

Voluntary cybersecurity risk disclosures and firms' characteristics: the moderating role of the knowledge-intensive industry

Harmandeep Singh

School of Commerce, Finance and Accountancy, Christ University, Bangalore, India

Abstract

Purpose – This study examines voluntary cybersecurity risk disclosures (VCRD) by listed Indian companies. It also investigates how it relates to firm-specific characteristics such as size, leverage, profitability, liquidity, beta, market growth and industry.

Design/methodology/approach – The extent of VCRD was measured by assessing the cumulative occurrence of cybersecurity risk keywords in the annual report of 100 listed Indian non-financial companies. Keyword extraction and occurrence counts were performed using Python software. A multiple regression analysis was applied to predict the characteristics of VCRD.

Findings – The results showed that the theoretical frameworks underpinned by agency and signalling theories continued to provide a valid explanation of VCRD by Indian companies. Specifically, the findings emphasized the importance of firm size, leverage, and beta as significant VCRD determinants. Additionally, the study found that knowledge-intensive industries had a favourable impact on the extent of VCRD.

Research limitations/implications – This study is relevant because it informs company management, regulators and investors about the nature and characteristics of companies that satisfy stakeholder demands to prevent cyber breaches.

Originality/value – Understanding disclosure characteristics is crucial from policy and regulatory perspectives. Studies on cybersecurity disclosures are related to developed economies such as the United States of America and Canada. This is the first study to explore this issue in a developing nation, in general, and in India, in particular, where cybersecurity risk disclosure has yet to be recognized.

Keywords Cybersecurity, Cybersecurity risk disclosure, Voluntary risk disclosure, Firm-characteristics, Knowledge-intensive

Paper type Research paper

1. Introduction

The increased reliance of companies on Internet-based products such as blockchains, cloud-based systems, and artificial intelligence has made them more vulnerable to data breaches (Tawalbeh *et al.*, 2020), which pose a serious risk to business performance and reputation (Kamiya *et al.*, 2021). Henceforth, companies practice cybersecurity risk management to protect against these threats, which aim to protect their systems, hardware, software, and data from unauthorized access (Gatzert and Schubert, 2022). The ultimate goal of cybersecurity risk management is to ensure the integrity, confidentiality, and availability of information systems (Gordon *et al.*, 2015). Additionally, companies may be legally required to protect certain types of information, such as stakeholders' data [1], because failing to secure such information properly can result in financial losses, legal penalties, and damage to a company's reputation (Huang *et al.*, 2023).



Given the substantial impact of cyber breaches, companies have become increasingly transparent about disclosing cybersecurity risks and mitigation strategies (Gao *et al.*, 2020). Companies aim to address these uncertainties by integrating cybersecurity risk disclosures into their disclosure practices, which minimizes the differences in knowledge about such risks with external stakeholders (D'Arcy and Basoglu, 2022). EY (2021) states that companies with cyber security risk disclosures manifest their responsibility and engagement in this issue and develop stakeholder trust. Previous research has focused on the disclosure of cybersecurity risks (Gao *et al.*, 2020; Héroux and Fortin, 2020; Li *et al.*, 2018). However, these studies have focused where regulatory bodies concerned with cybersecurity risk management. For instance, the Security and Exchange Commission (SEC) issued guidance on cybersecurity disclosures for the USA based companies (Morse *et al.*, 2017). The disclosure literature argues that there have been considerable advances in companies' voluntary disclosure of sensitive information, such as cybersecurity risks (Mazumder and Hossain, 2022). Furthermore, companies have realized that withholding information on such critical content, which has enormous implications for investors, can negatively impact a company's market value and reputation in the long run if discovered by external resources (Berkman *et al.*, 2018). Public and external stakeholders, such as investors, shareholders, auditors, and risk analysts, are interested in cybersecurity disclosures because their decisions depend on this information (Héroux and Fortin, 2020). Therefore, this study measures the level of voluntary cybersecurity risk disclosure (VCRD) and the potential drivers that may affect the level of VCRD in Indian companies listed on the Bombay Stock Exchange (BSE), where cybersecurity disclosure practices are not yet recognized. For that purpose, the various firm characteristics that might impact VCRD are identified from the literature and incorporated into the study, such as firm size, profitability, liquidity, leverage, beta and market growth. The study also explored the moderating role of industry characteristics, specifically in knowledge-intensive sectors. Singhania and Panda (2022) point out that in today's knowledge era, intellectual and knowledge capital is the primary driver of value creation and competitive advantage in companies. Knowledge-intensive firms are extant in utilizing such resources (Otcenášková *et al.*, 2012). Thus, studying the moderating impact of knowledge-intensive companies on the relationships between VCRD and firm characteristics becomes necessary when considering this sector's unique structure and challenges. With high reliance on intellectual capital, knowledge-intensive industries are prime targets for cyber-attacks because of the value of data and the nature of their operations. Further, these companies are early adopters of new technology with open corporate cultures, which are susceptible to cyber-attacks (Deloitte, 2023).

Given this background, this study contributes to the growing literature on cybersecurity risk disclosures. A few studies have examined the disclosure of cybersecurity risk information, mostly in developing countries, such as the USA (Gao *et al.*, 2020; Li *et al.*, 2018) and Canada (Héroux and Fortin, 2020). In their research, Gao *et al.* (2020) mentioned a further need to investigate cybersecurity disclosures in different legal and economic environments. To the best of author's knowledge, no study has examined cybersecurity risk disclosure in the context of a developing nation. This is the first study to explore this issue in a developing nation, in general, and in India particularly.

The Indian government faces a shortage of resources for regulating cybersecurity and lacks a framework for enforcing related regulations, standards, and guidelines (Kshetri, 2017). Thus, this study is essential as it helps to inform regulators, investors, and company management about the nature and characteristics of companies that do not satisfy stakeholders' demands for cyber breaches. Moreover, this pioneering study examines the VCRD of listed non-financial companies. Khlif and Hussainey (2014) state that the financial industry is usually highly regulated, implying higher disclosure. Hence, examining non-financial Indian companies contributes significantly to the literature on cybersecurity risk disclosure. Although the current study has specific relevance to Indian companies, it is believed that many other countries with similar cybersecurity breaches and needs could benefit from these results.

The remainder of this paper is organized as follows: [Section 2](#) discusses the literature and the development of the study's hypotheses. [Section 3](#) describes the study sample, data, and variables. [Section 4](#) presents the results of this study. The last section summarizes the findings.

2. Literature review and hypothesis development

2.1 Literature review

In the digital era, data breaches can cause significant harm to companies, such as financial losses and reputational damage, depending on the sensitivity and magnitude of the information ([Huang et al., 2023](#)). Companies regularly improve technological security measures to prevent such breaches, hire accounting cybersecurity professionals, and maintain risk management teams ([Cheng et al., 2017](#)). Researchers have observed that companies can recover quickly due to their strong cyber infrastructure and risk-management teams ([Berkman et al., 2018](#)). For that, companies use cybersecurity disclosure practices, including policies and related risks, in their annual reports to win the confidence of their stakeholders ([Walton et al., 2020](#)). A study of Dutch annual reports has found that even in the absence of stringent regulations on cybersecurity disclosures, many companies have started to include information about their cybersecurity measures and incidents ([Gordon et al., 2015](#)). [Berkman et al. \(2018\)](#) have found that investors perceive companies that take steps to improve their cybersecurity to be more valuable. [Gao et al. \(2020\)](#) have reported that cybersecurity breaches could negatively affect a company's reputation and customer relationships.

Public disclosures concerning cybersecurity governance and risk management contribute to increasing stakeholder confidence by clarifying how boards carry out their cybersecurity risk-oversight obligations ([Kelton and Pennington, 2019](#)). Most Canadian firms have observed growth in the disclosure patterns of cybersecurity facts in a company-specific manner ([Héroux and Fortin, 2020](#)). [Masoud and Al-Utaibi \(2022\)](#) report that if a cyber breach happens in a company, there is an increase in the disclosure of cybersecurity-related risks. The researcher also shows that cybersecurity risk disclosure is related to various firm and governance characteristics ([Mazumder and Hossain, 2022](#); [Radu and Smaili, 2021](#); [Héroux and Fortin, 2020](#); [Gao et al., 2020](#); [Li et al., 2018](#)).

Henceforth, it is inferred from the literature that researchers measuring cybersecurity risk disclosures are in developed countries, particularly in the USA ([Gatzert and Schubert, 2022](#); [Li et al., 2018](#)) and Canada ([Radu and Smaili, 2021](#); [Héroux and Fortin, 2020](#)). A single study has considered an emerging economy ([Mazumder and Hossain, 2022](#)). However, none of the studies have analysed the pattern of cybersecurity risk disclosures in the context of developing nations. Another observation from the prior literature is that studies have presented conflicting findings. For instance, [Berkman et al. \(2018\)](#) found that cybersecurity risk disclosure positively impacts a company's market valuation and increases its sustainability, while [Morse et al. \(2017\)](#) mentioned that companies that did disclose cybersecurity-related risks experienced significant negative stock market prices. Furthermore, [Radu and Smaili \(2021\)](#) found that larger corporations are more likely to disclose cybersecurity-related risks. In contrast, [Higgs et al. \(2016\)](#) showed that smaller companies disseminate more information to build stakeholder trust. Henceforth, the current study addresses these discrepancies to better understand the factors influencing VCRD by adopting agency, signalling and intellectual capital theory frameworks. The study will explore how different firm characteristics impact the extent of VCRD in developing nations' context.

2.2 Hypothesis development

Prior studies have employed various theories to explain the factors in voluntary risk disclosure practices ([Khelif and Hussainey, 2014](#)). Agency and signalling theories are prominent on the list ([Elshandidy et al., 2018](#)). According to the agency theory, managers are motivated to share information voluntarily to close the information gap between themselves and the shareholders

(Watson *et al.*, 2002). Similarly, managers might be persuaded to increase voluntary disclosure to improve their reputation and credibility with external stakeholders such as borrowers, suppliers, and customers (Mazumder and Hossain, 2022). This is because greater transparency boosts investors' confidence and improves access to financing. Hence, agency theory is well applicable to cybersecurity risk disclosures since such disclosure can be used as an external control mechanism for any possible cyber threats, which lessens agency costs and will strengthen the relationship with external stakeholders. Like agency theory, signalling theory proposes that managers have incentives to increase disclosure and signal their quality to stakeholders (Elshandidy *et al.*, 2018). According to the signalling theory, companies with viable futures and strong financial performance are more likely to disclose them voluntarily (Jorgensen and Kirschenheiter, 2003) and can reassure stakeholders about their performance and prospects, as they have less to hide and gain (Elshandidy *et al.*, 2013). In contrast, companies with weak financial performance may be less likely to disclose anything because they are concerned that doing so could damage their reputation and leave unfavourable consequences (Linsley and Shrives, 2006). Hence, the companies may release cybersecurity risk information to signal their competencies and capabilities to handle cyber threats and distinguish themselves from others, which might translate into an improved reputation. For the knowledge-intensive industry impact, the study utilized the intellectual capital theory (Khalique *et al.*, 2013). Bueno *et al.* (2006) stipulated that technological capital under the intellectual capital theory is the set of intangible assets based on innovation and technical processes. The theory highlights that value creation from the organization resources is needed to create knowledge assets (Singhania and Panda, 2022), which would be a source of competitive advantage (Ocean Tomo, 2020). Prior researchers indicate that intellectual capital theory helps the organization in achieving performance and success (Ting *et al.*, 2020). According to the OECD (1999), knowledge-intensive industries have more technology and intellectual capital inputs than traditional industries. Thus, there would be higher management monitoring (Singhania and Panda, 2022) and better reporting in the knowledge-intensive industries (Madhani, 2016), increasing the requirement for voluntary disclosures such as cybersecurity. Since cybersecurity is the major threat in the knowledge-intensive industry because of the higher value of technological inputs and intangible assets (Goswami, 2018), stakeholders alike would pay much attention towards cybersecurity-related information. This would make them disclose more information on identifying and mitigating cyber threats. The following hypotheses were developed based on the above concentration.

2.3 Firm size

Larger firms have greater resources, more complex operations, and more diversified stakeholders, which may lead to greater scrutiny and motivate them to disclose more risk information to avoid negative consequences (Watts and Zimmerman, 1983). Additionally, larger companies generally have greater public visibility, implying higher public scrutiny among stakeholders (Oliveira *et al.*, 2011). In the context of cybersecurity risk, larger firms have more resources, dedicated personnel, and expertise in managing cyber threats than smaller firms do. Therefore, companies may disclose higher cybersecurity risk-related information to preserve themselves from increased cyber threats (Ettredge *et al.*, 2018; Kamiya *et al.*, 2021). Pooser *et al.* (2018) show that smaller firms are early adopters of cyber risk identification. Hence, the first hypothesis is as follows:

H1. A positive relationship exists between firms' size and the extent of VCRD.

2.4 Profitability

According to the signalling theory, more profitable firms may be incentivized to engage in risk disclosure because they have more to gain from enhancing their reputation and reducing information asymmetry with stakeholders (Elshandidy *et al.*, 2013). This implies that highly

profitable firms have additional resources to invest in cyber threat management, which may permit them to disseminate more information. In contrast, less profitable firms may be less likely to engage in voluntary disclosure because of concerns about the negative impact of poor financial performance disclosure on their reputation (Gatzert and Schubert, 2022; Pooser *et al.*, 2018). The second hypothesis is as follows:

H2. There is a positive relationship between a firm's profitability and the extent of VCRD.

2.5 Liquidity

Companies with higher liquidity levels may disclose information voluntarily and more often because of fewer constraints on securing external financing, reduced information asymmetry, and lower disclosure costs (Elshandidy *et al.*, 2013). In other words, liquid firms tend to engage in voluntary risk disclosure because of their incentive to reduce information asymmetry and greater capacity to obtain external financing (Khelif and Hussainey, 2014). SEC (2018) recommends that firms address cybersecurity risk management and incidents if they have a material effect on liquidity results. The third hypothesis is as follows:

H3. A positive relationship exists between firms' liquidity and the extent of VCRD.

2.6 Leverage

According to the agency theory, companies with a high leverage ratio have higher agency costs and require higher risk disclosure (Jensen and Meckling, 1976). Thus, the more a firm increases its cybersecurity risk disclosure level through dependency on borrowed capital, the more pressing it becomes for it to be impeachable by external creditors (Higgs *et al.*, 2016). Similarly, Pooser *et al.* (2018) find that firms with high leverage are early adopters of cyber risk identification. However, Kamiya *et al.* (2021) suggest that highly leveraged firms may hesitate to voluntarily reveal cyber risk management information because of concerns about creditor monitoring and the possibility of adverse selection. Masoud and Al-Utaibi (2022) find a negative and insignificant association between cybersecurity risk disclosure and subsequent cyber breaches. The fourth hypothesis is as follows:

H4. A positive relationship exists between firms' leverage and the extent of VCRD.

2.7 Market growth

A company's growth may result in greater information asymmetry and higher costs for managing internal affairs (Gaver and Gaver, 1993). Businesses with high growth potential must communicate superior information to the market for their stocks to be viewed as fairly valued rather than overpriced. Studies reported a positive relationship between market growth and risk disclosure (Cheng and Courtenay, 2006). Companies with potential market growth are expected to highlight the firm's visibility and require rapid expansion (Masoud and Al-Utaibi, 2022). To achieve this, they must be aware of and cautious about cyber threats and disclose more information. Thus, the fifth hypothesis is as follows:

H5. A positive relationship exists between firms' market growth and the extent of VCRD.

2.8 Beta

Firms with a higher degree of risk are incentivized to disseminate more information to justify their unfavourable circumstances and the reason for this higher risk (Khalil and Maghraby, 2017). Moreover, when an organization faces a high level of risk, stakeholders pay closer attention to its operations and put more pressure on it to provide more information (Kanto and Schadewitz, 1997). Previous empirical studies have found a positive association between risk disclosures and beta (Elshandidy *et al.*, 2015), as well as no association (Khalil and Maghraby,

2017). This study assumes that companies with higher market risk signal more to stakeholders about managing cybersecurity risks. The sixth hypothesis is as follows:

H6. A positive relationship exists between firms' leverage and the extent of VCRD.

2.9 Moderation impact of knowledge-intensive industry

Prior studies have emphasized that companies in different industries are exposed to various risk appetites (Khlif and Hussainey, 2014). Li *et al.* (2018) find that highly regulated industries that face greater scrutiny from stakeholders, such as the financial industry, tend to have higher levels of cybersecurity risk disclosure. In contrast, industries that are less regulated and face fewer demands for disclosure, such as the retail industry, tend to have lower levels of cybersecurity risk disclosure (Gao *et al.*, 2020). Knowledge-intensive industries have a higher value of technological inputs and intangible assets, particularly intellectual capital, than traditional industries (Goswami, 2018). Héroux and Fortin (2020) presumed that high-technology firms are prone to cybersecurity threats. Thus, the seventh hypothesis is as follows.

H7. A positive relationship exists between Knowledge-intensive industry and the extent of VCRD

H7a. Knowledge intensity industry moderates the relationship between firms' characteristics and VCRD.

3. Research methodology

3.1 Sample and data collection

For the present study, the initial sample was taken as the BSE-200 Index on March 31, 2022. The companies listed in the BSE 200 index are selected as the companies in this index collectively account for 85% of the market capitalization [2]. This was further filtered through 156 non-financial companies. Financial companies were dropped, given that the regulatory framework for such companies varied greatly from that of non-financial companies (Khlif and Hussainey, 2014). Of 156 non-financial companies, 100 were randomly selected. This study's primary source of information was the companies' annual reports collected from their websites. Data on the independent variables were collected from the Bloomberg database as on March 31, 2022.

3.2 Dependent variable (VCRD)

The dependent variable for the current study is voluntary cybersecurity risk disclosure (VCRD). To identify the VCRD contents, the study first downloaded each company's annual reports for 2021–2022. Second, a list of cybersecurity keywords was developed based on the National Initiative of Cybersecurity Careers and Studies (NICCS) glossary of key cybersecurity terms utilized in prior studies (Berkman *et al.*, 2018). The study supplemented the NICCS list by including cyber-related keywords such as attack, cyber, virus, unauthorized access, hack, breach, etc. These keywords were then incorporated into the disclosure mapping logic to develop an initial corpus of VCRD. Lastly, the Python code searched these cybersecurity keywords for each annual report. The Python code converts the annual reports collected in PDF format into text format. Once the file was converted, each line was broken into one component, and the list of the selected keywords was scanned. A keyword appearing in an annual report adds one to the existing count, starting from zero. Once the code is run entirely, it lists keywords that occurred in the annual reports and the number of times it did so. The dependent variable was measured as the natural log of the number of keywords as follows:

$$VCRD = \ln (no. of keywords)$$

3.3 Independent variables

For the current research objective, seven independent variables—firm size, profitability, leverage, liquidity, beta, market growth, and industry group—are considered, as shown in Table 1.

3.4 Estimation model

An ordinary least squares model was utilized to test the hypotheses of the present study, which is widely used in the risk disclosure literature (Khelif and Hussainey, 2014). To analyse the impact of firms’ characteristics on the extent of VCRD, the study developed two models, as shown below. The regression equations using different independent variables are as follows:

$$VCRD = \beta_0 + \beta_1(SIZE) + \beta_2(PRF) + \beta_3(LEV) + \beta_4(LIQ) + \beta_5(BETA) + \beta_6(MKTGRW) + \varepsilon \tag{Model 1}$$

To test the moderating effect of the knowledge-intensive industry sector in the relationship between firm characteristics and VCRD, the following equation was utilized:

$$VCRD = \beta_0 + \beta_1(SIZE) + \beta_2(PRF) + \beta_3(LEV) + \beta_4(LIQ) + \beta_5(BETA) + \beta_6(MKTGRW) + \beta_7(KI * SIZE) + \beta_8(KI * LEV) + \beta_9(KI * PRF) + \beta_{10}(KI * LIQ) + \beta_{11}(KI * BETA) + \beta_{12}(KI * MKTGRW) + \varepsilon \tag{Model 2}$$

Table 1. Descriptions of dependent and independent variables

Variables	Description and measurement	Source	References
<i>Dependent variable</i>			
VCRD	Voluntary Cybersecurity Risk Disclosures, i.e. selected keywords occurrence in the annual report for the financial year 2021–22	Annual reports	Calderon and Gao (2020) and Gao et al. (2020)
<i>Independent variables</i>			
SIZE	Firm Size, i.e. the natural logarithm of total assets during the financial year 2021–22	Bloomberg Database	Kamiya et al. (2021)
LIQ	Liquidity, i.e. the current ratio for the financial year 2021–22	Bloomberg Database	Pooser et al. (2018)
LEV	Leverage, i.e. debt to equity ratio for the financial year 2021–22	Bloomberg Database	Elshandidy et al. (2013)
PRF	Profitability, i.e. Return on Assets for the financial year 2021–22	Bloomberg Database	Khelif and Hussainey (2014)
BETA	Beta, i.e. the market risk for the financial year 2021–22	Bloomberg Database	Elshandidy et al. (2013)
MKTGRW	Market Growth, i.e. the market value to book value ratio (MV/BV) for the financial year 2021–22	Bloomberg Database	Elshandidy et al. (2018)
KI	Knowledge-Intensive Industry Type, i.e. according to GICS classifications	Bloomberg Database	Khelif and Hussainey (2014)
Source(s): Author’s own work			

where:

VCRD – Voluntary cybersecurity disclosure index

SIZE – Firm size

PRF – Profitability

LEV – Leverage

LIQ – Liquidity

BETA – Beta

MKTGRW – Market growth

KI – Knowledge-intensive industry

KI*SIZE – Interaction knowledge-intensive industry and firm size

KI* PRF – Interaction knowledge-intensive industry and profitability

KI* LEV – Interaction knowledge-intensive industry and leverage

KI* LIQ – Interaction knowledge-intensive industry and liquidity

KI* BETA – Interaction knowledge-intensive industry and beta

KI* MKTGRW – Interaction knowledge-intensive industry and market growth

β_0 – Intercept

ε – Residual.

4. Results and discussions

4.1 Descriptive analysis

Table 2 presents the results of the descriptive statistics for both dependent and independent variables.

The VCRD, the target variable of the current study, obtained an average of only 20% (Table 2). It is clear that the level of VCRD is low among sampled companies. The disclosure level ranges from a maximum of 139 to a minimum of 0. This indicates that there are

Table 2. Summary of descriptive analysis

Variables	Min	Max	Mean	SD
VCRD	0.00	139.00	19.75	21.77
SIZE	16327.10	14996650.00	918799.10	1832746.38
PRF	-17.63	95.18	10.61	12.40827
LIQ	0.25	10.60	1.81	1.33342
LEV	1.06	18.26	2.64	2.41255
BETA	-81.04	55.33	3.90	14.21712
MKTGRW	0.00	701.02	22.05	75.39021
			N	Percentage (%)
KI	Dummy	= 1	34	34
		= 0	66	66

Source(s): Author's own work

companies with no cybersecurity-related disclosures in their annual reports and a high spread in cybersecurity disclosure patterns among these companies.

The “firm size” indicates that there is a high variation, as companies have maximum total assets of INR 1,49,96,650 million and a minimum of INR 16,327.10 million. This indicates that the selected companies are publicly visible. The “profitability” of a firm presents an average of 10.61%, varying between a minimum of –17.63 and a maximum of 95.18. Companies present, on average, a “liquidity” of 1.81%, varying between a minimum of 0.25 and a maximum of 10.60. Similarly, the average “leverage” of the sampled firms is 2.61, varying from 1.06 to 182.26. “Market growth” presents a mean value of 22.05%, with a maximum value of 701.02 and a minimum of 0%. “BETA” represents the relatively varying market risk, between –81.04% and 55.33%. Approximately 30% of the company’s observations correspond to knowledge-intensive firms.

4.2 Bivariate analysis

Table 3 shows the matrix of correlations between the dependent and independent variables. The results indicate that the dependent variable, VCRD, has a statistically significant correlation with firm size ($p < 0.01$), leverage ($p < 0.05$), and knowledge-intensive ($p < 0.05$). These results are consistent with the hypotheses presented in Section 2. By contrast, there is no correlation between VCRD and profitability, liquidity, beta, and market growth. The presence of a weak correlation between the predictors indicated a low level of multicollinearity.

4.3 Multivariate analysis

Table 4 contains a summary of the ordinary least squares for both models. To ensure robustness, the assumptions of the model were examined. The Value Inflated Factors (VIF) were used to assess multicollinearity, and it was discovered that the problem was minimal (VIF <10) (Table 4). The Durbin-Watson statistic was used to evaluate autocorrelation levels, which were within the range (max = 2.199). The multiple regression results show that the independent variables significantly predicted the extent of VCRD in both models ($p < 0.001$), indicating that firm characteristics significantly impact the extent of VCRD (Table 4). The adjusted R -squared for the base model was 0.253, indicating a 25.3% variance in the extent of VCRD (Table 4).

According to H1, the data supports a positive relationship between firm size and VCRD. The firm-size coefficients are positive and statistically significant, leading to the acceptance of H1. This finding supports agency theory’s contention that large organizations are more inclined to provide more voluntary disclosures as they are under greater pressure from stakeholders who closely watch them (Watts and Zimmerman, 1983). Additionally, it can be seen that larger firms disclose more cybersecurity information to reduce potential damage to

Table 3. Bivariate analysis

Variables	VCRD	SIZE	LIQ	LEV	PRF	BETA	MKT-GRW	KI
VCRD	1							
SIZE	0.329**	1						
PRF	–0.101	–0.284**	1					
LIQ	–0.152	–0.293**	0.112	1				
LEV	0.203*	0.272**	–0.334**	0.335**	1			
BETA	0.135	0.064	–0.113	–0.148	–0.270**	1		
MKTGRW	–0.025	–0.133	–0.166	–0.076	0.528**	–0.092	1	
KI	0.217*	–0.099	–0.038	–0.190	–0.039	–0.039	0.109	1

Source(s): Author’s own work

Table 4. Multiple regression results

Coefficients	Sign	Normal regression		Model 2		Rank transform regression		Model 4		Expanded regression	
		Model 1				Model 3				Model 5	
		β	t	β	t	β	t	β	t	β	t
Constant			−4.460***		6.994***		2.058**		5.305***		−4.401***
SIZE	+	0.441	4.889***	0.331	2.875***	0.442	4.960***	0.366	3.448***	0.472	4.983***
LIQ	+	0.011	0.109	0.019	0.166	−0.021	−0.040	−0.039	−0.343	−0.01	0.993
LEV	+	0.359	2.815**	0.445	2.952**	0.337	2.669**	0.406	3.026**	−0.361	2.762**
PRF	+	0.019	0.190	0.012	0.110	−0.044	−0.014	−0.023	−0.218	−0.010	0.920
MKTGRW	+	−0.182	−1.698*	−0.089	−0.336	−0.170	−1.610	−0.317	−1.179	−0.172	−1.604
BETA	+	0.257	2.571**	0.268	2.495**	0.223	2.264**	0.240	2.226**	0.259	2.560**
KI	+			0.249	2.680**			0.220	2.341**		
KI*SIZE	+			0.144	1.368			0.220	1.125		
KI* PRF	+			0.055	0.038			0.073	0.584		
KI* LEV	+			−0.407	−1.678*			−0.251	−1.023		
KI* LIQ	+			−0.1663	−1.232			−0.141	−1.073		
KI* BETA	+			0.718	0.475			−0.015	−0.143		
KI* MKTGRW	+			0.173	0.598			0.327	0.996		
BSIZE										−0.142	1.485
INDEP										0.096	0.911
DUAL										0.01	0.005
MEET										−0.099	−0.980
Adj r^2			0.253		0.315		0.272		0.299		0.252
Durbin-Watson			2.199		2.107		2.178		2.220		2.150
Max VIF			2.026		2.372		2.030		2.266		2.125
f statistics			6.242***		4.293***		6.789***		4.048***		4.139***
Observations			100		100		100		100		100

Source(s): Author's own work

the reputation and fulfil the demands of multiple stakeholders (Lenka *et al.*, 2023). These results are similar to those of the previous studies (Li *et al.*, 2018; Gao *et al.*, 2020).

The profitability results are inconsistent with the study's hypothesis, thus rejecting H2. The relationship between profitability and VCRD contradicts the agency theory, which states managers tend to disclose more risk-related information in highly profitable companies. However, the non-significant relationship shows the managerial maturity of Indian companies, as disclosing cybersecurity risk information with the market is driven by competitiveness among the firm industries and not profitability. Further, the results of these studies are in line with those of Ettredge *et al.* (2018), who report that profitability is not an incentive to adopt cybersecurity risk management. Additionally, the insignificant relationship can be understood through the stakeholder theory perspective, VCRD aimed to address the concerns of a wide range of stakeholders, who may prioritize transparency in cybersecurity risk management over profitability.

The multivariate results show an insignificant relationship between liquidity and VCRD, thus rejecting H3. The results contradicted agency theory, which states that high-liquid firms may disclose higher voluntary information to distinguish themselves from those with a liquidity ratio. However, if agency theory does not explain VCRD well, the size phenomenon may be related to the costs of cybersecurity risk management and competitive advantages rather than agency costs.

Table 4 shows that the variable leverage significantly relates to the VCRD level, thus supporting hypothesis H4. The results hold to the agency theory, which states that companies with high leverage ratios posit high risks and tend to disclose more information (Jensen and Meckling, 1976). The positive results highlighted the commitments of sampled companies toward their creditors and investors, who can fulfil their long- and short-term obligations despite the company's cyber security threat. Further, the findings can be explained by the fact that leverage is more linked to shareholders' powers, implying that a high debt ratio relative to equities leads to more cybersecurity risk-related disclosures. The results are consistent with the empirical risk disclosure literature (Elshandidy *et al.*, 2013; Pooser *et al.*, 2018).

The variable market growth had a negative but weak statistically significant association with VCRD. The results failed to provide empirical support for H5 and were inconsistent with Elshandidy *et al.* (2018) hypothesis that a firm's growth has significantly positive results with risk disclosure. However, a possible reason for the inverse relationship between a company's growth and VCRD is that companies with high potential market growth seeking broader financial expansion may need to pay more attention to the downplay of adequately disclosing cybersecurity risks. This may help them to hide cyber threats from stakeholders, such as investors, to reduce the company's reputational risks.

BETA had a significant positive association with VCRD, consistent with Hypothesis H6. The relationship between systematic risk and VCRD supports the notion of agency and signalling theories, suggesting that when a firm has a high degree of risk, managers receive greater consideration from stakeholders to disseminate more risk-related information (Elshandidy *et al.*, 2013). This shows that a company with a high systematic risk in the market that disseminates cyber security risks more transparently ensures investor confidence in such threats.

4.3.1 The moderating effect of the KI industry sector. Model 2 tests the moderating effect of the knowledge-intensive industry on the relationship between firm characteristics and VCRD levels. The findings highlight that VCRD disclosure is more pronounced in the KI industry (see Table 4). This can be understood with intellectual capital theory, which states that knowledge-intensive industries have a high value of intangible assets and these assets provide a competitive advantage to the company, leading to a better disclosure of cybersecurity risks. Further, VCRD in knowledge-intensive industry is higher because of the nature of the industry, which involves significant data security and privacy risks. The high level of public concern over data breaches and cyberattacks has led to increased pressure on knowledge-intensive

companies to disclose information regarding their security measures and data protection policies.

Further, it shows that only LEV and knowledge-intensive industry interaction (LEV*KI) have a weak significant negative relationship with the extent of VCRD (Table 4). This implies that with increased knowledge intensity, the impact of LEV is reduced in VCRD. The findings are consistent with the meta-analysis results of Khlif and Hussainey (2014), which highlight that industry type moderates the association between risk disclosure and financial leverage.

4.4 Additional analysis

The current study performs two additional statistical analyses to examine the robustness of the regression results. First, this study uses the rank transformation model to check the sensitivity of the results. A rank transformation was performed because it did not violate the assumptions of normality, homogeneity of variance, and outliers (Aly *et al.*, 2010). This study transformed the continuous dependent variable (VCRD) and the independent variable (firm size) into their ranks before running the regression using the formulae given by Lang and Lundholm (1993), as shown in the equation.

$$\text{Rank percentile} = \frac{\text{Rank} - 1}{\text{Number of companies} - 1}$$

The rank transforms ordinary least squares results are similar to those of the standard regression, as shown in Models 3 and 4 (Table 4). Thus, the rank transform regression model validates the results of the current study.

Secondly, following Nahar *et al.* (2016), the study re-estimated the hypothesis variables, including control variables, specifically board size, board independence, CEO duality and number of board meetings in a year. Mazumder and Hossain (2022) argue that the board of directors should be vigilant about the firm's exposure to cyber threats and play a proactive role in minimizing cyber risk. According to agency theory, the board of directors is the key monitoring apparatus of managerial actions and corporate accountability (Mazumder and Hossain, 2022). Table 4 (model 5) reports the results of hypothesis variables with additional control variables. The results of this inclusion remain the substantive significance of the coefficients reported in Table 4 (model 1).

4.5 Endogeneity issue analysis

Endogeneity is the primary concern of the disclosure studies. To minimize the endogeneity, the study employs an entropy balancing approach to more effectively minimize the variations in observable variables across the treatment and control groups. Entropy balancing is an approach which ensures that covariate imbalances improve after matching (Hainmueller, 2012). It also boosts the power of tests by minimizing data loss (Hossain and Kryzanowski, 2021). This balancing method to treat the endogeneity problem has been widely used in recent years (Ongsakul *et al.*, 2022; Hossain and Kryzanowski, 2021). To start entropy balancing, the paper divided the sample companies into four quartiles in terms of beta (market risk) because companies are likely to have higher market risk, making them a suitable group for analysing the impact of VCRD. To prepare the data, the study creates a binary variable where 1 indicates the treatment group, which had the companies in the top quartile as per beta and 0 for the control group (companies in the other three quartiles as per beta). After that, the study selected the covariates (independent variables other than beta like firm size, leverage, liquidity, etc.) that need to be balanced. Then, to conduct the test, the study used the default setup on Stata code provided by Hainmueller (2012) to converge on the sample means and skewness of covariates, which the sample data achieved in Panel A, Table 5. Panel B (Table 5) shows the multiple regression analysis using the sample constructed by entropy balancing. The results are consistent with the paper's baseline results (Table 4).

Table 5. Entropy balancing

Panel A						
Before: without entropy balancing						
Treat				Control		
	Mean	Variance	Skewness	Mean	Variance	Skewness
PRF	9.224	72.61	0.406	14.67	381.7	2.999
LEV	1.743	1.795	4.358	2.017	1.747	2.304
LIQ	2.527	2.004	1.434	2.993	17.35	3.017
MKTGRW	14.69	780	4.987	43.59	19989	4.453
SIZE	5.95	0.1121	0.7025	6.021	0.2078	1.122
After: with entropy balancing						
Treat				Control		
	Mean	Variance	Skewness	Mean	Variance	Skewness
PRF	9.224	72.61	0.406	9.223	72.61	6.104
LEV	1.743	1.795	4.358	1.743	1.795	3.177
LIQ	2.527	2.004	1.434	2.527	2.004	6.007
MKTGRW	14.69	780	4.987	14.7	780.9	19.51
SIZE	5.95	0.1121	0.7025	5.95	0.1121	1.859
Panel B: regression results using entropy balancing sample						
	Model 1 (without moderation)			Model 2 (with moderation)		
Coefficients	<i>t</i>	<i>p</i> > 0.05		<i>t</i>	<i>p</i> > 0.05	
Constant	−4.57	0.000		10.67	0.000	
SIZE	5.14	0.000		3.90	0.000	
LIQ	−0.95	0.343		0.43	0.667	
LEV	1.87	0.064		2.74	0.007	
PRF	−0.19	0.853		0.14	0.886	
MKTGRW	−0.68	0.497		0.68	0.497	
BETA	2.28	0.025		2.57	0.012	
KI				2.23	0.028	
KI*SIZE				1.60	0.113	
KI* PRF				−0.43	0.667	
KI* LEV				−1.88	0.063	
KI* LIQ				−1.78	0.079	
KI* BETA				−0.04	0.968	
KI* MKTGRW				−0.38	0.704	
R-squared		0.255			0.332	
Source(s): Author's own work						

5. Conclusion

Companies' increasing reliance on Internet-connected systems has also increased the risk of cyber threats, making cyber security crucial for protecting sensitive data and systems from unauthorized access, theft, and damage. Therefore, this study measured the VCRD in the annual reports of the top 100 non-financial BSE-listed Indian companies. It also measured the relationship between key firm characteristics and the level of VCRD. The results of the study indicate that among the identified keywords, on average, 20% of companies disclose their cybersecurity risk information, which is lower than in studies in other parts of the world (Calderon and Gao, 2020; Berkman *et al.*, 2018; Li *et al.*, 2018). The reason for lower VCRD is that they are not mandatory for Indian companies. This supports the interest of regulators in establishing disclosure policy within a framework to ensure consistency in cybersecurity risk

disclosure. Regulators should recognize those companies through rewards to improve cybersecurity risk transparency and disclosure. Furthermore, the results reveal that firm size, leverage, market risk, and growth affect VCRD in India. The results support the theoretical arguments of agency and signalling theories. The literature suggests that cyber threats have the potential to impact a company's reputation (Kamiya *et al.*, 2021; Gao *et al.*, 2020). The current study found that Indian companies use VCRD to mitigate litigation risks and potential reputational damage, as firm size significantly affects the VCRD. These results align with Oliveira *et al.* (2011) argument that larger firms are more visible to relevant stakeholders and are more likely to consider risk disclosure as a way to enhance corporate reputation through higher disclosure.

This study adds to the cybersecurity disclosures literature from a theoretical perspective. This study is the first to explore the potential factors affecting cybersecurity risk disclosure in developing economies, specifically India, although this is a pressing issue. It finds that despite the lack of stringent regulatory frameworks that can mandate such disclosures, Indian firms have opted for disclosures. The results of the Indian context also have to be considered in the context of wider regions, i.e. SAARC and ASEAN. Raska and Ang (2018) mentioned that cyber risks impede trust in the digital economy and prevent the ASEAN region from realizing its full potential. Therefore, the management of different companies can take insight from the results and emphasize strengthening the cybersecurity risk disclosure in their annual report to benefit external investors for better investment opportunities.

The study's results significantly impact companies seeking to enhance their cybersecurity structure and improve stakeholder confidence. HBGray (2013) reported that 70% of US investors are interested in reviewing companies' cybersecurity practices to assist in their investment decisions. D'Arcy and Basoglu (2022) found that public attention positively relates to cybersecurity risk disclosure. Based on this, it is assumed that the public appreciates the importance of cybersecurity disclosure, which influences their valuation of the firm. Hence, companies should be more aggressive in disclosing cybersecurity risks because the public acts as a moral authority.

Furthermore, the findings provide a valuable policy foundation for governments and regulatory entities to enhance their cybersecurity policies. Indian companies are not obliged to report such information because it is not material. It is suggested that Indian regulators may put it in place, and if not, why not approach the USA. The regulators can implement systems that increase public awareness of firm data breaches. For example, the Ministry of Corporate Affairs India can have a dedicated web page to make the public aware of the cybersecurity threats among corporate companies and disclose the potential risks of investment among companies with data breaches. Similarly, the Security and Exchange Board of India should enhance the requirement to disclose material cybersecurity incidents among Indian companies within the specified period. In addition to that, in the regional context, Asian countries can maximize existing important forums, such as SAARC and ASEAN Regional Forum, to add cybersecurity as the top priority in coming up with a unifying framework for the companies.

This study has several limitations. The Python code used in the study lacks sentiment analysis, identifying whether keywords are used positively or negatively. Further studies should include large language models in the code for further in-depth analyses such as sentiment and quality analysis. Furthermore, the research can extend to financial companies as the results are limited to non-financial companies. Future studies could also study in detail the corporate governance characteristics and cybersecurity disclosures, as the study found insignificant relationships. Lastly, investigating the perceptions and expectations of various internal and external stakeholders regarding cybersecurity risks can provide valuable insight.

Notes

1. <https://id4d.worldbank.org/guide/data-protection-and-privacy-laws>
2. <https://www.spglobal.com/spdji/en/indices/equity/sp-bse-200/#overview>

References

- Aly, D., Simon, J. and Hussainey, K. (2010), "Determinants of corporate internet reporting: evidence from Egypt", *Managerial Auditing Journal*, Vol. 25 No. 2, pp. 182-202, doi: [10.1108/02686901011008972](https://doi.org/10.1108/02686901011008972).
- Berkman, H., Jona, J., Lee, G. and Soderstrom, N. (2018), "Cybersecurity awareness and market valuations", *Journal of Accounting and Public Policy*, Vol. 37 No. 6, pp. 508-526, doi: [10.1016/j.jaccpubpol.2018.10.003](https://doi.org/10.1016/j.jaccpubpol.2018.10.003).
- Bueno, E., Salmador, M.P., Rodríguez, Ó. and Martín De Castro, G. (2006), "Internal logic of intellectual capital: a biological approach", *Journal of Intellectual Capital*, Vol. 7 No. 3, pp. 394-405, doi: [10.1108/14691930610681474](https://doi.org/10.1108/14691930610681474).
- Calderon, T.G. and Gao, L. (2020), "Cybersecurity risks disclosure and implied audit risks: evidence from audit fees", *International Journal of Auditing*, Vol. 25 No. 1, pp. 24-39, doi: [10.1111/ijau.12209](https://doi.org/10.1111/ijau.12209).
- Cheng, E.C.M. and Courtenay, S.M. (2006), "Board composition, regulatory regime and voluntary disclosure", *The International Journal of Accounting*, Vol. 41 No. 3, pp. 262-289, doi: [10.1016/j.intacc.2006.07.001](https://doi.org/10.1016/j.intacc.2006.07.001).
- Cheng, L., Liu, F. and Yao, D.D. (2017), "Enterprise data breach: causes, challenges, prevention, and future directions", *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, Vol. 7 No. 5, p. e1211, doi: [10.1002/widm.1211](https://doi.org/10.1002/widm.1211).
- D'Arcy, J. and Basoglu, A. (2022), "The influences of public and institutional pressure on firms' cybersecurity disclosures", *Journal of the Association for Information Systems*, Vol. 23 No. 3, pp. 779-805, doi: [10.17705/1jais.00740](https://doi.org/10.17705/1jais.00740).
- Deloitte (2023), "Global cyber executive briefing", available at: <https://www2.deloitte.com/tw/en/pages/risk/articles/High-Technology-Sector.html>
- Elshandidy, T., Fraser, I. and Hussainey, K. (2013), "Aggregated, voluntary, and mandatory risk disclosure incentives: evidence from UK FTSE all-share companies", *International Review of Financial Analysis*, Vol. 30, pp. 320-333, doi: [10.1016/j.irfa.2013.07.010](https://doi.org/10.1016/j.irfa.2013.07.010).
- Elshandidy, T., Fraser, I. and Hussainey, K. (2015), "What drives mandatory and voluntary risk reporting variations across Germany, UK and US?", *The British Accounting Review*, Vol. 47 No. 4, pp. 376-394, doi: [10.1016/j.intacc.2016.10.001](https://doi.org/10.1016/j.intacc.2016.10.001).
- Elshandidy, T., Neri, L. and Guo, Y. (2018), "Determinants and impacts of risk disclosure quality: evidence from China", *Journal of Applied Accounting Research*, Vol. 19 No. 4, doi: [10.1108/JAAR-07-2016-0066](https://doi.org/10.1108/JAAR-07-2016-0066).
- Ettredge, M., Guo, F. and Li, Y. (2018), "Trade secrets and cyber security breaches", *Journal of Accounting and Public Policy*, Vol. 37 No. 6, pp. 564-585, doi: [10.1016/j.jaccpubpol.2018.10.006](https://doi.org/10.1016/j.jaccpubpol.2018.10.006).
- EY (2021), "EY global information security survey India edition 2021", available at: https://www.ey.com/en_in/cybersecurity/ey-global-information-security-survey-india-edition-2021
- Gao, L., Calderon, T.G. and Tang, F. (2020), "Public companies' cybersecurity risk disclosures", *International Journal of Accounting Information Systems*, Vol. 38, 100468, doi: [10.1016/j.accinf.2020.100468](https://doi.org/10.1016/j.accinf.2020.100468).
- Gatzert, N. and Schubert, M. (2022), "Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value", *Journal of Risk and Insurance*, Vol. 89 No. 3, pp. 725-763, doi: [10.1111/jori.12381](https://doi.org/10.1111/jori.12381).
- Gaver, J.J. and Gaver, K.M. (1993), "Additional evidence on the association between the investment opportunity set and corporate financing, dividend, and compensation policies", *Journal of Accounting and Economics*, Vol. 16 Nos 1-3, pp. 125-160, doi: [10.1016/0165-4101\(93\)90007-3](https://doi.org/10.1016/0165-4101(93)90007-3).
- Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015), "Increasing cybersecurity investments in private sector firms", *Journal of Cybersecurity*, Vol. 1 No. 1, pp. 3-17, doi: [10.1093/cybsec/tyv011](https://doi.org/10.1093/cybsec/tyv011).

- Goswami, M. (2018), *Intellectual Capital and Firm Performance in Indian Manufacturing Sector: An Empirical Investigation*, North-Eastern Hill University, Shillong.
- Hainmueller, J. (2012), "Entropy balancing for causal effects: a multivariate reweighting method to produce balanced samples in observational studies", *Political Analysis*, Vol. 20 No. 1, pp. 25-46, doi: [10.1093/pan/mpr025](https://doi.org/10.1093/pan/mpr025).
- HBGary (2013), "Cybersecurity directly affects investor attitudes, new HBGary survey finds", available at: <https://www.prnewswire.com/news-releases/cybersecurity-directly-affects-investor-attitudes-new-hbgary-survey-finds-193105951.html>
- Héroux, S. and Fortin, A. (2020), "Cybersecurity disclosure by the companies on the S&/TSX 60 Index", *Accounting Perspectives*, Vol. 19 No. 2, pp. 73-100, doi: [10.1111/1911-3838.12220](https://doi.org/10.1111/1911-3838.12220).
- Higgs, J.L., Pinsker, R.E., Smith, T.J. and Young, G.R. (2016), "The relationship between board-level technology committees and reported security breaches", *Journal of Information Systems*, Vol. 30 No. 3, pp. 79-98, doi: [10.2308/isy-51402](https://doi.org/10.2308/isy-51402).
- Hossain, A.T. and Kryzanowski, L. (2021), "Political corruption and corporate social responsibility (CSR)", *Journal of Behavioral and Experimental Finance*, Vol. 31, 100538, doi: [10.1016/j.jbef.2021.100538](https://doi.org/10.1016/j.jbef.2021.100538).
- Huang, K., Wang, X., Wei, W. and Madnick, S. (2023), "The devastating business impacts of a cyber breach", *Harvard Business Review*, available at: <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>
- Jensen, M.C. and Meckling, W.H. (1976), "Theory of the firm: managerial behavior, agency costs and ownership structure", *Journal of Financial Economics*, Vol. 3 No. 4, pp. 305-360, doi: [10.1016/0304-405x\(76\)90026-x](https://doi.org/10.1016/0304-405x(76)90026-x).
- Jorgensen, B.N. and Kirschenheiter, M.T. (2003), "Discretionary risk disclosures", *The Accounting Review*, Vol. 78 No. 2, pp. 449-469, doi: [10.2308/accr.2003.78.2.449](https://doi.org/10.2308/accr.2003.78.2.449).
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. and Stulz, R.M. (2021), "Risk management, firm reputation, and the impact of successful cyberattacks on target firms", *Journal of Financial Economics*, Vol. 139 No. 3, pp. 719-749, doi: [10.1016/j.jfineco.2019.05.019](https://doi.org/10.1016/j.jfineco.2019.05.019).
- Kanto, A.J. and Schadewitz, H.J. (1997), "A multidimensional model for the disclosure policy of a firm", *Scandinavian Journal of Management*, Vol. 13 No. 3, pp. 229-249, doi: [10.1016/s0956-5221\(97\)00007-9](https://doi.org/10.1016/s0956-5221(97)00007-9).
- Kelton, A.S. and Pennington, R.R. (2019), "Do voluntary disclosures mitigate the cybersecurity breach contagion effect?", *Journal of Information Systems*, Vol. 34 No. 3, pp. 133-157, doi: [10.2308/isy-52628](https://doi.org/10.2308/isy-52628).
- Khalil, A. and Maghraby, M. (2017), "The determinants of internet risk disclosure: empirical study of Egyptian listed companies", *Managerial Auditing Journal*, Vol. 32 No. 8, pp. 746-767, doi: [10.1108/maj-04-2016-1370](https://doi.org/10.1108/maj-04-2016-1370).
- Khalique, M., Shaari, J.A.N.B. and Isa, A.H.B.M. (2013), "The road to the development of intellectual capital theory", *International Journal of Learning and Intellectual Capital*, Vol. 10 No. 2, p. 122, doi: [10.1504/ijlic.2013.052953](https://doi.org/10.1504/ijlic.2013.052953).
- Khlif, H. and Hussainey, K. (2014), "The association between risk disclosure and firm characteristics: a meta-analysis", *Journal of Risk Research*, Vol. 19 No. 2, pp. 181-211, doi: [10.1080/13669877.2014.961514](https://doi.org/10.1080/13669877.2014.961514).
- Kshetri, N. (2017), "Blockchain's roles in strengthening cybersecurity and protecting privacy", *Telecommunications Policy*, Vol. 41 No. 10, pp. 1027-1038, doi: [10.1016/j.telpol.2017.09.003](https://doi.org/10.1016/j.telpol.2017.09.003).
- Lang, M. and Lundholm, R. (1993), "Cross-sectional determinants of analyst ratings of corporate disclosures", *Journal of Accounting Research*, Vol. 31 No. 2, p. 246, doi: [10.2307/2491273](https://doi.org/10.2307/2491273).
- Lenka, A., Goswami, M., Singh, H. and Baskaran, H. (2023), "Cybersecurity disclosure and corporate reputation", in *Advances in Information Security, Privacy, and Ethics Book Series*, IGI Global, pp. 169-183, doi: [10.4018/978-1-6684-9018-1.ch008](https://doi.org/10.4018/978-1-6684-9018-1.ch008).

- Li, H., No, W.G. and Wang, T. (2018), "SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors", *International Journal of Accounting Information Systems*, Vol. 30, pp. 40-55, doi: [10.1016/j.accinf.2018.06.003](https://doi.org/10.1016/j.accinf.2018.06.003).
- Linsley, P.M. and Shrives, P.J. (2006), "Risk reporting: a study of risk disclosures in the annual reports of UK companies", *The British Accounting Review*, Vol. 38 No. 4, pp. 387-404, doi: [10.1016/j.bar.2006.05.002](https://doi.org/10.1016/j.bar.2006.05.002).
- Madhani, P.M. (2016), "Corporate governance and disclosure practices of firms: the impact of nature and types of intellectual capital", *The IUP Journal of Corporate Governance*, Vol. 15 No. 3, pp. 7-35, available at: <https://ssrn.com/abstract=2828539>
- Masoud, N. and Al-Utaibi, G. (2022), "The determinants of cybersecurity risk disclosure in firms' financial reporting: empirical evidence", *Research in Economics*, Vol. 76 No. 2, pp. 131-140, doi: [10.1016/j.rie.2022.07.001](https://doi.org/10.1016/j.rie.2022.07.001).
- Mazumder, M.M.M. and Hossain, D.M. (2022), "Voluntary cybersecurity disclosure in the banking industry of Bangladesh: does board composition matter?", *Journal of Accounting in Emerging Economies*, Vol. 13 No. 2, pp. 217-239, doi: [10.1108/jaee-07-2021-0237](https://doi.org/10.1108/jaee-07-2021-0237).
- Morse, E.A., Raval, V. and Wingender, J.R. (2017), "SEC cybersecurity guidelines: insights into the utility of risk factor disclosures for investors", *The Business Lawyer*, Vol. 73 No. 1, pp. 1-34.
- Nahar, S., Azim, M. and Jubb, C. (2016), "The determinants of risk disclosure by banking institutions: evidence from Bangladesh", *Asian Review of Accounting*, Vol. 24 No. 4, pp. 426-444, doi: [10.1108/ARA-07-2014-0075](https://doi.org/10.1108/ARA-07-2014-0075).
- Ocean Tomo (2020), "Intangible asset market value study", available at: www.Oceantomo.Com
- OECD (1999), *OECD Science, Technology and Industry Scoreboard 1999; Benchmarking Knowledge - Based Economies*, OECD Publishing, Paris.
- Oliveira, J., Rodrigues, L.L. and Craig, R. (2011), "Voluntary risk reporting to enhance institutional and organizational legitimacy", *Journal of Financial Regulation and Compliance*, Vol. 19 No. 3, pp. 271-289, doi: [10.1108/13581981111147892](https://doi.org/10.1108/13581981111147892).
- Ongsakul, V., Jaroenjitrkam, A., Treepongkaruna, S. and Jiraporn, P. (2022), "Does board gender diversity reduce 'CEO luck'", *Accounting and Finance*, Vol. 62 No. 1, pp. 243-260, doi: [10.1111/acfi.12788](https://doi.org/10.1111/acfi.12788).
- Otcenášková, T., Bureš, V. and Mikuleck_A, J. (2012), "Principal starting points of organizational knowledge intensity modelling", *Journal of Organizational Knowledge Management*, Vol. 2012, pp. 1-12, doi: [10.5171/2012.453016](https://doi.org/10.5171/2012.453016).
- Pooser, D.M., Browne, M.J. and Arkhangelska, O. (2018), "Growth in the perception of cyber risk: evidence from US P&C insurers", *The Geneva Papers on Risk and Insurance - Issues and Practice*, Vol. 43 No. 2, pp. 208-223, doi: [10.1057/s41288-017-0077-9](https://doi.org/10.1057/s41288-017-0077-9).
- Radu, C. and Smaili, N. (2021), "Board gender diversity and corporate response to cyber risk: evidence from cybersecurity related disclosure", *Journal of Business Ethics*, Vol. 177 No. 2, pp. 351-374, doi: [10.1007/s10551-020-04717-9](https://doi.org/10.1007/s10551-020-04717-9).
- Raska, M. and Ang, B. (2018), *Cybersecurity in Southeast Asia*, Asia Centre & DGRIS, Paris, available at: https://asiacentre.eu/wp-content/uploads/2021/11/NotePresentation-AngRaska-Cybersecurity_180518.pdf
- SEC (2018), "Commission statement and guidance on public company cybersecurity disclosures", available at: <https://www.sec.gov/rules/interp/2018/33-10459.pdf>
- Singhanian, A.K. and Panda, N.M. (2022), "Does AC effectiveness mediate the relationship between knowledge intensity and firm performance? Evidence from India", *Journal of Financial Reporting and Accounting*, Vol. ahead-of-print No. ahead-of-print, doi: [10.1108/JFRA-06-2022-0214](https://doi.org/10.1108/JFRA-06-2022-0214).
- Tawalbeh, L., Muheidat, F., Tawalbeh, M. and Quwaider, M. (2020), "IoT privacy and security: challenges and solutions", *Applied Sciences*, Vol. 10 No. 12, p. 4102, doi: [10.3390/app10124102](https://doi.org/10.3390/app10124102).

- Ting, I.W.K., Ren, C., Chen, F.-C. and Kweh, Q.L. (2020), "Interpreting the dynamic performance effect of intellectual capital through a value-added-based perspective", *Journal of Intellectual Capital*, Vol. 21 No. 3, pp. 381-401, doi: [10.1108/JIC-05-2019-0098](https://doi.org/10.1108/JIC-05-2019-0098).
- Walton, S., Wheeler, P.R., Zhang, Y.I. and Zhao, X.R. (2020), "An integrative review and analysis of cybersecurity research: current state and future directions", *Journal of Information Systems*, Vol. 35 No. 1, pp. 155-186, doi: [10.2308/isys-19-033](https://doi.org/10.2308/isys-19-033).
- Watson, A., Shrivies, P. and Marston, C. (2002), "Voluntary disclosure of accounting ratios in the UK", *The British Accounting Review*, Vol. 34 No. 4, pp. 289-313, doi: [10.1006/bare.2002.0213](https://doi.org/10.1006/bare.2002.0213).
- Watts, R.L. and Zimmerman, J.L. (1983), "Agency problems, auditing, and the theory of the firm: some evidence", *The Journal of Law and Economics*, Vol. 26 No. 3, pp. 613-633, doi: [10.1086/467051](https://doi.org/10.1086/467051).

Corresponding author

Harmandeep Singh can be contacted at: har90bal@gmail.com