THE IMPACT OF CYBERSECURITY RISK DISCLOSURE AND GOVERNANCE ON FIRM VALUE AND STOCK RETURN VOLATILITY

Abdullah A. Alsadoun [*], Maged M. Albaz [**]

[*] Department of Business Administration, College of Business Administration, Majmaah University, Al-Majma'ah, Saudi Arabia
[**] *Corresponding author,* Department of Accounting, College of Business Administration, Majmaah University, Al-Majma'ah, Saudi Arabia; Accounting Department, Faculty of Commerce, Suez Canal University, Ismailia, Egypt
Contact details: Department of Accounting, College of Business Administration, Majmaah University, Al-Majma'ah 11952, Saudi Arabia

OPEN ACCESS

How to cite this paper: 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

ISSN Online: 2306-6784
ISSN Print: 2220-9352

Received: 26.03.2024
Accepted: 21.01.2025

JEL Classification: M0, M1, M4, M40, M41
DOI: 10.22495/jgrv14i1art18

Abstract

The research aims to analyze the determinants of cybersecurity risk disclosure (CSRD) in Saudi Arabia and discover the influence of CSRD on both firm value and stock return volatility. The study used a mixed-methods approach that combines qualitative and quantitative techniques to determine the relationships used by the content analysis method to analyze the annual financial reports of Saudi firms for the period from 2015 to 2022, to estimate the volume of CSRD, firm value, and stock return volatility. The results of the study show that the impact of a firm's size, age, leverage, and profitability are positive and significant on CSRD. In contrast, free cash flow has no significant effect on CSRD. Moreover, a curvilinear relationship exists between operating expenses and CSRD. In addition, Firm value is positively and significantly correlated with CSRD and many firm characteristics. However, stock return volatility is negatively and significantly correlated with CSRD in the Saudi business environment.

Keywords: Cybersecurity, Risk Disclosure, Firm Value, Stock Return Volatility, Saudi Arabia

Authors' individual contribution: Conceptualization — A.A.A. and M.M.A.; Methodology — M.M.A.; Formal Analysis — A.A.A.; Investigation — M.M.A.; Writing — Original Draft — M.M.A.; Writing — Review & Editing — A.A.A. and M.M.A.; Supervision — A.A.A.

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

Acknowledgements: The Authors extend their appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through Project No. R-2025-1524.

1. INTRODUCTION

In today's increasingly digital era, cybersecurity risks (CSR) have emerged as a major threat to firms (Masoud & Al-Utaibi, 2022), where cybersecurity breaches can result in many negative consequences, including financial losses, reputational damage, and legal liability. As a result, firms are increasingly interested in handling, managing, and disclosing CSR as a major part of the annual financial reporting (Calderon & Gao, 2022a; Cheong et al., 2021). Therefore, cybersecurity risk disclosure (CSRD), in general, is the process of informing cybersecurity-associated risk to stakeholders, such as regulators and investors. Moreover, this type of disclosure can take a variety of forms, including press releases, written reports, and public statements. The level of disclosure can vary depending on many factors such as the firm's size, age, profitability, industry sector, leverage, expenses, and risk profile as a whole.

In academic research, CSRD refers to the practice of publicly reporting data and information about a firm's CSR and incidents.

This disclosure is valuable for all categories of stakeholders, as it can help them evaluate and assess the firm's financial health (Jiang et al., 2022). Furthermore, there are many critical reasons why CSRD is important in accounting thought (Gao et al., 2020). First, CSR can have a significant impact on a firm's financial health. Second, CSRD can help investors make informed decisions about their investments. Third, CSRD can help firms handle and manage their CSR (Berkman et al., 2018; Kelton, 2021), and to the best of our knowledge, there are some of the key elements of CSRD highlighted by (Alashi & Badi, 2020; Leiva & Clark, 2020; Sheneman, 2017; Cheong et al., 2019; Grant & Grant, 2014), such as 1) identification and assessment of CSR, 2) governance of CSR, 3) strategy for managing CSR, and 4) incident response plan.

Going further in 2019, the Capital Market Authority (CMA) in Saudi Arabia launched a cybersecurity guide — voluntary — to enhance confidence in the financial market and reduce risks, and it contained four main points: 1) cybersecurity governance, 2) CSR management and audit, 3) cybersecurity controls related to operational processes and 4) cybersecurity related to external parties.

Based on the above, this paper confirmed that CSRD is an important part of risk management and corporate governance; by publicly reporting on CSR, firms can help manage their reputation and financial health. More deeply, in our study, we are trying to discover the reality of CSRD in the Saudi business environment based on the huge digital transformation in all fields according to Saudi Vision 2030[1.] Moreover, we are trying to examine the impact of CSRD on both firm value and stock return. According to the foregoing, the current study investigates the determinants of CSRD in the Saudi business environment, in addition, the impact of this disclosure on both firm value and stock return volatility.

Thus, the structure of this paper is as follows. Section 2 reviews the relevant literature. Section 3 explains the methodology and develops the research models. Section 4 overviews the results. Section 5 discusses the main findings, and Section 6 presents the conclusion and future research directions.

2. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1. Determinants of cybersecurity risk disclosure

2.1.1. Firm size

Empirical research on the impact of firm size on CSRD has yielded mixed results. Some studies have found a positive impact, indicating that larger firms are more likely to disclose CSR. Gao et al. (2020) and Hilary et al. (2016) found that firm size positively influences the extent of CSRD in annual reports. This positive impact is likely a result of many elements highlighted by Ashraf and Sunder (2023), Berkman et al. (2018), and Ehioghiren et al. (2021) such as larger firms having more resources to allocate to CSR management. Moreover, larger firms are more likely to be targeted by cyberattacks. Other studies have found no significant impact of firm size on CSRD. For example, Frank et al. (2019), and Calderon and Gao (2021) did not find evidence to support a relation between firm size and CSRD and reported no significant impact of firm size on CSRD. Hence, there are several potential explanations for why there is no consistent impact or relation. Some of the most likely explanations were highlighted by Kelton and Pennington (2020), Lenka et al. (2023), and Swift et al. (2020) such as the importance of CSRD may vary across firms regardless of size. Moreover, the level of regulatory scrutiny, that firms face may vary across firms regardless of size. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H1: Firm size positively influences cybersecurity risk disclosure in the Saudi business environment.

2.1.2. Firm age

Some studies have found a positive impact, indicating that older firms are more likely to disclose CSR. Radu and Smaili (2022a) and Boss et al. (2022) found that firm age positively influences the extent of CSRD in annual reports, and observed that older firms tend to provide more detailed CSRD. This positive impact is likely a result of many elements highlighted by Frank et al. (2023), and Li et al. (2020), such as increased cybersecurity awareness and experience, where older firms have had more time to develop cybersecurity awareness and experience. Moreover, greater accumulation of cybersecurity resources, where older firms have had more time to accumulate cybersecurity resources. Other studies have found no significant impact of firm age on CSRD. For example, Masoud and Al-Utaibi (2022), and Mazumder and Hossain (2023) did not find evidence to support a relation between firm age and CSRD. There are several potential explanations for why there is no consistent relation. Some of the most likely explanations highlighted by Alashi and Badi (2020) and Hughes et al. (2023), such as varying importance of CSR, where the importance of CSR may vary across firms. Moreover, heterogeneous CSR management practices, where the way that firms measure and manage CSR may vary across firms. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H2: Firm age positively influences cybersecurity risk disclosure in the Saudi business environment.

2.1.3. Leverage

Research on the impact of leverage on CSRD has yielded mixed results. Some studies have found a positive impact. Sheneman (2017), and Masoud and Al-Utaibi (2022) found that leverage positively influences the extent of CSRD in annual reports. The positive relationship between firm leverage and CSRD can be attributed to several elements which highlighted by Bansal and Axelton (2024) and Ramírez et al. (2022), such as increased stakeholder scrutiny. Moreover, reputational risk management, where cybersecurity breaches can severely damage a firm's reputation. Other studies have found no significant impact of leverage on CSRD. For example, Radu and Smaili (2022b), and Chen et al. (2023) did

[1] https://www.vision2030.gov.sa/en

not find evidence to support a relation between leverage and CSRD. There are several potential reasons highlighted by Calderon and Gao (2021, 2022b), and Gao et al. (2020), such as varying industry risks and regulatory requirements. Moreover, alternative motivations for CSRD. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H3: Leverage positively influences cybersecurity risk disclosure in the Saudi business environment.

2.1.4. Operating expenses

Some studies have found a positive association, indicating that firms with higher operating expenses are more likely to disclose CSR. Smaili et al. (2023) and Cheong et al. (2021) observed that firms with higher operating expenses tend to provide more detailed CSRD. The positive relation can exist based on several explanations highlighted by Calderon and Gao (2022a, 2022b), and Kiesow Cortez and Dekker (2022), such as increased investment in cybersecurity capabilities. Moreover, enhanced CSR management practices, as operating expenses increase, firms may allocate more resources to establishing and maintaining effective CSR management practices. Other studies have found no significant association between operating expenses and CSRD. For example, Jiang et al. (2022) reported no significant association between operating expenses and CSRD. There are several potential reasons highlighted by Radu and Smaili (2022a), and EY Center for Board Matters (2021), such as alternative motivations for CSRD, where firms may disclose CSR for reasons other than operating expenses, like complying with industry standards, managing stakeholder expectations, or signaling their commitment to CSR management. Moreover, varying CSR profiles, where the relationship may vary across industries with different CSR profiles. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H4: Operating expenses positively influence cybersecurity risk disclosure in the Saudi business environment.

2.1.5. Free cash flow

Empirical research on the relationship between CSRD and free cash flow has yielded mixed results. Some studies have found a positive association. Hilary et al. (2016) and Hughes et al. (2023) observed that firms with a high level of free cash flow tend to have more disclosures about CSR. Several factors contribute to the positive relationship highlighted by Bansal and Axelton (2024) and Walton et al. (2021), such as resource availability and disclosure costs, where firms with stronger free cash flow have more resources to allocate towards CSR activities. Moreover, investor perceptions and disclosure incentives, where firms with stronger free cash flow are often perceived as more financially resilient and less susceptible to the negative impacts of cyberattacks. Other studies have found no significant association or even a negative relationship. For example, Mazumder and Hossain (2023), and Peng and Li (2022) did not find evidence to support a relationship between CSRD and cash flows. This is likely due to a number of factors highlighted by Havakhor et al. (2021) and Wang et al. (2022), such as comprehensiveness and quality of disclosure, where the effectiveness of CSRD hinges on the clarity, comprehensiveness, and timeliness of the information disclosed. Moreover, methodological challenges, where measuring both CSRD and free cash flow pose methodological challenges. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H5: Free cash flow positively influences cybersecurity risk disclosure in the Saudi business environment.

2.1.6. Profitability

Empirical research on the relationship between CSRD and firm profitability has yielded mixed results. Some studies have found a positive association. Boss et al. (2022) and Chen et al. (2023) indicated that firms with higher profitability are more likely to disclose CSR. The positive association was observed in some studies by Alashi and Badi (2020), and Mazumder and Hossain (2023) and highlighted several potential factors such as the signaling hypothesis, where profitable firms may have more resources to invest in robust cybersecurity measures and better incident response capabilities. Moreover, agency costs and risk management, where profitable firms shareholders and management incentives are more closely aligned, reduce agency costs. Other studies have found no significant association between profitability and CSRD. For example, Ramírez et al. (2022), and Bansal and Axelton (2024) did not find evidence to support a relationship between profitability and CSRD. Several reasons could explain this argument highlighted by Hughes et al. (2023) and Krus (2012), such as measurement challenges, where defining and measuring both "*profitability*" and "*cybersecurity risk disclosure*" can be complex and inconsistent across studies. Going further, disclosure motivation and strategy, where firms disclose risks for various reasons beyond profitability. Regulatory compliance, media pressure, or competitor behavior can drive disclosure even for less profitable firms. Additionally, disclosure strategies can differ. Some firms might release detailed information proactively, while others may adopt a more selective or reactive approach, regardless of their financial strength. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H6: Profitability positively influences cybersecurity risk disclosure in the Saudi business environment.

2.2. Cybersecurity risk disclosure and firm value

Despite the complexities, the research on CSRD suggests that disclosure can be an important tool for firms that are managing CSR, and disclosure can help to improve investor relations, enhance the firm's reputation, and reduce the cost of capital (Calderon & Gao, 2021; Chen et al., 2023). However, the relationship between CSRD and firm value is complicated, this is because how we measure firm value could influence significantly the outcome of the examined relationships (Shahrour et al., 2022; Viviani & Maurel, 2019). The impact of disclosure can depend on many factors, such as the type of disclosure, the firm's industry, and the market conditions. Furthermore, CSR has emerged as a significant threat to businesses in today's interconnected world. These risks can lead to substantial financial losses, reputational damage, and operational disruptions, potentially impacting a firm's overall value (Ehioghiren et al., 2021). As a result, firms are increasingly focused on managing and disclosing CSR effectively. Going further, some studies have found a positive impact, indicating that firms with higher CSRD are more likely to have an increased trend for firm value across years. For instance, Lenka et al. (2023) found that CSRD positively influences the firm value. Similarly, the studies by Firoozi and Mohsni (2023), Haapamäki and Sihvonen (2019), and Swift et al. (2020) ensured that impact. On the other hand, many studies have found no significant association between firm value and CSRD. For example, Sheneman (2017) did not find evidence to support a relationship between firm value and CSRD. Similarly, Eling et al. (2020) reported no significant association between firm value and CSRD. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H7: Cybersecurity risk disclosure positively influences firm value in the Saudi business environment.

2.3. Cybersecurity risk disclosure and stock return volatility

While the term "stock return volatility" is more common in finance research, it has increasing relevance in accounting research because of its impact on investor decision-making. In terms of theoretical considerations, signaling theory suggests that stock return volatility is mainly related to the volume of disclosure and the firm's reputation, especially in emerging stock markets. So firms with strong reputations and large volumes of disclosure have more to lose from a cyberattack. Disclosing risks proactively can signal their commitment to transparency and good governance, mitigating potential reputational damage (Frank et al., 2023). Also, legitimacy theory illustrates that firms strive for legitimacy in the eyes of stakeholders, including regulators and investors. Disclosing CSR can demonstrate compliance with regulations and responsible risk management practices, enhancing legitimacy and stakeholder theory. Argued that firms have obligations to various stakeholders, not just shareholders. Disclosing risks can demonstrate a commitment to protecting customers' data and employee privacy, fulfilling stakeholder expectations (Eaton et al., 2019). Going further, empirical research on the influence of CSRD on stock return volatility has yielded mixed results. Sheneman (2017) found that CSRD positively influences the performance of the stock in terms of trade volume. Similarly, the studies by Mazumder and Hossain (2023), and Peng and Li (2022) ensured that impact. From another side, many studies have found no significant association between stock return volatility and CSRD. For example, Zhang et al. (2018) did not find evidence to support a relationship between stock return volatility and CSRD. Based on the above, the following hypothesis can be developed to investigate this relation in Saudi Arabia:

H8: Cybersecurity risk disclosure positively influences stock return volatility in the Saudi business environment.

3. RESEARCH METHODOLOGY

3.1. Study sample

The population is represented by listed Saudi firms during the period from 2015 to 2022, where the total number of firms in the Saudi stock market is 226. This paper selected the sample based on three criteria, including: 1) the availability of firms' annual reports, 2) the firm has not been subject to merger, or discontinuation during the study period., and 3) excluding financial and banking sectors firms. Thus, the application of our criteria resulted in the selection of 109 firms to be the study sample, equivalent to 48.2% of the Saudi stock market.

Table 1. Tabulation of Global Industry Classification Standard (GICS) sector name

GICS sector name	*Firms*	*Freq.*	*Percent (%)*
Communication services	6	48	5.50
Consumer discretionary	12	96	11.01
Consumer staples	17	136	15.60
Energy	4	32	3.67
Health care	7	56	6.42
Industrials	16	128	14.68
Materials	38	304	34.86
Real estate	7	56	6.42
Utilities	2	16	1.83
Total	109	872	100.00

3.2. Variables measurement

3.2.1. Cybersecurity risk disclosure

Cybersecurity risk disclosure in Saudi firms' financial reporting was identified and ranked using an index, we developed the following index based on the past literature (Ehioghiren et al., 2021; Ramírez et al., 2022) and the official guide to cybersecurity for financial market institutions in Saudi Arabia.

Table 2. Cybersecurity risk disclosures index

Category	*Disclosure procedures and methods*
Cybersecurity and financial processes	1. Discloses the handling of ongoing cybersecurity issues. 2. Discloses the pre-protection methods and procedures of cybersecurity issues. 3. Discloses the evaluation and recognition of the consequences, costs, and risks of cybersecurity issues. 4. Discloses the insurance coverage of cybersecurity issues. 5. Discloses the future influence of cybersecurity issues on firm financial performance and market reaction. 6. Discloses the control of cybersecurity issues by the audit committee.
Cybersecurity governance	7. Discloses the engagement of the board of directors (BOD) in controlling cybersecurity-associated opportunities and risks. 8. Discloses the engagement of the General Assembly of Shareholders (GAOS) in controlling cybersecurity-associated opportunities and risks. 9. Discloses the establishment of a committee related directly to BOD dedicated to overseeing cybersecurity and information security. 10. Discloses the establishment of a committee related directly to BOD to supervise cybersecurity-related issues, such as risks or information security. 11. Discloses specific reports on the role of BOD in designing and evaluating the firm's information security risk management.
Cybersecurity management, operational processes and third parties	12. Discloses a description of information security and/or CSR. 13. Discloses data and information protection as a major issue. 14. Discloses specific Reports on response policies to cybersecurity issues in the firm's systems. 15. Discloses information security and/or cybersecurity as an essential part of the financial reports. 16. Discloses the improvement of tests and monitoring to ensure the validity of procedures and policies related to cybersecurity. 17. Discloses information security and/or cybersecurity as a risk element in the financial reports. 18. Discloses data and information privacy as a risk element in the financial reports. 19. Discloses CSR as part of organizational risks. 20. Discloses future information on cybersecurity issues or past incidents that may be considered as a risk element. 21. Discloses the number of meetings to the cybersecurity committee or similar committees related to BOD. 22. Discloses claims related to privacy violations and customer data. 23. Discloses the engagement of the internal audit in the management of information security and CSR. 24. Discloses the engagement of the external advisor in cybersecurity-related risk assessment and management. 25. Discloses the preparation methods of a cybersecurity policy aimed at handling and managing information security. 26. Discloses about the information security system. 27. Discloses that the information security system is acting according to internationally recognized standards. 28. Discloses on the guarantee of digital rights policy and/or personal data protection. 29. Discloses the adoption of information awareness and training strategies for employees to reduce CSR. 30. Discloses the existence of appropriate communication policies that provide cybersecurity information to all categories of stakeholders.

3.2.2. Determinants of cybersecurity risk disclosure

Table 3 presents the measurement of *CSRD* determinants.

Table 3. The measurement of cybersecurity risk disclosure (*CSRD*) determinants

Variable	*Measurement method*
Firm size (FS)	The natural logarithm of total assets.
Firm age (FA)	The natural logarithm of the number of years after the first financial statement date.
Leverage (LEV)	Debt-to-equity ratio, total liabilities divided by total shareholders' equity.
Operating expenses (OPEX)	Operating expense ratio. This expresses OPEX as a percentage of revenue.
Free cash flows (FCF)	The ratio of a firm's free cash flow per share to its current market price per share.
Profitability (ROA)	Return on assets (ROA), net income divided by total assets.

3.2.3. Firm value

The most common method in literature to measure the value of the firm is Tobin's Q, (Masoud & Al-Utaibi, 2022) which compares the market value of the firm to the replacement cost of its assets.

$$Tobin's\ Q = \frac{Market\ capitalization}{Replacement\ cost\ of\ assets} \quad (1)$$

3.2.4. Stock return volatility

Stock return volatility (*SRV*) in literature refers to the standard deviation of daily stock returns of the firm (Dai et al., 2023; Rupande et al., 2019) and is calculated as follows:

$$SRV_{i,t} = \sqrt{\sum\nolimits_{i}^{N} \left(R_{\,i,m,t} - MEAN_{i,t}\right)^2 \times (1/N)} \quad (2)$$

where,

- $R_{\,i,m,t}$ is the daily return of stock *i* at the day *m* in the period *t*;
- $MEAN_{i,t}$ is the annual average of daily stock return of the firm *i* in the period *t*;
- N is the number of trading days.

3.3. Research model

To test hypotheses (from *H1* to *H6*), the linear regression model using the panel data method will be applied, where the research model develops as follows below.

$$CSRD_{i,t} = \beta_0 + \beta_1 FS_{i,t} + \beta_2 FA_{i,t} + \beta_3 LEV_{i,t} + \\ \beta_4 OPEX_{i,t} + \beta_5 FCF_{i,t} + \beta_6 ROA_{i,t} + \beta_7 INDT_{i,t} + \\ \beta_4 OPEX_{i,t} + \beta_5 FCF_{i,t} + \beta_6 ROA_{i,t} + \beta_7 INDT_{i,t} \tag{3}$$

where,

- $CSRD_{i,t}$ is the CSRD index's result of the firm *i* during the period *t*;
- $FS_{i,t}$ is the size of the firm *i* during the period *t*;
- $FA_{i,t}$ is the age of the firm *i* during the period *t*;
- $LEV_{i,t}$ is the leverage of the firm *i* during the period *t*;
- $OPEX_{i,t}$ is the operation expenses of the firm *i* during the period *t*;
- $FCF_{i,t}$ is the free cash flow of the firm *i* during the period *t*;
- $ROA_{i,t}$ is the return on assets of the firm *i* during the period *t*.

To test *H7*, the linear regression model using the panel data method will be applied, where the research model develops as follows:

$$FV_{i,t} = \beta_0 + \beta_1 CSRD_{i,t-1} + \\ \sum \beta_{2-7} Control\ variables_{i,t} + E_{i,t} \tag{4}$$

where,

- $FV_{i,t}$ is the value of the firm *i* during the period *t*;
- $CSRD_{i,t-1}$ is the CSRD index's result of the firm *i* during the period *t - 1*.

To test *H8*, the linear regression model using the panel data method will be applied, where the research model develops as follows:

$$SRV_{i,t} = \beta_0 + \beta_1 CSRD_{i,t-1} + \\ \sum \beta_{2-7} Control\ variables_{i,t} + E_{i,t} \tag{5}$$

where,

- $SRV_{i,t}$ is stock return volatility of the firm *i* during the period *t*;
- $CSRD_{i,t-1}$ is the CSRD index's result of the firm *i* during the period *t - 1*.

4. RESEARCH RESULTS

4.1. Descriptive statistics

Table 4 presents the statistical summary for firm value, stock return volatility, CSRD, and firm-specific control variables in our sample, covering the period from 2015 to 2022. The variables are subjected to Winsorization, where the extreme values at the top and bottom 2% are replaced with less extreme values to reduce the impact of outliers. Over the period from 2015 to 2022.

Table 4. Descriptive statistics

Variables	*Obs.*	*Mean*	*Median*	*Std. dev.*	*Min*	*Max*
FV	872	2.649	1.650	3.221	0.630	32.200
SRV	872	0.021	0.019	0.009	0.000	0.176
CSRD	872	16.588	16.000	4.500	8.000	28.000
FS	872	21.630	21.505	1.610	16.460	26.910
FA	872	14.766	15.000	6.744	1.000	45.000
LEV	872	0.238	0.220	0.204	0.000	2.280
FCF	872	0.029	0.030	0.088	-0.300	0.300
ROA	872	0.042	0.030	0.068	-0.030	0.400
OPEX	872	0.416	0.367	0.282	0.002	1.000

FV, as measured by Tobin's Q, for the 872 observations is 2.649. This average value is higher than the median value of 1.650, indicating that the listed firms in Saudi Arabia are imbalanced. Specifically, it suggests that the top firms possess superior firm value, while most firms have a lower firm value. Regarding *SRV*, it shows a standard deviation of 0.009, which represents around (42%) of the mean (0.021). This implies that the values of the *SRV* show widespread around the mean through time and across firms. *CSRD* shows a mean of 16.588 with low dispersion around the mean of 4.5, meaning that firms have the same CSRD practices.

On firms' characteristics control variables, *FS* applies the logarithm on total assets, resulting in small variances in *FS* among the sample firms. Thus, the *FS* shows a standard deviation of 1.61, which is very small relative to the overall mean of 21.63. In addition, the small range between the minimum value of 16.46 and the maximum value of 26.91 reflects the homogeneity in *FS*. In contrast, *FA* shows a standard deviation of 6.74, which is large relative to the overall mean of 14.766. In addition, the large range between the minimum value of 1.000 and the maximum value of 45.000 reflects the heterogeneity in *FA* for Saudi Arabia-listed firms. *LEV* shows around 20.4% standard deviation around the overall mean of 23.8%. This implies that some firms depend heavily on debt to finance their assets. Meanwhile, other firms show a minor dependence on debt to finance their assets. *FCF* shows a mean of 0.029 with a standard deviation of 0.088. Concerning the *ROA*, its standard deviation of 0.068 represents around 162% of its overall mean of 0.042. Indicating that the return on assets varies significantly among the research sample. Finally, *OPEX* shows a mean of 0.416 with a 0.282 standard deviation.

4.2. Correlation analysis

The correlation matrix offers preliminary insight into the association between the dependent and independent variables. Furthermore, it assists in detecting potential multicollinearity, which can lead to inaccurate estimations. We calculate the variance inflation factor for every independent variable to assess this matter. The calculated variance inflation factors range from 1.01 to 1.57, which is lower than the threshold of 10 specified by Porzio (2013). Hence, there is no multicollinearity detected between regressors used to test the impact of *CSRD* on *FV* and *SRV*. The highest correlation coefficient is 0.534 which is found between *ROA* and *FCF* as shown in Table 5.

Table 5 reports the Pearson correlation coefficients for our research variables. All firm-specific characteristics except for *LEV*, *FCF*, and OPEX are positively and significantly associated with *CSRD*. *FV* is positively and significantly correlated with *CSRD* and many of the firm characteristics, all control variables except *ROA* and *FA* are significantly correlated with firm value. In contrast, *SRV* is negatively and significantly correlated with *CSRD*, all control variables except *FA* are significantly correlated with *SRV*.

Table 5. Correlation matrix

Variables	FV	SRV	CSRD	FS	FA	LEV	FCF	ROA	OPEX
FV	1.000								
SRV	-0.012	1.000							
	(0.722)								
CSRD	0.078**	-0.073**	1.000						
	(0.022)	(0.031)							
FS	-0.329***	-0.153***	0.220***	1.000					
	(0.000)	(0.000)	(0.000)						
FA	0.049	-0.013	0.065*	-0.064*	1.000				
	(0.148)	(0.711)	(0.056)	(0.059)					
LEV	-0.125***	0.096***	0.038	0.258***	-0.133***	1.000			
	(0.000)	(0.005)	(0.269)	(0.000)	(0.000)				
FCF	-0.078**	-0.179***	0.013	0.202***	-0.122***	-0.182***	1.000		
	(0.021)	(0.000)	(0.704)	(0.000)	(0.000)	(0.000)			
ROA	0.084**	-0.173***	0.084**	0.147***	-0.132***	-0.352***	0.534***	1.000	
	(0.013)	(0.000)	(0.014)	(0.000)	(0.000)	(0.000)	(0.000)		
OPEX	0.077**	0.062*	0.012	-0.173***	-0.171***	0.178***	0.087**	0.128***	1.000
	(0.023)	(0.069)	(0.713)	(0.000)	(0.000)	(0.000)	(0.010)	(0.000)	

Note: *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.

4.3. Stationarity test

Before analyzing the effect of *CSRD* on *FV* and *SRV*, we initially assessed the stationarity features of the variables as a preliminary test. Harris-Tzavalis unit-root test is conducted to examine whether the time series of each variable is stationary or has a unit-root of balanced panel data. According to Table 6, the firm's age is stationary at first difference. On the other hand, all the other variables are stationary. This indicates that the variables do not possess a unit root. Therefore, the null hypothesis (H_0) regarding the presence of a unit root test is disproven.

Table 6. Panel unit-root test

Variables	Harris-Tzavalis unit-root test
FV	-20.8385***
SRV	22.3791***
CSRD	-4.3185***
FS	-2.0257**
D1.FA	-17.5226***
LEV	-8.5566***
FCF	-16.1682***
ROA	-11.4170***
OPEX	-14.9271***

Note: *, **, and *** show the rejection of H_0 of a unit root at 10%, 5%, and 1%.

4.4. Cointegration test

The cointegration test extends the stationarity test. The cointegration test examines the stationarity among more than one series. Therefore, the cointegration test evaluates the stationarity of the time series of several variables included altogether in a specific model. However, each single time series of these variables has proven to be stationary using the unit root test. However, the unit root test does not assess the long-run stochastic trends among many time series. Therefore, the cointegration test is used to examine the existence of an equilibrium phenomenon, that is, a constant long-run structural association among a set of variables. We performed a cointegration test using the Kao method to determine whether the variables are cointegrated. Table 7 demonstrates that the variables exhibit cointegration. Therefore, a long-term relationship exists between the variables for all models of the research.

Table 7. Cointegration test

Model	Harris-Tzavalis unit-root test
Firm-specific determinants → CSDR	-4.7441***
CSRD → FV	-16.3961***
CSRD → SRV	-18.3770***

Note: *, **, and *** show the rejection of H_0 of no cointegration at 10%, 5%, and 1%.

4.5. Hypotheses test

The models mentioned above are estimated using ordinary least squares (OLS) and the panel-corrected standard errors (PCSE) technique as a robustness estimation. The PCSE technique is utilized because of its ability to generate an estimate that is clear of autocorrelation, precise standard error estimate, and reduced susceptibility to outlier estimates. The PCSE technique is employed for analyzing dynamic heterogeneous panel data (Bailey & Katz, 2011).

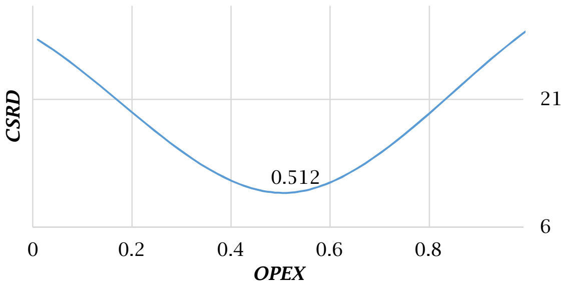
Table 8. Cybersecurity risk disclosure (*CSRD*) determinants

CSRD	*OLS*	*PCSE*
FS	0.3593***	0.4897***
FA	0.0728***	0.0633***
LEV	3.0235***	0.8894*
ROA	11.3665***	3.1105**
FCF	-1.049	-0.734
Std_OPEX	-0.5706***	-0.2570*
Std_OPEX2	0.5149***	0.3357***
Obs.	872	872
R^2	0.495	0.639
Year fixed effect	Included	Included
Industry fixed effect	Included	Included

*Note: *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.*

Table 8 shows the results of the empirical model of Eq. (1) which tests the determinants of *CSRD*. The results presented in Table 8 confirm our hypotheses *H1*, *H2*, *H3*, *H6*. Especially, as expected, we find that the coefficients of the impact of *FS*, *FA*, *LEV*, and *ROA* are positively and significant (coefficient: 0.359; p-value < 0.01; coefficient: 0.0728; p-value < 0.01; coefficient: 3.0235; p-value < 0.01; and coefficient: 11.3665; p-value < 0.01) respectively. In contrast, this research rejects hypothesis *H5*, *FCF* has no significant effect on *CSRD*. Moreover, this research reveals that a curvilinear relationship exists between *OPEX* and *CSRD*, which means the existence of an optimal level of *OPEX*. Any deviation will lead to inefficiency in *CSRD*. There is an inverted U-shape between them. Where the *OPEX* parameter is positive (> 0) and significant, and *OPEX* squared is negative (< 0) and significant. Therefore, hypothesis *H4* is rejected. Thus, the optimal level of the *OPEX* maximizes *CSRD*.

Figure 1. Quadratic effect of operating expenses on cybersecurity risk disclosure



This means the *OPEX* ratio from 0 to 55% shows a positive association between *OPEX* and *CSRD*. In addition, the OPEX ratio exceeding 55% will negatively impact *CSRD*, therefore, the optimal operating expenses in association with *CSRD* is 0.55.

Table 9. Cybersecurity risk disclosure (*CSRD*) and firm value (*FV*)

FV	*OLS*	*PCSE*
CSRD	0.1114***	0.1190***
FS	0.0244**	-0.7088***
FA	0.1165***	0.0915**
FA2	-0.0031***	-0.0025***
LEV	-9.6693***	-6.2044***
LEV2	9.4359***	7.0937***
ROA	0.083	-1.080
FCF	-5.3783***	-2.1815***
FCF2	26.2838**	12.7268***
OPEX	1.5220***	1.8272***
Obs.	872	872
R^2	0.535	0.650
Year fixed effect	Included	Included
Industry fixed effect	Included	Included

*Note: *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.*

Table 9 shows the results of the empirical model of Eq. (2) which tests the impact of *CSRD* on *FV*. The results presented in Table 9 confirm our hypothesis *H7*. Especially, as expected, we find that *CSRD* has a positive and significant impact on *FV* (coefficient: 0.1114; p-value < 0.01). In addition, *FS* and *OPEX* have a positive and significant impact on *FV*. On the other hand, there is no significant impact of *ROA* on *FV*. In addition, *FA*, *LEV*, and *FCF* firmly reveal a curvilinear relationship exists with *FV*, which means the existence of a turning point presented below.

Figure 2. Non-linear turning points of Model 2

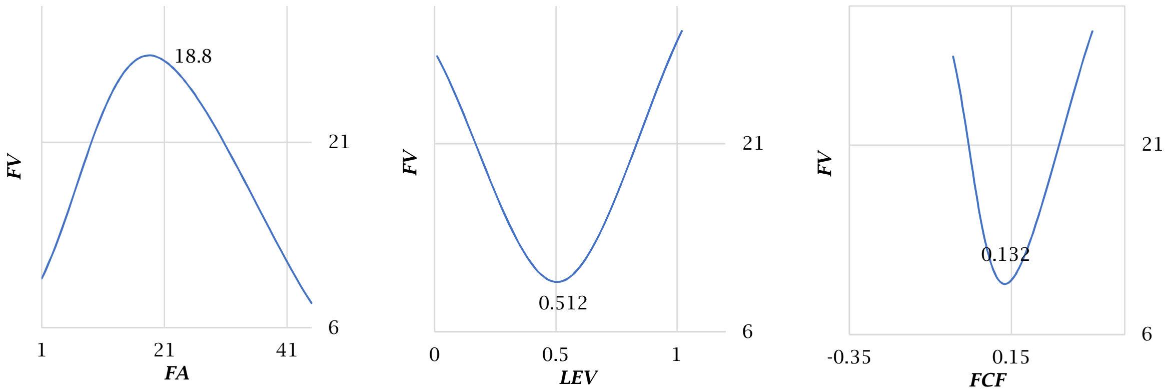


Figure 2a. Firm age (*FA*): Inverted (U) shape

Turning point = 18.8

Figure 2b. Leverage (*LEV*): (U) shape

Turning point = 51.2%

Figure 2c. Free cash flows (*FCF*): (U) shape

Turning point = 0.095

As for Figure 2a, this means an *FA* range from 0 to 18.8 shows a positive association between *FA* and *FV*. In addition, *FA* exceeding 18.8 will negatively impact *FV*.

As for Figure 2b, this means a *LEV* rate from 0 to 0.512 shows a negative association between *LEV* and *FV*. In addition, *LEV* exceeding 0.512 will positively impact *FV*.

As for Figure 2c, this means an *FCF* rate from -0.3 to 0.09 shows a negative association between *FCF* and *FV*. In addition, *FCF* exceeding 0.09 will positively impact *FV*.

Table 10. Cybersecurity risk disclosure (*CSRD*) and stock return volatility (*SRV*)

SRV	***OLS***	***PCSE***
CSRD	-0.001**	-0.002*
FS	-0.0008***	-0.0007***
FA	0.000	0.000
LEV	0.0086***	0.0071**
LEV2	-0.0071***	-0.0044**
ROA	-0.0311***	-0.0214**
ROA2	0.1174***	0.0959**
FCF	-0.0114**	-0.0116***
OPEX	0.000	0.001
Obs.	872	872
R^2	0.252	0.288
Year fixed effect	Included	Included
Industry fixed effect	Included	Included

*Note: *, **, and *** denote significance at the 10%, 5%, and 1% levels, respectively.*

Table 10 shows the results of the empirical model of Eq. (3) which tests the impact of *CSRD* on *SRV*. The results presented in Table 10 confirm our *H8*. Especially, as expected, we find that *CSRD* has a negative and significant impact on *SRV* (coefficient: -0.001; p-value < 0.05). In addition, *FS* and *FCF* have a negative and significant impact on *SRV*. On the other hand, there is no significant impact of *FA* and *OPEX* on *SRV*. In addition, *LEV*, and *ROA* to firm reveal a curvilinear relationship exists with *SRV*, which means the existence of a turning point as follows below.

Figure 3. Non-linear turning points of Model 3

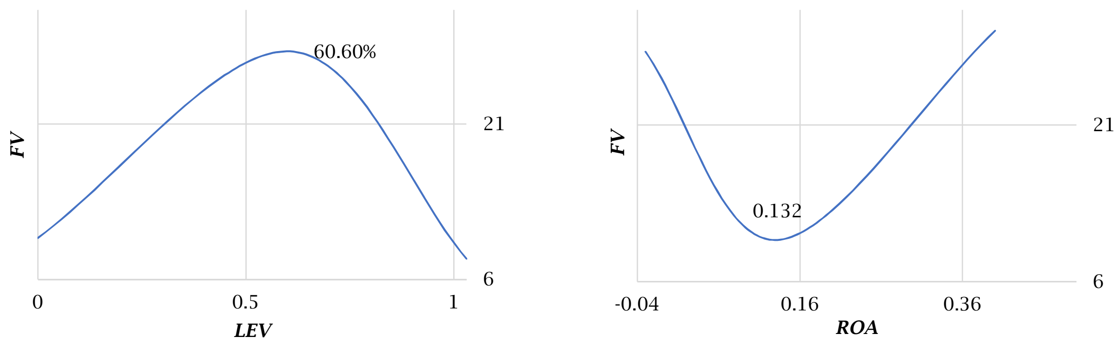


Figure 3a. *LEV*: Inverted (U) shape

Turning point = 60.6%

Figure 3b. *ROA*: (U) shape

Turning point = 13.25%

As for Figure 3a, this means a *LEV* rate from 0 to 60.6 shows a positive association between *LEV* and *SRV*. In addition, *LEV* exceeding 0.606 will negatively impact *SRV*.

As for Figure 3b, this means an *ROA* rate from 0 to 0.132 shows a negative association between *LEV* and *SRV*. In addition, *LEV* exceeding 0.132 will positively impact *SRV*.

5. DISCUSSION

In terms of firm value, past empirical evidence suggests a complex relationship between CSRD and firm value. Studies consistently show that timely and comprehensive disclosure positively correlates with investor trust. Furthermore, Investors appear to reward firms that proactively communicate about potential cyber threats, viewing such disclosures as signs of effective risk management and corporate responsibility. Nevertheless, the nature of the disclosed risks and the subsequent risk management strategies significantly influence the financial market's reaction. High-severity cyber incidents, when properly communicated and mitigated, may have a muted impact on firm value. On the other hand, instances of inadequate disclosure or delayed responses lead to negative market reactions, manifesting as declines in stock prices and diminished market capitalization. Our findings from the Saudi business environment ensure the positive impact of CSRD on firm value and underscore the importance of not only disclosing CSR but also ensuring the quality, accuracy, and timeliness of such disclosures. Firms must recognize the potential consequences of insufficient communication, as it may erode stakeholder trust and negatively impact their overall market valuation. In terms of stock return dynamics, the analysis of stock volatility in the context of CSRD shows a dynamic relationship shaped by many factors. While disclosure itself may contribute to short-term increases in volatility as markets react to perceived uncertainties, the overarching impact is contingent on the effectiveness of risk mitigation and the subsequent market sentiment. However, effective disclosure, coupled with evidence of robust cybersecurity measures, may act as a stabilizing factor, mitigating the potential for prolonged volatility. On the other hand, insufficient or delayed disclosures may exacerbate market uncertainties, leading to increased volatility and heightened trading volumes. Furthermore, understanding the dynamics of stock volatility requires a nuanced consideration of market expectations, the severity of disclosed risks, and the broader economic environment. Our findings from the Saudi business environment ensure the positive impact of CSRD on decreasing stock return volatility and support the notion that while CSRD can contribute to short-term market fluctuations, its long-term impact on stock volatility is intricately linked to the market's perception of a firm's resilience and adaptability in the face of evolving cyber threats. So, our findings are consistent with Firoozi and Mohsni (2023), Haapamäki and Sihvonen (2019), and Swift et al. (2020).

6. CONCLUSION

The investigation into the impact of CSRD on firm value and stock return volatility has provided valuable insights into the intricate dynamics between information transparency, market reactions, and financial performance. As firms confront an ever-evolving digital landscape, understanding the implications of disclosing CSR is crucial for shaping effective risk management strategies and sustaining stakeholder trust. Based on the Saudi business environment from 2015 to 2022, the findings underscore the critical importance of proactive and transparent communication regarding CSR. Firms that prioritize comprehensive disclosure, coupled with robust risk management practices, are better positioned to maintain stakeholder trust, preserve firm value, and avoid stock return volatility. This study emphasizes the need for continuous efforts to improve the quality, accuracy, and timeliness of CSRD, aligning them with evolving market expectations and regulatory requirements. Based on the above arguments, our findings from the Saudi business environment are consistent with Alashi and Badi (2020), Mazumder and Hossain (2023), and Peng and Li (2022). In brief, there were limitations to our research paper, divided into place limits (the Saudi business environment) and time limits (2015–2022). Going further, the impact of CSRD on FV and stock return volatility is a multifaceted and evolving phenomenon. This research contributes to the academic understanding of this relationship in Saudi Arabia's business environment while offering practical implications for organizations seeking to enhance their CSR management practices and, consequently, their overall financial health and market stability. Finally, this study identifies several challenges that warrant further exploration. Quantifying the financial impact of CSR remains a formidable task, as the intangible nature of these risks complicates traditional valuation methodologies. Additionally, the potential for market overreaction to cybersecurity disclosures raises questions about the optimal level of information to be disclosed and the role of regulatory frameworks in shaping disclosure practices.

REFERENCES

Alashi, S. A., & Badi, D. H. (2020). The role of governance in achieving sustainable cybersecurity for business corporations. *Journal of Information Security & Cybercrimes Research, 3*(1), 97–112. https://doi.org/10.26735/EINT7997

Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review, 98*(4), 1–32. https://doi.org/10.2308/TAR-2020-0787

Bailey, D., & Katz, J. N. (2011). Implementing panel-corrected standard errors in R: The PCSE package. *Journal of Statistical Software, 42*(code snippet 1), 1–11. https://doi.org/10.18637/jss.v042.c01

Bansal, G., & Axelton, Z. (2024). Impact of cybersecurity disclosures on stakeholder intentions. *Journal of Computer Information Systems, 64*(1), 78–91. https://doi.org/10.1080/08874417.2023.2180785

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

Boss, S. R., Gray, J., & Janvrin, D. J. (2022). Accountants, cybersecurity isn't just for "techies": Incorporating cybersecurity into the accounting curriculum. *Issues in Accounting Education, 37*(3), 73–89. https://doi.org/10.2308/ISSUES-2021-001

Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Auditing, 25*(1), 24–39. https://doi.org/10.1111/ijau.12209

Calderon, T. G., & Gao, L. (2022a). Changes in corporate cybersecurity risk disclosures after SEC comment letters. *Journal of Accounting and Public Policy, 41*(5), Article 106993. https://doi.org/10.1016/j.jaccpubpol.2022.106993

Calderon, T. G., & Gao, L. (2022b). Comparing the cybersecurity risk disclosures of U.S. and foreign firms. *Journal of Emerging Technologies in Accounting, 19*(2), 61–79. https://doi.org/10.2308/JETA-2020-008

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*, 199–224. https://doi.org/10.1007/s10551-022-05107-z

Cheong, A., Cho, S., No, W. G., & Vasarhelyi, M. A. (2019). *If you cannot measure it, you cannot manage it: Assessing the quality of cybersecurity risk disclosure through textual imagification.* https://doi.org/10.2139/ssrn.3474575

Cheong, A., Yoon, K., Cho, S., & No, W. G. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems, 35*(2), 179–194. https://doi.org/10.2308/ISYS-2020-031

Dai, Z., Zhang, X., & Li, T. (2023). Forecasting stock return volatility in data-rich environment: A new powerful predictor. *The North American Journal of Economics and Finance, 64*, Article 101845. https://doi.org/10.1016/j.najef.2022.101845

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing, 13*(2), C1–C9. https://doi.org/10.2308/ciia-52419

Ehioghiren, E. E., Ojeaga, J. O., & Eneh, O. (2021). Cyber security: The perspective of accounting professionals in Nigeria. *Accounting & Taxation Review, 5*(2), 15–29. https://www.zbw.eu/econis-archiv/bitstream/11159/6566/1/1780947623_0.pdf

Eling, M. (2020). Cyber risk research in business and actuarial science. *European Actuarial Journal, 10*, 303–333. https://doi.org/10.1007/s13385-020-00250-1

EY Center for Board Matters. (2021). *How cybersecurity risk disclosures and oversight are evolving in 2021.* https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/board-matters/ey-cbm-cybersecurity-disclosures-2021.pdf

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

Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems, 33*(3), 183–200. https://doi.org/10.2308/isys-52374

Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B. (2023). Implications of enhanced cybersecurity risk management reporting and independent assurance. *Current Issues in Auditing, 17*(1), P11–P18. https://doi.org/10.2308/CIIA-2022-018

Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems, 38*, Article 100468. https://doi.org/10.1016/j.accinf.2020.100468

Grant, G. H., & Grant, C. T. (2014). SEC cybersecurity disclosure guidance is quickly becoming a requirement. *The CPA Journal, 84*(5), 69–71. https://surl.li/wktnua

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal, 34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Havakhor, T., Rahman, M. S., & Zhang, T. (2021). Disclosure of cybersecurity investments and the cost of capital. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3553470

Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-risk disclosure: Who cares?* https://doi.org/10.2139/ssrn.2852519

Hughes, H., Smith, T. J., & Walton, S. (2023). Material contract redactions and cybersecurity breaches. *Accounting Horizons, 37*(3), 193–219. https://doi.org/10.2308/HORIZONS-2020-166

Jiang, W., Legoria, J., Reichelt, K. J., & Walton, S. (2022). Firm use of cybersecurity risk disclosures. *Journal of Information Systems, 36*(1), 151–180. https://doi.org/10.2308/ISYS-2020-067

Kelton, A. S. (2021). How to reduce the cybersecurity breach contagion effect. *Current Issues in Auditing, 15*(2), P1–P9. https://doi.org/10.2308/CIIA-2020-025

Kelton, A. S., & Pennington, R. R. (2020). Do voluntary disclosures mitigate the cybersecurity breach contagion effect? *Journal of Information Systems, 34*(3), 133–157. https://doi.org/10.2308/isys-52628

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

Krus, C. M. (2012). Who is listening? The SEC emphasizes importance of cybersecurity disclosure. *Journal of Investment Compliance, 13*(1), 30–32. https://doi.org/10.1108/15285811211216673

Leiva, A. M., & Clark, M. E. (2020). COVID-19 considerations for SEC cybersecurity guidance, disclosure, enforcement, and parallel proceedings: Navigating the new normal. *Journal of Investment Compliance, 21*(2–3), 111–126. https://doi.org/10.1108/JOIC-08-2020-0018

Lenka, A., Goswami, M., Singh, H., & Baskaran, H. (2023). Cybersecurity disclosure and corporate reputation: Rising popularity of cybersecurity in the business world. In F. Adedoyin & B. Christiansen (Eds.), *Effective cybersecurity operations for enterprise-wide systems* (pp. 169–183). IGI Global. https://doi.org/10.4018/978-1-6684-9018-1.ch008

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing, 39*(1), 151–171. https://doi.org/10.2308/ajpt-52593

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

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

Peng, J., & Li, C.-W. (2022). Security breaches and modifications on cybersecurity disclosures. *Accounting and Management Information Systems, 21*(3), 452–470. https://doi.org/10.24818/jamis.2022.03007

Porzio, G. C. (2013). Regression analysis by example. *Journal of Applied Statistics, 40*(12), 2776–2777. https://doi.org/10.1080/02664763.2013.817041

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

Radu, C., & Smaili, N. (2022b). Correction to: Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure. *Journal of Business Ethics, 177*, 375. https://doi.org/10.1007/s10551-021-04760-0

Ramírez, M., Ariza, L. R., Miranda, M. E. G., & 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

Rupande, L., Muguto, H. T., & Muzindutsi, P.-F. (2019). Investor sentiment and stock return volatility: Evidence from the Johannesburg Stock Exchange. *Cogent Economics & Finance, 7*(1), Article 1600233. https://doi.org/10.1080/23322039.2019.1600233

Shahrour, M. H., Girerd-Potin, I., & Taramasco, O. (2022). Corporate social responsibility and firm default risk mitigation: The moderating role of the legal context. *Finance Contrôle Stratégie*, *25*(1), 1–30. https://doi.org/10.4000/fcs.8784

Sheneman, A. (2017). *Cybersecurity risk and the cost of debt.* https://doi.org/10.2139/ssrn.3406217

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

Swift, O., Colon, R., & Davis, K. (2020). The impact of cyber breaches on the content of cybersecurity disclosures. *Journal of Forensic and Investigative Accounting*, *12*(2). https://web.nacva.com/JFIA/Issues/JFIA-2020-No2-2.pdf

Viviani, J.-L., & Maurel, C. (2019). Performance of impact investing: A value creation approach. *Research in International Business and Finance*, 47, 31–39. https://doi.org/10.1016/j.ribaf.2018.01.001

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: current state and future directions. *Journal of Information Systems*, *35*(1), 155–186. https://doi.org/10.2308/ISYS-19-033

Wang, T., Yen, J.-C., & Yoon, K. (2022). Responses to SEC comment letters on cybersecurity disclosures: An exploratory study. *International Journal of Accounting Information Systems*, *46*, Article 100567. https://doi.org/10.1016/j.accinf.2022.100567

Zhang, J., Djajadikerta, H. G., & Zhang, Z. (2018). Does sustainability engagement affect stock return volatility? Evidence from the Chinese financial market. *Sustainability*, *10*(10), 3361. https://doi.org/10.3390/su10103361