4.20	6.80	-0.10	2.00
INF	5742	2.300	1.600	0.30	5.90	0.20	1.80

Overall, the distributional properties of all variables — confirmed through skewness and kurtosis — fall within acceptable ranges for panel regression analysis. The variation across key measures, particularly in governance and disclosure, underscores the suitability of the dataset for investigating how *CSD* and board characteristics affect bank performance. The alignment with prior international studies supports external validity and enhances confidence in the generalizability of the results.

4.2. Bivariate correlations

Table 4 reports pairwise correlations among the main variables. *CSD* is positively correlated with both *ROE* ($r = 0.211$, $p < 0.001$) and *TobinQ* ($r = 0.155$, $p < 0.001$), supporting the argument that greater transparency enhances financial performance through reduced information asymmetry and stronger stakeholder trust.

Governance variables show expected patterns. *AC_Expertise* is strongly associated with both *ROE* and *TobinQ,* while *BGD* also shows positive effects. Board skills correlate positively with *ROE* but not with *CSD*, indicating that technical competence alone does not drive disclosure.

Bank size is positively linked to *ROE, TobinQ,* and *CSD*, suggesting larger institutions face stronger disclosure incentives. Bank age is positively correlated with performance, while leverage shows a mixed pattern — positively related to *CSD* but negatively to performance — implying that highly leveraged banks may use disclosure as a reputational tool.

Macroeconomic indicators behave as expected: *GDP* growth supports performance, while inflation correlates positively but may reflect omitted variable bias. Board independence shows no significant correlation with *CSD* or *ROE*, underscoring that independence alone is insufficient without complementary governance qualities.

Overall, the correlations provide preliminary evidence of a positive association between cybersecurity transparency, governance quality, and financial outcomes, laying the foundation for multivariate analysis.

Table 4. Pairwise correlations

Variables	*(1)*	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*	*(8)*	*(9)*	*(10)*	*(11)*	*(12)*
(1) *ROE*	1.000	-	-	-	-	-	-	-	-	-	-	-
(2) *TobinQ*	0.193* (0.002)	1.000	-	-	-	-	-	-	-	-	-	-
(3) *CSD*	0.155* (0.000)	0.211* (0.000)	1.000	-	-	-	-	-	-	-	-	-
(4) *AC_Expertise*	0.164* (0.000)	0.255* (0.000)	0.037 (0.37)	1.000	-	-	-	-	-	-	-	-
(5) *BGD*	0.176* (0.000)	0.143* (0.0021)	-0.022 (0.616)	0.118* (0.003)	1.000	-	-	-	-	-	-	-
(6) *B_Independent*	-0.015 (0.714)	0.124* (0.002)	0.003 (0.941)	0.042 (0.284)	0.101* (0.011)	1.000	-	-	-	-	-	-
(7) *B_Skills*	0.214* (0.000)	0.154* (0.000)	-0.007 (0.853)	0.381* (0.000)	-0.064 (0.106)	0.035 (0.381)	1.000	-	-	-	-	-
(8) *B_SIZE*	0.426* (0.000)	0.488* (0.000)	0.194* (0.000)	0.055 (0.243)	0.233* (0.000)	0.261* (0.000)	-0.021 (0.666)	1.000	-	-	-	-
(9) *B_AGE*	0.241* (0.000)	0.088* (0.033)	0.04 (0.29)	-0.044 (0.36)	0.091* (0.021)	-0.133* (0.001)	-0.033 (0.416)	0.262* (0.000)	1.000	-	-	-
(10) *B_LEV*	-0.069* 0.0031	-0.044* 0.0001	0.453 0.0000	0.121* 0.0000	0.111* 0.0000	0.046* 0.0211	0.042* 0.0365	0.11* 0.0000	-0.047* 0.02	1.000	-	-
(11) *GDP*	0.114* (0.087)	0.226* (0.094)	0.569 (0.155)	0.153 (0.110)	0.311 (0.113)	0.108 (0.110)	0.372 (0.106)	-0.216* (0.093)	0.113* (0.073)	0.066* (0.082)	1.000	-
(12) *INF*	0.551* (0.089)	0.440* (0.067)	0.527 (0.108)	0.088* (0.078)	0.192* (0.015)	0.084* (0.098)	0.274* (0.088)	0.207 (0.128)	0.114* (0.086)	-0.064 (0.181)	-0.226* (0.094)	1.000

*Note: * p < 0.05 (2-tailed).*

4.3. Multicollinearity assessment

Variance inflation factor diagnostics show no evidence of multicollinearity (mean VIF = 1.17; all values < 5). The highest VIF is 1.25 for leverage (*B_LEV*), followed by *AC_Expertise* (1.22) and *B_SIZE* (1.21), indicating only modest intercorrelation. Variables such as *CSD* (1.06), *BGD* (1.15), *B_Skills* (1.17), and *B_Independent* (1.11) present low redundancy, while macroeconomic controls (*GDP* = 1.18; *INF* = 1.16) also remain within safe limits. These results confirm that the regression models are free from multicollinearity concerns, ensuring reliable coefficient estimates without requiring variable exclusion or transformation (Khalaf et al., 2023).

Table 5. Variance inflation factor analysis

Variable	*VIF*	*1/VIF*
CSD	1.06	0.943
AC_Expertise	1.22	0.821
BGD	1.15	0.870
B_Independent	1.11	0.900
B_Skills	1.17	0.854
B_SIZE	1.21	0.827
B_AGE	1.05	0.953
B_LEV	1.25	0.800
GDP	1.18	0.847
INF	1.16	0.862
Mean VIF	1.17	—

4.4. Primary findings

Panel regression analysis examines the effect of CSD on the performance of banks across Europe. This baseline approach utilizes an estimation model primarily pooled OLS. Table 6 presents OLS regression results for *ROE* and *TobinQ*, examining the impact of *CSD* and governance variables on bank profitability. The F-test values (32.114 for *ROE*, 30.788 for *TobinQ*) and Prob. > F (0.000) confirms that both models are highly significant. The R-squared values (19.2% for *ROE*, 21.3% for *TobinQ*) indicate that the model explains a moderate portion of the variation in performance. CSD positively influences *ROE* (Coef. = 0.317) and *TobinQ* (Coef. = 0.233), both significant at the 1% level, indicating that increased *CSD* improves profitability and valuation. Thus, this result reinforces the *H1* hypothesis.

Governance factors also demonstrate positive and highly significant impacts on financial performance. This research supports stakeholder and agency theory propositions by demonstrating that *CSD* reduces information asymmetry (Barry et al., 2022), increases investor confidence (Gordon et al., 2010), and enhances governance effectiveness, leading to improved bank performance (Elsayed et al., 2024). Our finding — that transparent disclosure is positively linked to bank performance — aligns with signaling theory, as cybersecurity is viewed as a competitive edge and a means to build trust (Wang et al., 2024).

When considering governance factors, the analysis indicates that *AC_Expertise* positively influences *ROE* (Coef. = 0.199) and *TobinQ* (Coef. = 0.294), demonstrating that well-structured governance mechanisms contribute to financial performance. Similarly, *BGD* shows a positive and significant effect on *ROE* (Coef. = 0.221) and *TobinQ* (Coef. = 0.303), reinforcing the idea that diverse board compositions enhance decision-making and risk management. Our research confirms Kurnia and Ardianto's (2024) claim that a significant number of women on boards improves corporate social disclosures. The resource dependence and upper echelon theories support this conclusion. *B_Independent* also exhibits a positive relationship with *ROE* (Coef. = 0.205) and *TobinQ* (Coef. = 0.192), signifying that independent oversight strengthens profitability. Likewise, *B_Skills* contribute positively to both *ROE* (Coef. = 0.163) and *TobinQ* (Coef. = 0.144), highlighting the importance of financial and governance expertise in banking performance. Conversely, *B_SIZE* negatively affects both *ROE* (Coef. = -0.076) and *TobinQ* (Coef. = -0.087), indicating that operational inefficiencies may arise in larger institutions. *B_AGE* demonstrates a positive relationship with both indicators, while *B_LEV* maintains a negative correlation with profitability. Finally, *GDP* shows a positive association with bank performance, while inflation (*INF*) displays a slight negative effect.

Table 6. Panel regression results for ROE and Tobin's Q

Variables	*Pooled OLS model*		*FE model*	
	ROE	*TobinQ*	*ROE*	*TobinQ*
	Coef. (SE)	*Coef. (SE)*	*Coef. (SE)*	*Coef. (SE)*
CSD	0.317*** (0.0495)	0.233*** (0.0882)	0.395*** (0.093)	0.288*** (0.1342)
AC_Expertise	0.199*** (0.0384)	0.294*** (0.0263)	0.189*** (0.039)	0.431*** (0.087)
BGD	0.221*** (0.0672)	0.303*** (0.0275)	0.065*** (0.0155)	0.091*** (0.0142)
B_Independent	0.205*** (0.0520)	0.192*** (0.0761)	0.041*** (0.0068)	0.034*** (0.0062)
B_Skills	0.163*** (0.0359)	0.144*** (0.0286)	0.109* (0.0492)	0.093*** (0.0158)
B_SIZE	-0.076** (0.0135)	-0.087*** (0.0297)	-0.084*** (0.0127)	-0.071*** (0.0105)
B_AGE	0.312* (0.1991)	0.144* (0.0932)	0.208** (0.0823)	0.325*** (0.0241)
B_LEV	-0.054** (0.0251)	-0.095*** (0.0234)	-0.148*** (0.0240)	-0.201*** (0.0233)
GDP	0.057** (0.0266)	0.069** (0.0311)	0.051** (0.0213)	0.073** (0.0286)
INF	-0.038* (0.0244)	-0.058** (0.0298)	-0.042* (0.0221)	-0.061** (0.0254)
Constant	0.193*** (0.0145)	2.146*** (0.6110)	3.391*** (0.4972)	3.455*** (0.4743)
Year FE	✓	✓	✓	✓
Country FE	✓	✓	✓	✓
F-statistic	32.114	30.788	218.309	327.643
Prob. > F	0.000	0.000	0.000	0.000
R^2	0.192	0.213	-	-
Within-R^2	-	-	42.6%	37.2%
Breusch & Pagan	-	-	99.75***	109.84***
Hausman test	-	-	77.32***	35.91***
No. of groups	638	638	638	638
Observations	5,742	5,742	5,742	5,742

*Note: Standard errors are in parentheses, *** p < 0.01, ** p < 0.05, * p < 0.1.*

4.5. Fixed-effects model validation

This study conducts an additional test using the FE model to ensure the robustness of outcomes. Table 6 also presents the FE regression results, accounting for unobserved heterogeneity across European banks. The model integrates country and year-FE, enhancing its reliability in capturing temporal and geographic-specific dynamics.

To determine the best-fitting model, both the Breusch-Pagan and Hausman tests were applied. The Breusch-Pagan test results (99.75 for *ROE* and 109.84 for *TobinQ*, $p < 0.01$) suggest heteroscedasticity, indicating the need to move beyond pooled OLS estimation. The Hausman test results (77.32 for *ROE* and 35.91 for *TobinQ*, $p < 0.01$) confirm that the FE model is preferable over random effects, as it effectively controls for time-invariant omitted variables.

Results demonstrate that *CSD* has a positive and significant impact on both *ROE* (Coef. = 0.395, $p < 0.01$) and *TobinQ* (Coef. = 0.288, $p < 0.01$), reinforcing the earlier findings and supporting *H1*. This implies that enhanced *CSD* strengthens both profitability and market value.

Among governance variables, *AC_Expertise* exerts a strong influence on *ROE* (0.189, $p < 0.01$) and *TobinQ* (0.431, $p < 0.01$), highlighting the value of specialized oversight. Similarly, *BGD* shows robust significance (*ROE*: 0.065, $p < 0.01$; *TobinQ*: 0.091, $p < 0.01$), confirming the positive effects of board diversity. *B_Independent* remains statistically significant across both models (*ROE*: 0.041, $p < 0.01$; *TobinQ*: 0.034, $p < 0.01$), affirming the contribution of independent directors to performance monitoring. *B_Skills* positively correlates with *ROE* (0.109, $p < 0.1$) and *TobinQ* (0.093, $p < 0.01$), underlining the role of board expertise.

Conversely, *B_SIZE* has a significant negative effect (*ROE*: -0.084, *TobinQ*: -0.071; $p < 0.01$), likely reflecting coordination costs and inefficiencies in larger institutions. *B_AGE* remains positively associated with performance (*ROE*: 0.208, $p < 0.05$; *TobinQ*: 0.325, $p < 0.01$), consistent with institutional maturity and operational experience. Importantly, *B_LEV* is negatively significant in both models (*ROE*: -0.148, *TobinQ*: -0.201; $p < 0.01$), indicating that higher leverage erodes firm performance.

Among macroeconomic controls, *GDP* positively influences outcomes (*ROE*: 0.051, *TobinQ*: 0.073; $p < 0.05$), while *INF* retains a modest but statistically significant negative impact (*ROE*: -0.042, *TobinQ*: -0.061; $p < 0.1$ and $p < 0.05$, respectively), indicating inflationary pressure's dampening effect on profitability. These results validate earlier OLS findings while providing a more conservative estimation framework, confirming that cyber transparency and governance continue to be central to bank performance across Europe.

4.6. Robustness checks: System GMM estimation

To address potential endogeneity arising from self-selection, omitted variable bias, and reverse causality, this study employs system GMM estimation. While FE models account for unobserved heterogeneity, they do not capture the dynamic nature of firm behavior and performance

(Mazumder & Hossain, 2023). In contrast, system GMM provides a robust framework that addresses endogeneity and autocorrelation by using internal instruments — specifically, lagged levels and differences of endogenous variables.

Given that past profitability may influence current financial performance, lagged dependent variables (ROE_{t-1} and $TobinQ_{t-1}$) are included as regressors. Moreover, variables such as *CSD* and governance attributes (e.g., *AC_Expertise, BGD*) are potentially endogenous due to firm-specific strategies and unobservable factors (Alodat et al., 2025; Héroux & Fortin, 2020). Therefore, we treat these as endogenous and instrument them accordingly. Macroeconomic variables (*GDP* and *INF*) are treated as exogenous, consistent with prior studies (Karyani et al., 2024; Kiesow Cortez & Dekker, 2022).

Table 7. Results of system GMM estimation

Variables	*ROE*	*TobinQ*
	Coef. (t-stat)	*Coef. (t-stat)*
ROE_{t-1}	0.274 (3.688***)	0.217 (3.105***)
$TobinQ_{t-1}$	0.384 (4.027***)	0.593 (4.106***)
CSD	0.0412 (2.759**)	0.0385 (3.419***)
AC_Expertise	0.398 (3.224***)	0.549 (3.674***)
BGD	0.0145 (4.283***)	0.0724 (3.241***)
B_Independent	0.0367 (3.801***)	0.0489 (3.695***)
B_Skills	0.182 (1.942*)	0.1195 (3.771***)
B_SIZE	-0.0627 (3.007***)	-0.0408 (2.387**)
B_AGE	0.588 (5.002***)	0.423 (4.416***)
B_LEV	-0.0725 (3.013***)	-0.0973 (4.982***)
GDP	0.0486 (2.814**)	0.0622 (3.055**)
INF	-0.0364 (2.249**)	-0.0457 (2.693**)
Constant	0.0714 (3.502***)	0.0217 (2.158**)
Year FE	✓	✓
Country FE	✓	✓
Hansen J. (p)	0.294	0.357
AR(1) (p)	0.007***	0.005***
AR(2) (p)	0.662	0.741
Instruments	115	121
Groups	638	638
Obs.	5742	5742

*Note: *** p < 0.01, ** p < 0.05, * p < 0.1.*

As shown in Table 7, the lagged dependent variables are positive and significant, confirming performance persistence, a dynamic characteristic well established in bank performance literature (Héroux & Fortin, 2020). Both the lagged and current values of *CSD* are statistically significant, reinforcing the hypothesis that *CSD* improves both short-term and long-term financial performance. These findings are consistent with Elsayed et al. (2024), who found that increased transparency enhances firm value, and Arroyabe et al. (2024), who noted CSD's signaling role in financial markets.

Governance variables also behave as theoretically expected. *AC_Expertise, BGD*, and *B_Independent* exert significant positive effects on *ROE* and *TobinQ,* consistent with the resource dependence and upper echelon theories (Alodat et al., 2025; Radu & Smaili, 2022). The negative coefficients of *B_SIZE* and *B_LEV* reflect structural inefficiencies and financial constraints associated with large or highly leveraged banks (Ramírez et al., 2022). *B_AGE*'s strong positive effect is consistent with findings by Kiesow Cortez and Dekker (2022), suggesting experienced boards foster financial resilience. Macroeconomic variables — *GDP* and *INF* — also show consistent directional effects: economic growth enhances performance, while inflation exerts a dampening impact, in line with Karyani et al. (2024).

Instrument validity is confirmed by the Hansen J-statistic ($p > 0.10$), indicating that overidentifying restrictions are not violated. AR(1) results show expected first-order serial correlation, while AR(2) results suggest the absence of second-order serial correlation. The number of instruments is well below the number of groups, mitigating concerns of overfitting.

In summary, the system GMM estimation validates the core findings from OLS and FE models. *CSD* significantly and positively influences financial performance, both contemporaneously and over time. Moreover, strong board governance structures amplify these effects, reinforcing the strategic and regulatory importance of transparency in cybersecurity reporting across the European banking sector.

4.7. Heterogeneous effects: Bank risk profile

To investigate whether the impact of *CSD* on bank performance differs based on institutional risk exposure, we conduct a subgroup analysis using financial leverage as a proxy for bank risk. Leverage represents a critical indicator of financial vulnerability, with highly leveraged banks being more exposed to external shocks, funding constraints, and investor scrutiny (Elsayed et al., 2024; Héroux & Fortin, 2020). In such settings, cybersecurity transparency may serve as a strategic signaling mechanism to reduce perceived risks and reinforce stakeholder trust.

We divide the sample into two groups — high-leverage and low-leverage banks — based on the median value of the leverage ratio (*B_LEV*) across the sample period. Separate system GMM estimations are conducted for each group using the same dynamic specification to assess whether the relationship between *CSD* and financial performance differs according to risk exposure.

Table 8. System GMM estimation: Heterogeneous effects based on high vs. low leverage

Variables	*ROE*		*TobinQ*	
	High-leverage	*Low-leverage*	*High-leverage*	*Low-leverage*
CSD	0.049*** (0.0116)	0.021* (0.0123)	0.081*** (0.0141)	0.033** (0.0149)
AC_Expertise	0.382*** (0.0675)	0.295** (0.1252)	0.441*** (0.0718)	0.328*** (0.0853)
BGD	0.059*** (0.0124)	0.046*** (0.0139)	0.071*** (0.0113)	0.054** (0.0251)
B_Independent	0.033*** (0.0078)	0.029*** (0.0084)	0.041*** (0.0092)	0.037*** (0.0088)
B_Skills	0.097* (0.0524)	0.076 (0.0611)	0.103** (0.0486)	0.082 (0.0572)
B_SIZE	-0.077*** (0.0142)	-0.061** (0.0171)	-0.069*** (0.0184)	-0.053** (0.0215)
B_AGE	0.212*** (0.0634)	0.195** (0.0798)	0.334*** (0.0542)	0.288*** (0.0697)
B_LEV	-0.101*** (0.0227)	-0.062** (0.0244)	-0.123*** (0.0213)	-0.058** (0.0252)
GDP	0.049** (0.0205)	0.036** (0.0183)	0.061** (0.0232)	0.042** (0.0211)
INF	-0.037** (0.0178)	-0.033* (0.0192)	-0.045** (0.0187)	-0.041* (0.0229)
Constant	0.079*** (0.0276)	0.065*** (0.0292)	0.023** (0.0111)	0.018* (0.0104)
Year FE	✓	✓	✓	✓
Country FE	✓	✓	✓	✓
Hansen J. (p)	0.281	0.306	0.344	0.328
AR(1) (p)	0.008***	0.010***	0.006***	0.009***
AR(2) (p)	0.681	0.725	0.748	0.739
Instruments	57	63	59	64
Groups	314	324	314	324
Observations	2,854	2,888	2,854	2,888

*Note: Standard errors in parentheses, *** p < 0.01, ** p < 0.05, * p < 0.1. All models include robust standard errors clustered at the bank level.*

Table 8 presents the results, revealing a stronger and more statistically significant association between *CSD* and financial performance among high-leverage banks. Specifically, for *ROE*, the coefficient of *CSD* is 0.049 ($p < 0.01$) for high-leverage institutions, compared to 0.021 ($p < 0.10$) for their low-leverage counterparts. A similar pattern is observed for Tobin's Q, where the effect of *CSD* is more pronounced in high-leverage banks (0.081, $p < 0.01$) than in low-leverage banks (0.033, $p < 0.05$).

These results suggest that the marginal value of cybersecurity transparency increases with financial risk. In highly leveraged banks, greater disclosure of cybersecurity practices likely helps mitigate stakeholder concerns related to default risk and operational resilience, thereby enhancing firm valuation and profitability. This supports the predictions of signaling theory, which posits that voluntary disclosure reduces information asymmetry in high-risk contexts (Gordon et al., 2010), and aligns with agency theory, where greater transparency disciplines managerial behavior and reassures external investors (Alodat et al., 2025).

This heterogeneous effect reinforces the importance of tailoring cybersecurity governance to the institution's financial structure and stakeholder expectations, especially under conditions of heightened leverage-related risk.

5. DISCUSSION

The empirical evidence from this study indicates that voluntary CSD plays a financially valuable role in the European banking sector. Both profitability (as measured by ROE) and market valuation (via Tobin's Q) are positively and significantly associated with increased levels of CSD across pooled OLS, FE, and system GMM estimations. These findings strongly suggest that CSD functions as more than symbolic compliance; it is a strategic governance mechanism that enhances both internal performance and external stakeholder perceptions.

This is consistent with signaling theory, which posits that firms disclose private information to differentiate themselves in uncertain environments. In the context of cybersecurity, where asymmetries in risk knowledge are common, voluntary disclosure signals digital maturity and resilience. Vo and Pham (2025) found that firms facing higher cyber risk or financial fragility strategically use optimistic disclosures to reassure markets. Similarly, Chen et al. (2023) demonstrated that such disclosures reduce investor uncertainty and increase information informativeness, validating our interpretation that CSD serves as a commitment device and risk-mitigating tool (Héroux & Fortin, 2025).

These effects are further reinforced by corporate governance mechanisms. Our results show that board and audit committee characteristics — specifically expertise, diversity, and skills — amplify the financial value of CSD. Guohong et al. (2025) confirm that audit committees with cybersecurity expertise significantly improve the quality of disclosure. Radu and Smaili (2022) find that gender diversity, particularly when a critical mass is achieved, enhances board attentiveness to cyber risks. Meanwhile, Smaili et al. (2023) and Alodat et al. (2025) show that independent and financially literate boards are more likely to support transparent cyber governance frameworks. These governance variables work as enablers of effective disclosure, increasing both credibility and substance.

However, size-related variables exhibit a different dynamic. Both board size and bank size

are negatively associated with performance, which is in line with Héroux and Fortin (2024), who suggest that larger institutions often suffer from coordination costs and diluted accountability. This result indicates that governance effectiveness, not structural size, is what truly matters in cybersecurity oversight. This distinction is crucial, especially in institutions where the complexity of operations can obscure lines of responsibility in cyber risk management.

One of the study's most revealing insights comes from the heterogeneity analysis: banks with higher leverage experience greater marginal benefits from voluntary CSD. This suggests that firms with higher risk exposure use disclosure to reassure creditors and investors, consistent with agency theory. Masoud and Al-Utaibi (2022) found that post-breach disclosure is often more intense in firms that already suffer from low financial reporting quality, making CSD a reputational hedge. However, as Karyani et al. (2024) caution, disclosure without strong internal resilience can backfire, weakening performance. Thus, disclosure must be supported by genuine cyber governance capabilities.

These findings must be contextualized within the pre-DORA environment (2014–2022), where CSD across the EU banking sector was largely voluntary and non-standardized. Despite this lack of regulatory enforcement, many institutions disclosed proactively and were rewarded for it — highlighting that disclosure was driven by internal governance logic and market incentives rather than compliance. With the DORA coming into force in 2025, these findings provide a critical benchmark. As noted by Clausmeier (2023) and Calliess and Baumgarten (2020), DORA seeks to unify operational resilience disclosures across the EU. However, as regulatory mandates grow, there is a risk that strategic voluntary signaling — now shown to have positive financial effects — may diminish.

CSD is not only a matter of financial and operational strategy; it increasingly plays a role in ESG and corporate ethics. Khan et al. (2025) and Chebbi (2025) reframe CSD as part of a firm's social responsibility to stakeholders, particularly in data-sensitive industries like finance. Their findings align with ours: that cyber transparency generates reputational capital and strengthens stakeholder trust, both of which contribute to financial performance. This links well with stakeholder theory, which argues that firms accrue legitimacy and long-term value by responding to broader social expectations. Our results indicate that such ESG-oriented disclosure is not only ethically commendable but economically rational.

This study contributes to a growing body of work that repositions cybersecurity governance as central to financial performance. It empirically confirms the theoretical claims of signaling, agency, and stakeholder perspectives, while highlighting the conditions under which voluntary disclosure is most valuable. Specifically, well-governed and high-leverage banks gain the most from CSD. These insights are validated by recent evidence from Tan et al. (2025), Trinh et al. (2025), and others, making a compelling case for firms and regulators to consider disclosure not merely as a compliance requirement but as a core component of corporate governance and financial strategy.

6. CONCLUSION

This study investigates the financial relevance of voluntary CSD in the European banking sector from 2014 to 2022 — a period of regulatory transition prior to the enforcement of the DORA. Using robust econometric methods, including system GMM estimation, the results reveal that banks engaging in higher levels of CSD experience superior financial outcomes, both in terms of ROE and market valuation (Tobin's Q). These results indicate that CSD is not merely a compliance tool but a strategic asset with quantifiable economic value.

The analysis shows that effective disclosure contributes to reducing information asymmetries (agency theory), builds market confidence through signaling operational maturity (signaling theory), and strengthens stakeholder trust in line with ESG expectations (stakeholder theory). Additionally, the value of disclosure is shown to be amplified in firms with strong internal governance mechanisms — particularly those with technically proficient, diverse, and independent boards. This reinforces the role of cybersecurity governance as a performance-enhancing corporate function rather than a risk-aversion formality.

Importantly, the study reveals heterogeneous effects based on institutional risk profiles. Banks with higher leverage — a proxy for heightened financial risk — derive greater marginal benefits from voluntary disclosure. This indicates that CSD acts as a reputational and strategic buffer, especially where firm vulnerability is more visible to capital markets. However, the sustainability of such benefits depends on whether disclosure is matched with actual cyber resilience and board-level accountability.

The findings have several important policy implications. First, they offer empirical support for regulatory efforts such as DORA by demonstrating the financial materiality of cybersecurity governance and disclosure. However, the results also caution against fully eliminating the discretionary nature of disclosure. Voluntary CSD currently functions not only as a transparency tool but also as a strategic differentiator among firms. Thus, regulatory frameworks should aim for balance — providing standardized minimum requirements while leaving room for firms to tailor enhanced disclosures based on their governance capacity, risk exposure, and stakeholder expectations.

Second, regulators and industry bodies should prioritize board-level capacity-building. The positive role of audit committee expertise and board gender diversity in driving effective CSD suggests that policy efforts to professionalize board governance — especially around cyber risk — can indirectly improve disclosure quality and financial stability. Third, there is scope for integrating CSD metrics into broader ESG and prudential supervision frameworks. Doing so would align cyber governance with sustainable finance objectives and risk-based oversight models already evolving across the European regulatory landscape.

This study is not without limitations. First, it focuses on listed European banks, limiting generalizability to smaller or non-listed institutions and other sectors. Second, although the study uses rigorous econometric techniques, it cannot fully account for unobserved variables influencing both

disclosure and performance. Third, the measurement of CSD remains challenging due to the lack of standardized indices, and future research would benefit from integrating more granular disclosure quality metrics or natural language processing techniques.

Looking ahead, future studies should examine the post-DORA era to evaluate how mandatory compliance affects disclosure behavior, market perceptions, and firm performance. Comparative studies across jurisdictions — particularly between regulated and lightly regulated environments — could provide further insight into the optimal design of CSD mandates. Moreover, integrating CSD within ESG scoring systems and examining its role in credit risk modeling, insurance pricing, or shareholder activism would extend the understanding of cybersecurity's evolving role in corporate finance.

This study concludes that voluntary CSD is both a governance signal and a financial asset. When coupled with effective board oversight and strategic intent, CSD enhances corporate transparency, stakeholder confidence, and market valuation. As financial institutions confront escalating digital threats and stricter regulatory environments, cybersecurity governance must transition from a compliance checkbox to a boardroom priority.

REFERENCES

Alhasnawi, M. Y., Alshdaifat, S. M., Mansour, M., Saleh, M. W., & Hu, G. (2025). How does performance-based budgeting enhance sustainable performance? A mediated-moderated model of innovation and information quality. *International Journal of Innovation Science*. Advance online publication. https://doi.org/10.1108/IJIS-08-2025-0418

Alodat, A. Y., Hao, Y., Nobanee, H., Ali, H., Mansour, M., & Al Amosh, H. (2025). Board characteristics and cybersecurity disclosure: Evidence from the UK. *Electronic Commerce Research, 25*, 4717–4735. https://doi.org/10.1007/s10660-024-09867-w

Alrfai, M. M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., & Almaiah, M. A. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. *Cogent Social Sciences, 9*(2), Article 2243719. https://doi.org/10.1080/23311886.2023.2243719

Alsadoun, A. A., & Albaz, M. M. (2025). The impact of cybersecurity risk disclosure and governance on firm value and stock return volatility. *Journal of Governance & Regulation, 14*(1), 194–205. https://doi.org/10.22495/jgrv14i1art18

Alshdaifat, S. M., Saleh, M. W. A., Mansour, M., Khassawneh, A., Shubita, M. F., Hanaysha, J. R., Al-Matari, E. M., Qamhan, M. A., & Alrawad, M. (2024). Audit committee effectiveness in times of crisis: Empirical insights on key audit matters disclosure. *Heritage and Sustainable Development*, *6*(2), 845–860. https://doi.org/10.37868/hsd.v6i2.860

Al-Tahat, S., Bani-Khaled, S., Jaradat, Z., Mansour, M., & Al-zoubi, A. M. (2025). State ownership as a moderator in the relationship between board characteristics and ESG performance: Evidence from Asia-Pacific markets. *Journal of Business and Socio-economic Development*. Advance online publication. https://doi.org/10.1108/JBSED-05-2025-0145

Arroyabe, M. F., Arranz, C. F. A., Fernandez de Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society, 78*, Article 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. *Journal of Accounting and Public Policy, 41*(6), Article 106998. https://doi.org/10.1016/j.jaccpubpol.2022.106998

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU. The example of the financial sector: A legal perspective. *German Law Journal, 21*(6), 1149–1179. https://doi.org/10.1017/glj.2020.67

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime, 32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Chebbi, K. (2025). The impact of cyber threats on environmental, social, and governance performance. *Journal of Environmental Management, 389*, Article 126184. https://doi.org/10.1016/j.jenvman.2025.126184

Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics, 187*(1), 199–224. https://doi.org/10.1007/s10551-022-05107-z

Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review, 4*(1), 79–90. https://doi.org/10.1365/s43439-022-00076-5

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*(1), Article 115. https://doi.org/10.1186/s43093-024-00402-9

European Banking Authority (EBA). (2022). *Report on the peer review on ICT risk assessment under the SREP* (EBA/REP/2022/25). https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2022/1041612/Peer%20Review%20Report%20on%20ICT%20Risk%20assessment%20under%20the%20SREP.pdf

European Central Bank (ECB). (n.d.). *Cyber resilience strategy for financial market infrastructures: Pillar 1*. https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews180502.en.html

European Commission. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014 and (EU) 2016/1011. *Official Journal of the European Union, 333*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR

European Union Agency for Cybersecurity (ENISA). (2024). *ENISA threat landscape: Financial sector.* Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector

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

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly, 34*(3), 567–594. https://doi.org/10.2307/25750692

Guohong, Z., Zhongwei, X., Feng, H., & Zhongyi, X. (2025). The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk. *Research in International Business and Finance, 73*(Part A), Article 102542. https://doi.org/10.1016/j.ribaf.2024.102542

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics, 3*(5), Article 97. https://doi.org/10.1007/s43546-023-00477-6

Héroux, S., & Fortin, A. (2020). Cybersecurity disclosure by the companies on the S&P/TSX 60 Index. *Accounting Perspectives, 19*(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Héroux, S., & Fortin, A. (2024). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance, 28*(2), 359–404. https://doi.org/10.1007/s10997-022-09660-7

Héroux, S., & Fortin, A. (2025). How the three lines of defense can contribute to public firms' cybersecurity effectiveness. *International Journal of Disclosure and Governance, 22*(2), 377–396. https://doi.org/10.1057/s41310-024-00226-7

Kanyongo, G., & Wadesango, N. (2025). Impact of cybersecurity on risk mitigation strategy by commercial banks in emerging markets: A legal perspective case study. *Corporate Law & Governance Review, 7*(1), 28–37. https://doi.org/10.22495/clgrv7i1p3

Karyani, E., Faturohman, T., Noveria, A., & Rahadi, R. A. (2024). Financial resilience in ASEAN-4 banking sector: Impact of cyber risk disclosure. *Kasetsart Journal of Social Sciences, 45*(3), 901–914. https://doi.org/10.34044/j.kjss.2024.45.3.20

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University — Computer and Information Sciences, 34*(8, Part B), 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018

Khalaf, A. M., Ismail, W. N. B. W., Marei, A., Saleh, M. W. A., & Mansour, M. M. (2023). The framework for system trust's effect on the organizational commitment in the Jordanian public sector. *SciPap, 31*(2). https://doi.org/10.46585/sp31021696

Khan, W. N., Lee, J. K., & Liu, S. (2025). Is cybersecurity a social responsibility? *Information Systems Frontiers, 27*, 1367–1391. https://doi.org/10.1007/s10796-024-10565-z

Kiesow Cortez, E., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation, 13*(3), 443–463. https://doi.org/10.1017/err.2022.10

Kurnia, P., & Ardianto. (2024). Board gender diversity and cyber security disclosure in the Indonesian banking industry: A two-tier governance context. *Corporate Governance, 24*(7), 1614–1637. https://doi.org/10.1108/CG-01-2023-0010

Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics, 76*(2), 131–140. https://doi.org/10.1016/j.rie.2022.07.001

Matemane, R., Denhere, V., Mokabane, M., & Ojeyinka, T. A. (2024). Cybersecurity risk disclosure, board characteristics, and firm performance in the fourth industrial revolution era: Evidence from an emerging economy. *African Finance Journal, 26*(1), 34–53. https://hdl.handle.net/10520/ejc-finj_v26_n1_a2

Mazumder, M. M. 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

Radu, C., & Smaili, N. (2022). Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics, 177*(2), 351–374. https://doi.org/10.1007/s10551-020-04717-9

Ramírez, M., Rodríguez Ariza, L., Gómez Miranda, M. E., & Vartika. (2022). The disclosures of information on cybersecurity in listed companies in Latin America — Proposal for a cybersecurity disclosure index. *Sustainability, 14*(3), Article 1390. https://doi.org/10.3390/su14031390

Saleh, M. W. A., & Mansour, M. (2024). Is audit committee busyness associated with earnings management? The moderating role of foreign ownership. *Accounting Research Journal, 37*(1), 80–97. https://doi.org/10.1108/ARJ-04-2023-0106

Saleh, M. W. A., Alshdaifat, S. M., Shubita, M. F., Mansour, M., & Lutfi, A. (2025). Gender diversity and environmental, social, and governance: Unlocking solutions to corporate risk. *Business Strategy & Development, 8*(1), Article e70097. https://doi.org/10.1002/bsd2.70097

Shubita, M. F., Mansour, M., Saleh, M. W. A., Lutfi, A., Saad, M., & Shubita, D. (2024). Impact of advertising and sales promotion expenses on the sales performance of Jordanian companies: The moderating role of firm size. *Innovative Marketing, 20*(4), 146–157. https://doi.org/10.21511/im.20(4).2024.13

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

Tabash, M. I., AsadUllah, M., Siddiq, Q., Mansour, M., Daniel, L. N., & Al-Absy, M. S. M. (2024). Symmetries or asymmetries: How MSCI index advanced European markets' exchange rates respond to macro-economic fundamentals. *Economies, 12*(12), Article 326. https://doi.org/10.3390/economies12120326

Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal, 90*, Article 102646. https://doi.org/10.1016/j.pacfin.2024.102646

Thanasas, G. L., Slimistinou, A., Kontogeorga, G., & Lampropoulos, S. (2023). Environmental taxation as a boost mechanism for European Union green growth: The Greek response. *Risk Governance and Control: Financial Markets & Institutions, 13*(1), 8–15. https://doi.org/10.22495/rgcv13i1p1

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis, 76*, Article 101795. https://doi.org/10.1016/j.irfa.2021.101795

Trinh, V. Q., Elnahass, M., & Pasiouras, F. (2025). Personal traits of CEOs and cybersecurity-related disclosure. *Journal of International Accounting, Auditing and Taxation, 58*, Article 100680. https://doi.org/10.1016/j.intaccaudtax.2025.100680

Vo, H., & Pham, M. D. (2025). Beware of false prophets: Cybersecurity risk and strategic voluntary disclosure. *The British Accounting Review*, Article 101578. https://doi.org/10.1016/j.bar.2025.101578

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security, 147*, Article 104051. https://doi.org/10.1016/j.cose.2024.104051

Xing, Y., Yeoh, K. K., & Jaafar, A. R. (2025). Unpacking the drivers of innovation performance: The interplay between managerial, relational, technological, and learning capabilities with innovation strategy. *Business Performance Review, 3*(1), 105–116. https://doi.org/10.22495/bprv3i1p10

Yip, P. C. W., Pang, E., & Yu, T. T. K. (2025). The integration of environmental, social, and governance metrics and market value: A multi-dimensional analysis of corporate sustainability and financial performance. *Corporate Governance and Sustainability Review, 9*(3), 145–154. https://doi.org/10.22495/cgsrv9i3p12