ISSN 1611-1699 / eISSN 2029-4433

VILNIUS TECH
Vilnius Gediminas Technical University

JOURNAL of BUSINESS ECONOMICS & MANAGEMENT

2026
Volume 27
Issue 2
Pages 323–343

https://doi.org/10.3846/jbem.2026.25751

TRUST IN THE DIGITAL AGE: HOW CYBERSECURITY GOVERNANCE WILLINGNESS SHAPES TRADE CREDIT – EVIDENCE FROM SUPPLIER CREDIT DECISIONS

Ding LI [1], Han YAN [2]✉, Shenglin MA [3]

[1]School of Economic and Management, Heilongjiang Bayi Agricultural University, Heilongjiang, China
[2]School of Business, Nan Kai University, Tianjin, China
[3]School of Economics and Management, North University of China, Taiyuan, China

Article History:
- received 17 November 2024
- accepted 25 November 2025

Abstract. In the digital economy, the importance of robust cybersecurity governance for corporate financing stability has become increasingly salient. Using a sample of Chinese A-share listed companies from 2011 to 2023, we employ the Word2vec natural language processing technique to develop a measure of corporate cybersecurity governance commitment. Our study empirically examines its impact on trade credit financing. The results indicate that a firm's expressed commitment to cybersecurity governance is positively associated with the trade credit it receives from suppliers. We find that information asymmetry and corporate reputation are key mechanisms through which this effect operates. Heterogeneity analysis reveals that this effect is more pronounced for firms that have received regulatory inquiry letters, those without political ties, those operating during periods of high economic policy uncertainty, and those located in regions with low social trust. Furthermore, we show that when firms' stated commitments align with their actions, suppliers adjust their business relationships by allocating a greater share of procurement volume to them, thereby strengthening long-term supply chain trust. Our findings offer valuable insights for firms in emerging economies seeking to enhance their cybersecurity governance and optimize their financing environment.

Keywords: cybersecurity governance commitment, supplier credit, trade credit, signaling theory, Word2vec text analysis, corporate reputation.

JEL Classification: G32, G41, L14.

✉Corresponding author. E-mail: ***haccept@163.com***

1. Introduction

The rapid development of global information technology and cyberspace has led to a continuous rise in the frequency and cost of cyberattacks and data breaches (Kamiya et al., 2021). Industry reports consistently show that cybercrime has evolved into a global systemic risk. Morgan (2020) notes that since 2007, a cyberattack has occurred on average every 39 seconds worldwide, with the economic damage from cybercrime projected to reach $10.5 trillion by 2025. IBM (2024) further reports that in 2024, the average cost of a global data breach hit a record high of $4.88 million. High-profile incidents, such as the major attack on Yahoo in 2013 (which compromised approximately 3 billion accounts and resulted in losses exceeding $350 million) and the recent

"largest-scale IT failure in history" caused by a CrowdStrike software vulnerability (which impacted nearly 30,000 businesses and government agencies and severely compromised the security of the Microsoft ecosystem), underscore a critical shift (Janakiraman et al., 2018; Kamiya et al., 2021; Zhu et al., 2024). These events demonstrate that cybersecurity is no longer merely a technical issue but a central concern for global economic stability and a driver of long-term corporate development (Yarovenko et al., 2021; Silva Atencio, 2025).

Prior research offers extensive evidence on the economic consequences of cybersecurity, covering market value (Cavusoglu et al., 2004; Berkman et al., 2018), reputation (Steinbart et al., 2013), cash holdings (Garg, 2020), customer trust (Eisenbach et al., 2022), and innovation (Wang et al., 2024). Yet most studies emphasize post-incident outcomes, focusing on how exogenous shocks such as cyberattacks affect firms' market and financial performance, while overlooking the signaling role of governance willingness prior to risks. In contexts without mandatory disclosure, governance willingness is a prerequisite for cyber risk management (Gatzert & Schubert, 2022). It influences firms' future actions, is perceived by stakeholders, shapes risk assessments and decisions, and ultimately affects long-term relationships with supply chain partners (Lattanzio & Ma, 2023; Florackis et al., 2023).

Trade credit is a critical component of supply chain management and is widely used in regions with imperfect capital markets due to its interest-free and collateral-free nature (Kong et al., 2020; Zhou et al., 2024). More specifically, trade credit is a short-term credit facility provided by suppliers when they offer products or raw materials on deferred payment terms. By building trust with suppliers, a firm can secure flexible payment conditions and alleviate short-term liquidity pressures. Through trade credit, upstream and downstream firms form a tight-knit supply chain network where they are mutually interdependent (Alfaro et al., 2021; Crosignani et al., 2023). In this network, both risks and signals can diffuse along the supply chain. On one hand, a buyer's operational risk can be amplified and transmitted to the supplier, leading to a tightening of credit. On the other hand, a buyer's improved performance or governance behavior can also send positive signals, enhancing a supplier's confidence in the buyer's stability and leading to more lenient credit terms (Tan et al., 2025). According to signaling theory, in an environment of information asymmetry, a firm's specific actions can serve as credible signals that influence the perceptions of external parties. A firm's commitment to cybersecurity governance, as a prerequisite for cyber risk management (Gatzert & Schubert, 2022), is precisely this type of "informal but recognizable" signal. Therefore, we hypothesize that suppliers, when evaluating credit risk, may factor in a firm's expressed cybersecurity governance commitment and adjust the size or terms of trade credit accordingly.

China's rapidly developing digital economy and growing cybersecurity risks provide a unique context for studying corporate cybersecurity governance commitment. According to Deloitte (2021), China has become a major player in the global digital economy. Further data from the China Academy of Information and Communications Technology (2023) reveals that the scale of China's digital economy reached 50.2 trillion yuan in 2022, accounting for 41.5% of the national GDP. This rapid expansion, particularly in areas like cloud computing, AI, and big data, has significantly heightened corporate cybersecurity risks. This backdrop has prompted firms to prioritize cybersecurity governance and to articulate their commitment to it in public disclosures like annual reports. Furthermore, since 2017, China has introduced a series of regulations, including the "Cybersecurity Law", "Data Security Law", "Personal Information Protection Law", and "Cybersecurity Review Measures". These regulations have strengthened corporate information disclosure and compliance requirements. While they do not mandate the disclosure of governance commitment, they have increased the frequency and breadth of corporate cybersecurity-related discussions in their public documents, providing a strong

foundation for using text analysis to construct a governance commitment index.

Additionally, the unique characteristics of China's corporate financing landscape further enhance the value of this research. The Chinese economy is in a transition period, and its capital market system remains underdeveloped (Shahzad et al., 2022; Yan et al., 2025). Severe information asymmetry between banks and firms often leads banks to lend cautiously to mitigate risk, which in turn constrains the availability of corporate credit (Peón & Guntín, 2021; Yan et al., 2024). This makes supply chain trade credit a critical source of liquidity for Chinese firms (J. Chen et al., 2025). In an environment lacking formal credit ratings and mandatory governance disclosures, a firm's expressed governance commitment in its annual report often becomes key qualitative information for suppliers to assess operational stability and sustainability. Therefore, investigating how cybersecurity governance commitment influences supplier credit allocation decisions in the Chinese context is not only of practical significance but also provides valuable lessons for other emerging markets on how to use governance signals to optimize the financing environment.

Our study makes several key contributions to the literature. First, we expand the research on cybersecurity governance commitment by examining it from the perspective of supplier credit, thereby enriching the understanding of cybersecurity governance through the lens of signaling theory. Existing studies primarily investigate the economic impact of cybersecurity events from the perspectives of market reaction (Berkman et al., 2018; Kamiya et al., 2021), financial decisions (Garg, 2020), and stock price crash risk (Ball et al., 2012; Kim & Zhang, 2014). The limited literature on cybersecurity governance has focused on its effects on business stability, innovation, and financial performance (Dhillon & Backhouse, 2001; Berkman et al., 2018; Blind et al., 2024; Tan et al., 2025), with less attention paid to the signaling effect of a firm's expressed commitment. In contrast, by adopting a supplier credit perspective, our study provides a novel view on how cybersecurity governance commitment serves as crucial supplementary non-financial information in supplier lending decisions.

Second, our research complements the literature on the determinants of corporate trade credit by introducing the often-overlooked issue of cybersecurity in the digital economy. While previous studies have analyzed the factors influencing trade credit from both macro and micro perspectives (Benmelech et al., 2017; Kong et al., 2020; Fisman & Love, 2003), they have not considered the increasingly important role of corporate cybersecurity. As digital technology and the real economy become more deeply integrated, new technologies improve efficiency but also introduce new cybersecurity challenges. Based on signaling theory, our study comprehensively explores how a firm's commitment to cybersecurity governance affects its trade credit, thereby enriching the related body of research.

Finally, we leverage Word2vec deep learning and natural language processing techniques to construct a comprehensive cybersecurity governance index from unstructured annual report text data, offering a novel methodological reference for future studies. Previous research has often relied on questionnaires to measure cybersecurity governance, but these methods can suffer from limited sample size and potential selection bias due to design flaws. While some studies in the U.S. market have manually screened keywords (Florackis et al., 2023) and used a dictionary-based word frequency approach on 10-K annual reports and conference call transcripts, this method is not directly applicable to the Chinese A-share market[1]. The traditional dictionary-based approach also suffers from two

[1] The U.S. Securities and Exchange Commission (SEC), in its Management Regulation S-K Item 305 since 2011, requires companies to disclose information on the impact of cybersecurity risks on their operations, particularly significant risks and events, in the "Risk Factors" section of their financial reports. In contrast, Chinese regulatory agencies do not mandate companies to disclose cybersecurity risks and management status in their annual reports.

types of bias: keywords from prior empirical studies may not be present in the annual reports, and prior texts may not encompass all relevant expressions, potentially leading to omitted information and measurement bias. To overcome these limitations, we employ a deep learning approach to analyze Chinese listed company annual reports, which allows us to create a more comprehensive and accurate cybersecurity governance index and bypass the constraints of traditional manual screening.

The remainder of this paper is organized as follows. Section 2 presents the theoretical framework and research hypotheses. Section 3 describes the data, variable definitions, and empirical model design. Section 4 reports the baseline results and robustness tests. Section 5 provides further analyses, including mechanism and heterogeneity tests, as well as the consistency analysis between rhetoric and practice. Section 6 concludes the study and discusses its theoretical implications, practical recommendations, and directions for future research.

2. Theoretical analysis and research assumptions

In markets characterized by information asymmetry, the transmission and interpretation of signals influence the decisions and behaviors of market participants (Zhang & Lin, 2025). As cybersecurity threats grow, a firm's willingness to engage in cybersecurity governance, recognized as a prerequisite for managing cyber risks (Gatzert & Schubert, 2022), can be interpreted by stakeholders as a credible signal. This willingness reflects a firm's internal management capacity and risk control, which can reduce information gaps, strengthen reputational credibility within supply chains, and ultimately affect supplier decision-making (Tan et al., 2025).

First, cybersecurity governance willingness reduces supply chain information asymmetry, thereby affecting supplier credit decisions. Supplier credit decisions involve balancing expected returns with risks, while the challenges arising from information asymmetry, such as increased bad debt risk and costly screening, remain central concerns (X. Chen & Cheng, 2024). In China's capital market, where cybersecurity risk disclosure is not mandatory, suppliers rely on voluntarily disclosed reports, announcements, and media coverage to access governance-related information (Feldman et al., 2010). Firms that disclose their attention to cybersecurity risks and the measures they have implemented send a signal of active and structured governance (Gordon et al., 2010; Florackis et al., 2023). These signals provide insight into a firm's risk management capacity (Feldman et al., 2010), complement financial disclosures (Tan et al., 2025), and strengthen confidence in its repayment ability and long-term prospects. They also reduce suppliers' expected collection costs and credit risks, increasing their willingness to extend trade credit. In addition, suppliers' decisions are shaped by competitive pressures. According to buyer market theory, trade credit serves as a strategic tool to attract clients, boost sales, and sustain growth (X. Chen & Cheng, 2024). In settings with limited information and underdeveloped financial markets, suppliers are more inclined to support firms perceived as financially sound and well governed (C. Chen et al., 2019). Expressing cybersecurity governance willingness thus increases a firm's likelihood of securing supplier credit.

Second, governance willingness enhances a firm's reputation, further reinforcing supplier confidence. Reputation, a key intangible asset, promotes trust and collaboration with stakeholders (Maulidiyah & Harto, 2025). Within supply chains, reputation often diffuses across interconnected firms (Tan et al., 2025). Disclosing cybersecurity efforts builds reputational capital by signaling accountability and effective risk control, strengthening the firm's credibility in the network (Gatzert & Schubert, 2022). Reputation also provides resilience in the face of

unexpected events, enabling faster recovery and reducing partners' potential losses (Kamiya et al., 2021) In contrast, nondisclosure may be perceived as a sign of weak governance, raising doubts about risk management capabilities (Florackis et al., 2023). In digital supply chains, reputational damage spreads quickly. If firms are exposed for cybersecurity vulnerabilities and fail to demonstrate governance intent, their reputation may deteriorate, prompting suppliers to question business stability and reduce credit (Tan et al., 2025). Expressing cybersecurity commitment not only reinforces the perception of strong internal controls but also elevates reputation, improving access to trade credit support. The conceptual link between these variables is illustrated in Figure 1.

Accordingly, we propose the following hypothesis:

H1: *All else equal, firms exhibiting stronger cybersecurity governance willingness are more likely to obtain greater trade credit.*

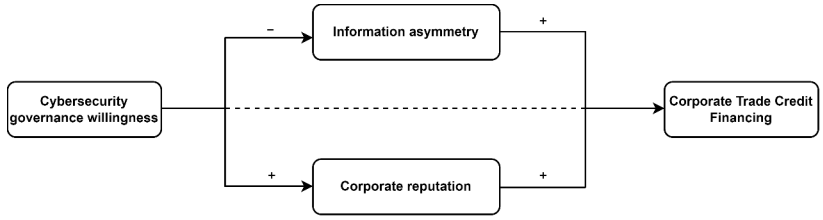

Figure 1. Theoretical framework

3. Research design

3.1. Data sources and sample selection

Our sample consists of Chinese A-share listed companies from 2011 to 2023. We exclude (1) financial firms, (2) firms under special treatment (ST and *ST)[2], and (3) firms with missing data for key variables. All continuous variables are winsorized at the 1% and 99% levels. Data were primarily sourced from the CSMAR and Wind databases, while annual report texts were obtained from the official websites of the Shanghai and Shenzhen Stock Exchanges.

3.2. Definition of variables

3.2.1. Corporate net trade credit

Following prior research (Fisman & Love, 2003; Tian & Tian, 2022), we measure supplier Trade Credit (TC) using the following equation:

$$\text{Trade Credit} = \frac{\text{Accounts Payable} + \text{Notes Payable} - \text{Advances to suppliers}}{\text{Total Assets}} \times 10. \quad (1)$$

A higher value for this measure indicates a greater level of net trade credit a firm receives from its suppliers, suggesting a stronger willingness from suppliers to extend credit and a greater level of trust in the firm.

[2] In the Chinese capital market, firms that have been specially flagged by the stock exchange due to continuous losses or financial irregularities are designated as ST firms. If their financial condition is more severe or they face a risk of delisting, they are flagged as *ST firms.

3.2.2. Cybersecurity governance commitment

The "Management Discussion and Analysis" (MD&A) section of a firm's annual report reflects its operational and strategic priorities. A frequent mention of cybersecurity governance in this section is therefore indicative of a strong corporate commitment to the issue (Florackis et al., 2023; Tan et al., 2025).

The specific construction process is as follows: First, we compiled a list of 31 seed words[3] by consulting relevant regulations, research reports, and academic literature (Lattanzio & Ma, 2023; Florackis et al., 2023). Second, using the MD&A texts of our sample firms and a 1.2-billion-word general corpus, we trained a Word2vec word vector model[4]. By identifying terms with high semantic similarity to our seed words, we generated an expanded list of more than 60 cybersecurity governance-related terms, including "access control" and "data breach prevention". Third, we used Python to match and count the frequency of these keywords within the MD&A texts. Finally, we weighted the keywords to correct for potential biases from high-frequency and common words (Loughran & Mcdonald, 2011). This process resulted in our cybersecurity governance commitment index, for which we then took the natural logarithm (lnCyber).

The keywords were weighted using the following method:

$$w_{i,j} = \begin{cases} \dfrac{1+\ln\left(tf_{i,j}\right)}{1+\ln\left(\alpha_j\right)} \ln\dfrac{N}{df_i}, & \text{if } tf_{i,j} \geq 1 \\ 0, & \text{if } tf_{i,j} = 0 \end{cases}, \tag{2}$$

where, $w_{i,j}$ is the weight of keyword i. $tf_{i,j}$ is the term frequency of keyword i in the MD&A section of annual report a_j is the length of the MD&A section in annual report j; N is the total number of corporate annual reports; and df_i is the number of annual reports that contain keyword i. In the Appendix, we provide comprehensive tests of the validity and robustness of this indicator.

3.2.3. Control variables

Consistent with prior literature (Kong et al., 2020; Lattanzio & Ma, 2023; Florackis et al., 2023), we include a set of control variables that may influence trade credit: Firm size (Size), Cash flow ratio (Cashflow), Return on equity (ROE), Debt-to-asset ratio (Lev), Growth (Growth), Firm age (Firmage), Percentage of shares held by the largest shareholder (Top1), Proportion of independent directors (Indep), Board size (Board), Audit opinion type (Opinion), Big Four auditor dummy (Big4), IT background of the board (IT), R&D intensity (RD), Executive compensation (TMTPay), CEO-duality (Dual), and Overseas experience of executives and directors (Mover). See the Appendix for specific variable definitions.

[3] Seed words and their expansions: cybersecurity, cyberattack, data security, data breach, system vulnerability, computer virus, malware, Trojan, worm, hacker attack, denial of service, intrusion, data backup, encryption technology, encrypted transmission, access control, authentication, security policy, security audit, security monitoring, system security, data tampering, data privacy, internal threat, cloud security, security vulnerability, backdoor, hijacking, downtime, disaster recovery, and internet security.

[4] The Word2vec method, proposed by Mikolov et al. (2013), is a deep learning model that processes text into high-dimensional vector representations. Cosine similarity in this vector space can then be used to measure the semantic similarity of the text.

3.3. Model design

To test our hypothesis, we estimate the following regression model:

$$TC_{i,t} = \alpha_0 + \alpha_1 \ln cyber_{i,t-1} + \alpha_i Control_{i,t-1} + Year + Firm + \varepsilon_{i,t}, \quad (3)$$

where $TC_{i,t}$ represents the firm's supplier trade credit in period t, and $lnCyber_{i,t-1}$ refers to the cybersecurity governance of firm i in the previous year ($t-1$). We cluster standard errors at the firm level.

4. Empirical results

4.1. Descriptive statistics

The mean of corporate Trade Credit (TC) is 1.155. Since the variable is scaled by total assets, this indicates that trade credit provided by suppliers averages approximately 11.55% of a firm's total assets. With a variance of 0.933, the data show substantial differences in the ability of firms to obtain trade credit. The mean of cybersecurity governance attention (lnCyber) is 0.244, with a standard deviation of 0.582. This suggests that firms, on average, have a relatively low level of attention to cybersecurity governance, and there is significant variation across firms.

4.2. Benchmark regression

Before presenting the regression results, we first report the correlation analysis among the variables. As shown in Figure 2, there is no evidence of multicollinearity. We then present the baseline regression results in Table 1. The coefficient of lnCyber is significantly positive in all models, with and without firm and time fixed effects, which indicates that a firm's attention to cybersecurity governance increases the supply of supplier trade credit. In terms of economic significance, as shown in column 2, a one-standard-deviation increase in a firm's cybersecurity governance attention is associated with a 12.4% increase in supplier trade credit from its mean (0.246 × 0.582 ÷ 1.155), which supports our Hypothesis H1.

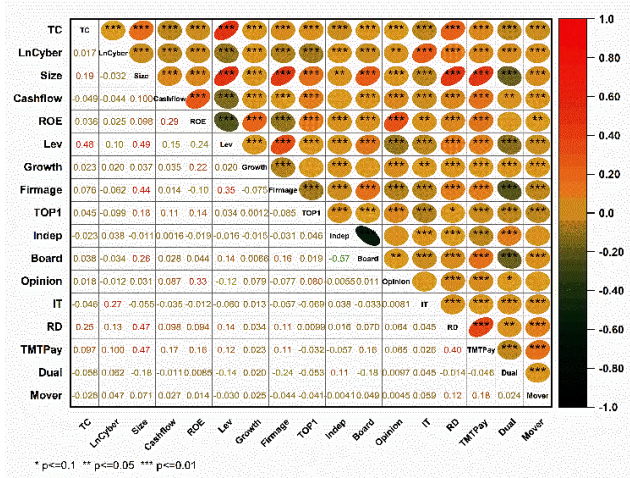

Figure 2. Correlation analysis

Table 1. Benchmark regression

Variable	(1)	(2)
	TC	TC
lnCyber	0.278***	0.246***
	(3.54)	(2.68)
Constant	10.679***	16.023***
	(8.15)	(3.70)
Obs	32837	32837
adj. R2	0.305	0.810
Controls	YES	YES
Firm	NO	YES
Year	NO	YES

Notes: The t-statistics are provided in parentheses below the coefficients. *, ** and *** represents significant at 10%, 5% and 1% level, respectively, the same as below.

4.3. Robustness tests

4.3.1. Instrumental variable

To address endogeneity concerns, we employ an Instrumental Variable (IV) approach. We instrument our variable using the establishment of specialized Intellectual Property (IP) courts and tribunals in China since 2014. One of the primary motivations for cyberattacks is the theft of intellectual property. The creation of these specialized courts has significantly enhanced the judicial protection of IP, reducing firms' potential losses from IP theft and, in turn, incentivizing them to strengthen their cybersecurity governance to protect their R&D outcomes. Critically, because these courts specialize in IP cases, their establishment is not directly related to a firm's routine financing activities, such as trade credit, which satisfies the exogeneity requirement for a valid instrument. Given the courts' more pronounced impact on R&D-intensive firms, we construct our IV as an interaction term between the IP court dummy and a dummy for a firm's R&D expenditure being above the sample median. Our IV passes the Kleibergen-Paap rk Wald F test for weak instruments, confirming the validity of the underlying identification. As shown in Table 2, the coefficient on lnCyber is 3.972 and significant at the 1% level, confirming our finding's robustness to endogeneity.

4.3.2. Heckman two-step regression

To address potential sample selection bias, which can arise from the multiple factors influencing a firm's willingness to adopt cybersecurity governance, we employed a Heckman two-step regression. In the first stage, a Probit regression modeled a dummy variable (dum_Cyber) based on the presence of cybersecurity keywords in annual reports. An IV was included to estimate the inverse Mills ratio (IMR). In the second stage, we incorporated the IMR into the original model as a control variable. The significantly positive IMR coefficient in Table 2 confirms the presence of sample selection bias. After controlling for this bias, the cybersecurity governance coefficient remained significant at the 1% level.

4.3.3. PSM+EBM

To address endogeneity arising from selection bias, we apply Propensity Score Matching (PSM) as a robustness check. Specifically, we define dum_Cyber as the treatment variable

and implement 1:1 nearest-neighbor matching with a 0.01 caliper. Since PSM may reduce the sample size, we further re-estimate the model on the re-weighted sample using entropy balancing (EBM). Table 2 shows that the results remain robust.

Table 2. Robustness tests I

Variable	IV		Heckman	PSM	EBM
	(1)	(2)	(4)	(5)	(6)
	lnCyber	TC	TC	TC	TC
IV	0.045***				
	(3.71)				
lnCyber		3.972***	0.219**	0.214***	0.225**
		(3.93)	(2.08)	(2.60)	(2.20)
IMR			0.568***		
			(6.77)		
Obs	30188	30188	30188	21143	32837
adj. R2	0.782		0.840	0.832	0.838
Controls	YES	YES	YES	YES	YES
Firm	YES	YES	YES	YES	YES
Year	YES	YES	YES	YES	YES

4.3.4. Double debiased machine learning

The baseline regression may suffer from specification errors, the curse of dimensionality in high-dimensional controls, and multicollinearity. To address these issues, we re-estimate the model using double debiased machine learning (Chernozhukov et al., 2018). We apply a random forest model with interaction terms, splitting the sample into training and test sets at ratios of 1:4 and 1:7, and include both linear and quadratic terms of the controls while controlling for year and individual fixed effects. Table 3 shows that all coefficients are positive and significant at the 1% level.

Table 3. Robustness Test II

Variable	Random Forest 1:4		Random Forest 1:7	
	(1)	(2)	(3)	(4)
	TC	TC	TC	TC
lnCyber	0.253***	0.271***	0.250***	0.259***
	(3.70)	(3.99)	(3.65)	(3.79)
First-order term	YES	YES	YES	YES
Second-order term	NO	YES	NO	YES
Obs	32837	32837	32837	32837
Firm	YES	YES	YES	YES
Year	YES	YES	YES	YES

Notes: z-statistics in parentheses; ***, **, and * denote significance at the 1%, 5%, and 10% levels.

4.3.5. Clustered robust standard errors

To enhance reliability, we re-estimate model (2) with industry-clustered standard errors. Table 4 shows that the coefficient of the core explanatory variable remains significantly positive, confirming the robustness and generalizability of the findings.

4.3.6. Adding fixed effects

To control for industry characteristics and their time variation, we include industry fixed effects and industry-year fixed effects. Table 4 shows that all coefficients remain positive and significant.

4.3.7. Adding control variables

Recent studies suggest that ESG ratings, CSR transparency, institutional cross-holdings, and bank loans also affect trade credit (Tian & Tian, 2022; Hendijani Zadeh et al., 2023; Liu & Hou, 2023). We therefore add them as additional controls. Table 4 indicates that the results remain robust.

Table 4. Robustness Test III

Variable	Industry	Adding fixed effects		Adding control variables
	(1)	(2)	(3)	(4)
	TC	TC	TC	TC
lnCyber	0.246***	0.245***	0.217***	0.274***
	(3.62)	(3.15)	(3.29)	(2.64)
Obs	32837	32837	32821	31462
adj. R2	0.810	0.812	0.814	0.810
Controls	YES	YES	YES	YES
Firm	YES	YES	YES	YES
Year	YES	YES	YES	YES
Industry	NO	YES	YES	NO
Industry×Year	NO	NO	YES	NO
Add Controls	NO	NO	NO	YES

4.3.8. Alternative variable specifications

We further assess robustness by altering both the dependent and key independent variables. Supplier trade credit is proxied by accounts payable to total assets (TC1) and by the sum of accounts payable and notes payable to total assets (TC2). Governance willingness is captured by the frequency of "cybersecurity governance willingness" keywords in annual reports (Cyber_ratio). Table 5 shows that the results remain robust.

5. Further analysis

5.1. Mechanism test

Consistent with information signaling theory, a firm's willingness to adopt cybersecurity governance can influence suppliers' credit decisions through two channels: mitigating

Table 5. Robustness test IV

Variable	Dependent variable		Independent variable
	(1)	(2)	(3)
	TC1	TC2	TC
lnCyber	0.219***	0.252***	
	(2.96)	(2.78)	
Cyber_ratio			3.125***
			(2.61)
Obs	32837	32837	32837
adj. R2	0.814	0.813	0.810
Controls	YES	YES	YES
Firm	YES	YES	YES
Year	YES	YES	YES

supply chain information asymmetry and enhancing corporate reputation. To identify this mechanism, we follow the two-stage approach of Di Giuli and Laux (2022). This method offers three key advantages over traditional mediation analysis (e.g., Baron and Kenny, 1986). First, it mitigates endogeneity bias in the mechanism variables. For instance, a firm's reputation can be influenced by its financing relationships, creating reverse causality with trade credit access. Using a predicted value for the mechanism variable can partially address this endogeneity. Second, the two-stage approach reduces multicollinearity and specification bias when the core independent and mechanism variables are included in the same regression, making channel effect identification more effective. Third, it isolates the "net effect" of governance willingness, providing more robust empirical evidence for the effectiveness of the signaling channels. It is important to note that this method relies on the exclusion restriction assumption, which posits that cybersecurity governance willingness primarily affects trade credit via the mechanism variables. However, as willingness to govern could also directly signal to suppliers, we interpret our results as supportive evidence consistent with the theoretical mechanism rather than a strict causal decomposition of the mediation effect.

Based on these considerations, we specified the following two-stage regression models:

$$\hat{\mathcal{M}}_{i,t} = \alpha_0 + \alpha_1 \ln cyber_{i,t-1} + \alpha_i Control_{i,t-1} + Year + Firm + \varepsilon_{i,t}; \quad (4)$$

$$TC_{i,t} = \alpha_0 + \alpha_1 \hat{\mathcal{M}}_{i,t} + \alpha_i Control_{i,t-1} + Year + Firm + \varepsilon_{i,t}, \quad (5)$$

where, the mechanism variables ($\hat{\mathcal{M}}_{i,t}$) include two components: information asymmetry (AbsDA), measured by the absolute value of the modified Jones model residuals (a larger value indicates lower transparency); and corporate reputation (REP), a comprehensive score derived from a factor analysis of 12 indicators[5] and assigned a value from 1 to 10 on a ten-level scale.

[5] The corporate reputation indicators cover four dimensions: consumers and society, creditors, shareholders, and the firm itself. These include industry rankings for assets, revenue, net profit, and value, as well as the debt-to-asset ratio, current ratio, long-term debt ratio, earnings per share, dividends per share, auditing firm, sustainable growth rate, and the proportion of independent directors.

Table 6 presents the empirical results. In columns (1)–(2), the negative coefficient on lnCyber indicates that a firm's willingness to govern improves trade credit access by mitigating information asymmetry. In columns (3)–(4), the significantly positive coefficient on lnCyber shows that this willingness also enhances corporate reputation, increasing supplier trust and leading to more trade credit. Overall, our mechanism tests support the "dual-channel" hypothesis under the information signaling theory.

Table 6. Mechanism test

Variable	(1)	(2)	(3)	(4)
	AbsDA	TC	REP	TC
lnCyber	–0.004***		0.070**	
	(–5.22)		(2.12)	
$\hat{M}1$		–5.663***		
		(–2.64)		
$\hat{M}2$				3.463***
				(2.62)
Obs	31507	31507	32754	32754
adj. R2	0.691	0.813	0.728	0.809
Controls	YES	YES	YES	YES
Firm	YES	YES	YES	YES
Year	YES	YES	YES	YES

5.2. Heterogeneity analysis

5.2.1. Stock exchange inquiries

As primary regulators of listed firms, stock exchanges issue inquiry letters on corporate disclosures, shaping the information environment. Stakeholders often perceive such inquiries as "bad news", triggering adverse market reactions, intensifying information asymmetry, and weakening market trust. In this setting, firms that actively signal commitment to cybersecurity governance are more likely to provide supplementary information, foster positive expectations, and reduce uncertainty arising from regulatory inquiries (Tan et al., 2025). Using the CNRDS database, we identify whether sample firms received inquiry letters from the Shanghai or Shenzhen Stock Exchange and conduct sub-sample analyses. As shown in Figure 3, for firms receiving inquiries, the estimated coefficient of lnCyber is larger, and statistical tests confirm a significant difference between the two groups.

5.2.2. Political ties

From the perspective of institutional embeddedness, political ties in China reflect distinctive relational and interest linkages between government and enterprises, often functioning as "institutional insurance" (J. Chen et al., 2024). Politically connected firms tend to rely on implicit government guarantees or policy preferences to obtain trade credit, rather than primarily on their cybersecurity governance. By contrast, firms without political ties lack such endorsement, so their proactive commitment to cybersecurity governance is more salient to suppliers as a differentiated advantage, thereby exerting a stronger marginal effect on trade credit supply. Accordingly, we classify firms based on whether the chairman or general

manager currently or previously held government office and run subgroup regressions. As shown in Figure 3, cybersecurity governance willingness more significantly enhances trade credit for firms without political ties.

5.2.3. Economic policy uncertainty

Transaction cost theory identifies uncertainty as a core determinant of trading stability. When policy uncertainty is high, suppliers worry more about firms' future stability and adopt a cautious approach to trade credit. In this context, firms that signal commitment to cybersecurity governance are better able to reduce information asymmetry and market concerns, thereby enhancing credit access. By contrast, when policy uncertainty is low, systemic uncertainty is weaker and the signaling effect diminishes. We split the sample at the median of the economic policy uncertainty index and run regressions. Figure 3 shows that cybersecurity governance willingness more strongly promotes trade credit under high policy uncertainty.

5.2.4. Social trust

Economic activity is embedded in social networks, where trust can substitute for formal contracts and external oversight, sustaining credit-based transactions. In high-trust regions, cooperation relies on reputation and long-term relationships, so suppliers place less weight on governance signals, weakening the marginal effect of cybersecurity governance willingness. In low-trust regions, weaker institutional and reputational constraints raise the risk of opportunism, leading suppliers to rely more on disclosed cybersecurity commitment when assessing reliability. In this context, governance willingness becomes a salient signal that more strongly promotes trade credit. To capture the trust environment, we use China's social credit system pilot program, coding regions as 1 if included in that year or later and 0 otherwise, and conduct subgroup regressions. Figure 3 shows that cybersecurity governance willingness more strongly promotes trade credit in low-trust regions.

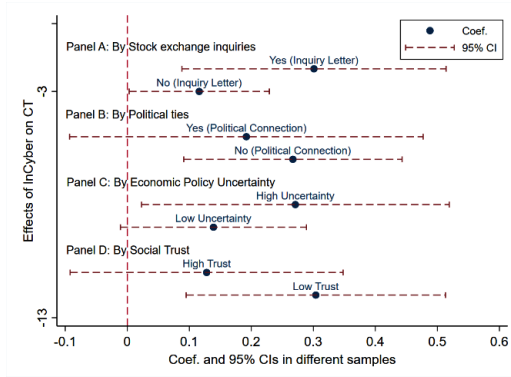

Figure 3. Heterogeneity test

5.3. Rhetoric-practice consistency and suppliers' business adjustments

The preceding analysis examined how firms' cybersecurity governance willingness influences suppliers' trade credit. Yet willingness and practice may diverge, raising the question of whether firms that signal but do not invest can secure the same supplier trust and support as those showing rhetoric-practice consistency.

To test this, we adopt IT investment as a proxy for governance practice, since implementation requires resources in hardware, software, and information management. IT investment is divided into hardware and software[6] and grouped into high, medium, and low based on industry-year averages. Using the same method, we classify the word-frequency measure of governance willingness. Combining the two dimensions yields a four-quadrant matrix (Figure 4), distinguishing "more rhetoric-more practice", "less rhetoric-more practice", "more rhetoric-less practice", and "less rhetoric-less practice". To capture supplier responses to alignment, we focus on the first and fourth quadrants, defining rhetoric-practice consistency (Iac_1) and rhetoric-practice gap (Iac_0). We then analyze procurement from the top five suppliers disclosed by listed firms.

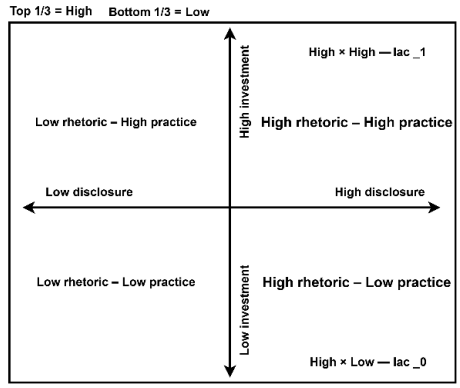

Figure 4. Quadrant matrix

Figure 5 shows that rhetoric–practice consistency (Iac_1) significantly raises supplier procurement in both the current and $t+1$ periods, with the effect strengthening over time, while rhetoric–practice gap (Iac_0) yields only a modest contemporaneous effect and none in $t+1$. These findings indicate that consistency in cybersecurity governance not only consolidates short-term relationships but also builds long-term trust, shaping suppliers' business adjustments.

6. Conclusions

We develop a Word2vec-based indicator of cybersecurity governance willingness in China and, drawing on signaling theory, examine its impact on trade credit from suppliers. Results show that expressing such willingness increases suppliers' trade credit, with information asymmetry and corporate reputation as mechanisms. Heterogeneity tests indicate stronger effects for firms receiving inquiry letters, lacking political ties, facing higher policy uncertainty, or operating in low-trust regions. Moreover, when rhetoric and practice are consistent, suppliers adjust by allocating more procurement, thereby reinforcing supply chain trust.

This study has important theoretical and practical implications. First, from the supplier-credit perspective, it fills a gap in research that focuses on cyberattacks while neglecting

[6] IT hardware investment is measured by the year-end balances of electronic equipment and computers reported under fixed assets, while IT software investment is measured by the year-end balances of software, systems, and information-related categories reported under intangible assets.

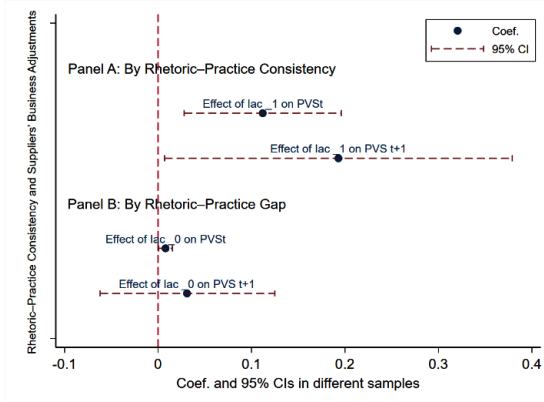

Figure 5. Economic Consequence Analysis

governance willingness as an "informal signal". We show that expressing willingness enhances trade credit and, when aligned with actual investment, builds long-term trust. This resonates with findings on disclosure and supply chain trust and adds evidence on dynamic supply chain adjustments. Second, we extend the determinants of trade credit to include firms' willingness expression, offering empirical support for signaling theory in supply chain finance. Third, by combining Word2vec with text mining, we construct a governance willingness indicator suited to the Chinese market, providing methodological insights for future unstructured text research.

Our study has several limitations. First, while we used IT investment as a proxy for firms' cybersecurity governance practices, this metric may not fully capture their actual actions. As our study only quantified the willingness to govern, it would be beneficial for future research to introduce more detailed indicators of governance practices to more accurately capture firm behavior. Second, due to data constraints, our study focuses on Chinese listed companies. Given that non-listed companies also face cybersecurity challenges, future research could expand data sources to include firms of different sizes and industries, thereby building a more comprehensive body of research.

Based on our findings, we propose the following policy recommendations to optimize corporate cybersecurity governance practices and improve the credit environment.

For enterprises, we recommend that they strengthen their cybersecurity governance awareness as they undergo digital transformation. They can do this by clearly articulating cybersecurity plans and enhancing the transparency of information disclosure to signal their commitment to external stakeholders and reduce information asymmetry risks. In particular, firms facing regulatory scrutiny, high economic policy uncertainty, or low social trust should prioritize the strategic importance of cybersecurity governance. They should regularly disclose their governance measures to help stakeholders better understand their situation, thus enhancing overall corporate resilience and trust.

For policymakers, we recommend a continuous effort to improve the standards and regulatory frameworks for cybersecurity governance. This includes promoting the establishment of a disclosure system for firms' governance intentions. Through industry guidance, talent training, and incentive mechanisms, policymakers should enhance the understanding of the strategic value of cybersecurity among corporate management and promote greater

attention and action across society. In addition, it is essential to accelerate the development of multi-level corporate credit service platforms to facilitate the signaling and transmission of cybersecurity information within the supply chain, thereby improving the overall financing efficiency and risk control capabilities of the real economy.

Funding

Horizontal Research Project of Heilongjiang Bayi Agricultural University (Project Number: 2024035).

Acknowledgements

We would like to express our sincere gratitude to Dr. Martinkutė-Kaulienė, the Managing Editor of the Journal of Business Economics and Management, as well as the anonymous reviewers, for their valuable feedback and suggestions, which significantly improved the quality of this manuscript.

Author contributions

Han Yan and Ding Li contributed equally to this work as co-first authors. Han Yan and Ding Li collaboratively developed the theoretical framework, conducted the Word2vec text analysis, and were responsible for the data interpretation and analysis. Han Yan wrote the initial draft of the manuscript and led the refinement of the research design and methodology. Ding Li played a key role in data collection, processing, and performing the Word2vec text analysis, and also contributed significantly to the revision and finalization of the manuscript. Shenglin Ma provided valuable feedback on the manuscript and contributed to the overall study design and interpretation of results.

Disclosure statement

The authors declare that they have no competing interests.

AI Acknowledgement

The authors acknowledge the use of Claude Sonnet 4.5 (Anthropic, 2025) to refine the language and improve the clarity of this manuscript. The AI tool was used solely for proofreading and language editing purposes using the prompt: "Please proofread and edit the following text to improve clarity and academic tone". All intellectual content, research design, analysis, and conclusions are entirely the work of the authors.

References

Alfaro, L., García-Santana, M., & Moral-Benito, E. (2021). On the direct and indirect real effects of credit supply shocks. *Journal of Financial Economics*, *139*(3), 895–921. https://doi.org/10.1016/j.jfineco.2020.09.004

Ball, R., Jayaraman, S., & Shivakumar, L. (2012). Audited financial reporting and voluntary disclosure as complements: A test of the confirmation hypothesis. *Journal of Accounting & Economics*, *53*(1–2), 136–166. https://doi.org/10.1016/j.jacceco.2011.11.005

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173–1182. https://doi.org/10.1037/0022-3514.51.6.1173

Benmelech, E., Meisenzahl, R. R., & Ramcharan, R. (2017). The real effects of liquidity during the financial crisis: Evidence from automobiles. *Quarterly Journal of Economics*, *132*(1), 317–365. https://doi.org/10.1093/qje/qjw031

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

Bharath, S. T., & Shumway, T. (2008). Forecasting default with the Merton distance to default model. *The Review of Financial Studies*, *21*(3), 1339–1369. https://doi.org/10.1093/rfs/hhn044

Blind, K., Niebel, C., & Rammer, C. (2024). The impact of the EU General data protection regulation on product innovation. *Industry and Innovation*, *31*(3), 311–351. https://doi.org/10.1080/13662716.2023.2271858

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

China Academy of Information and Communications Technology. (2023). *Research Report on China's Digital Economy* (*2023*). https://www.caict.ac.cn/kxyj/qwfb/bps/202304/t20230427_419051.htm

Chen, C., Kim, J., Wei, M., & Zhang, H. (2019). Linguistic information quality in customers' forward-looking disclosures and suppliers' investment decisions. *Contemporary Accounting Research*, *36*(3), 1751–1783. https://doi.org/10.1111/1911-3846.12471

Chen, J., Zhu, D., Ding, S., & Qu, J. (2024). Government environmental concerns and corporate green innovation: Evidence from heavy-polluting enterprises in China. *Business Strategy and the Environment*, *33*(3), 1920–1936. https://doi.org/10.1002/bse.3583

Chen, J., Guo, X., Geng, Y., & Liu, R. (2025). Climate risk and trade credit financing: Evidence from China. *International Journal of Finance & Economics*, *30*(3), 2514–2535. https://doi.org/10.1002/ijfe.3027

Chen, X., & Cheng, X. (2024). How does the digital economy affect corporate business credit supply? *Journal of Business Economics and Management*, *25*(4), 685–708. https://doi.org/10.3846/jbem.2024.22027

Chernozhukov, V., Chetverikov, D., Demirer, M., Duflo, E., Hansen, C., Newey, W., & Robins, J. (2018). Double/debiased machine learning for treatment and structural parameters. *The Econometrics Journal*, *21*(1), C1–C68. https://doi.org/10.1111/ectj.12097

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432–448. https://doi.org/10.1016/j.jfineco.2022.12.002

Deloitte. (2021). *Technology, media, and telecommunications predictions 2021*. https://branden.biz/wp-content/uploads/2020/12/PL_2021-TMT-predictions.pdf

Di Giuli, A., & Laux, P. A. (2022). The effect of media-linked directors on financing and external governance. *Journal of Financial Economics*, *145*(2), 103–131. https://doi.org/10.1016/j.jfineco.2021.07.017

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3), 802–826. https://doi.org/10.1016/j.jfineco.2021.10.007

Feldman, R., Govindaraj, S., Livnat, J., & Segal, B. (2010). Management's tone change, post earnings announcement drift and accruals. *Review of Accounting Studies*, *15*, 915–953. https://doi.org/10.1007/s11142-009-9111-x

Fisman, R., & Love, I. (2003). Trade credit, financial intermediary development, and industry growth. *Journal of Finance*, *58*(1), 353–374. https://doi.org/10.1111/1540-6261.00527

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, *49*(2), 503–519. https://doi.org/10.1111/fima.12274

Gatzert, N., & 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*, *89*(3), 725–763. https://doi.org/10.1111/jori.12381

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

Hendijani Zadeh, M., Naaman, K., & Sahyoun, N. (2023). Corporate social responsibility transparency and trade credit financing. *International Journal of Accounting & Information Management*, *31*(2), 247–269. https://doi.org/10.1108/IJAIM-05-2022-0099

IBM. (2024). *Cost of a data breach report 2024*. https://www.ibm.com/reports/data-breach

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85–105. https://doi.org/10.1509/jm.16.0124

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kim, J.-B., & Zhang, L. (2014). Financial reporting opacity and expected crash risk: Evidence from implied volatility smirks. *Contemporary Accounting Research*, *31*(3), 851–875. https://doi.org/10.1111/1911-3846.12048

Kong, D., Pan, Y., Tian, G. G., & Zhang, P. (2020). CEOs' hometown connections and access to trade credit: Evidence from China. *Journal of Corporate Finance*, *62*, 101574. https://doi.org/10.1016/j.jcorpfin.2020.101574

Lattanzio, G., & Ma, Y. (2023). Cybersecurity risk and corporate innovation. *Journal of Corporate Finance*, *82*, Article 102445. https://doi.org/10.1016/j.jcorpfin.2023.102445

Loughran, T., & Mcdonald, B. (2011). When is a liability not a liability? Textual analysis, dictionaries, and 10-Ks. *The Journal of Finance*, *66*(1), 35–65. https://doi.org/10.1111/j.1540-6261.2010.01625.x

Liu, H., & Hou, C. (2023). Institutional cross-ownership and trade credit: Evidence from China. *Corporate Governance*: *An International Review*, *31*(6), 845–868. https://doi.org/10.1111/corg.12505

Maulidiyah, D. N., & Harto, P. (2025). The role of social control in deterring corporate financial statement fraud. *Discover Global Society*, *3*, Article 20. https://doi.org/10.1007/s44282-025-00155-y

Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2013). *Efficient estimation of word representations in vector space*. Arxiv. https://doi.org/10.48550/arXiv.1301.3781

Miller, K. D., & Leiblein, M. J. (1996). Corporate risk-return relations: Returns variability versus downside risk. *Academy of Management Journal*, *39*(1), 91–122. https://doi.org/10.5465/256632

Morgan, S. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Peón, D., & Guntín, X. (2021). Bank credit and trade credit after the financial crisis: Evidence from rural Galicia. *Journal of Business Economics and Management*, *22*(3), 616–635. https://doi.org/10.3846/jbem.2021.14270

Shahzad, U., Liu, J., & Luo, F. (2022). Stock liquidity and corporate trade credit strategies: Evidence from China. *Journal of Business Economics and Management*, *23*(1), 40–59. https://doi.org/10.3846/jbem.2021.15655

Silva Atencio, G. (2025). Effective cybersecurity strategies for mitigating remote work and IoT risks in enterprises. *FinTech and Sustainable Innovation*, *1*, Article A13. https://doi.org/10.47852/bonviewFSI52025962

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2013). Information security professionals' perceptions about the relationship between the information security and internal audit functions. *Journal of Information Systems*, *27*(2), 65–86. https://doi.org/10.2308/isys-50510

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

Tian, H., & Tian, G. (2022). Corporate sustainability and trade credit financing: Evidence from environmental, social, and governance ratings. *Corporate Social Responsibility and Environmental Management*, *29*(5), 1896–1908. https://doi.org/10.1002/csr.2335

Wang, J., Ho, C. Y. C., & Shan, Y. G. (2024). Does cybersecurity risk stifle corporate innovation activities? *International Review of Financial Analysis*, *91*, Article 103028. https://doi.org/10.1016/j.irfa.2023.103028

Wu, K., Fu, Y., & Kong, D. (2022). Does the digital transformation of enterprises affect stock price crash risk?. *Finance Research Letters*, *48*, Article 102888. https://doi.org/10.1016/j.frl.2022.102888

Yan, H., Li, Y., Zhong, Y., & Xia, Z. (2024). Will the 'government-court coordination' of corporate bankruptcy disposal improve ESG performance? Evidence from China. *Applied Economics Letters*, *32*(20), 2998–3002. https://doi.org/10.1080/13504851.2024.2358189

Yan, H., Yao, X., Li, Y., & Xiong, Z. (2025). Capital market liberalization and corporate ESG rating divergence: A quasi-natural experiment based on the trading system of SSHC. *Applied Economics*, *57*(60), 11107–11121. https://doi.org/10.1080/00036846.2025.2449849

Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *Business Economics and Management*, *22*(2), 369–387. https://doi.org/10.3846/jbem.2021.13925

Zhang, Q., & Lin, Z. (2025). Development of corporate governance practices and capital market reforms in China. *Journal of Comprehensive Business Administration Research*, *2*(3), 205–216. https://doi.org/10.47852/bonviewJCBAR52024189

Zhou, T., Li, Z., Bai, H., Du, Z., Huang, J., & Ding, Z. (2024). Does unconventional monetary policy improve credit support for the industry chain? The mechanism of trade credit. *International Review of Economics & Finance*, *91*, 180–192. https://doi.org/10.1016/j.iref.2023.12.009

Zhu, W., Li, W.-J., & Wang, L. (2024). The impact of environmental, social, and governance ratings on corporate innovation: From the perspective of informal institutions. *Managerial and Decision Economics*, *45*(4), 2000–2022. https://doi.org/10.1002/mde.4110

APPENDIX

A. Variable definitions

Table A1. Variable definition

Variable	Definition
TC	See Eq. (1)
lnCyber	Natural logarithm of word frequency plus one
Size	Natural logarithm of total assets
Cashflow	Ratio of net cash flow from operating activities to total assets
ROE	Return on equity
Lev	Ratio of total liabilities to total assets
Growth	Current year's operating revenue divided by last year's operating revenue minus one
Firmage	Natural logarithm of listing age plus one
TOP1	Shareholding ratio of the largest shareholder
Indep	Ratio of independent directors to board size
Board	Natural logarithm of board size
Opinion	Equals 1 if the firm's annual financial report receives a standard unqualified audit opinion, and 0 otherwise

Variable	Definition
IT	Equals 1 if the CEO has an information technology background, and 0 otherwise
RD	Natural logarithm of R&D expenditure plus one
TMTPay	Natural logarithm of total compensation of the top three executives
Dual	Equals 1 if the chairman and CEO are the same person, and 0 otherwise
Mover	Equals 1 if any directors, supervisors, or executives have overseas experience, and 0 otherwise

B. Validity and robustness tests of the indicator

To validate the cybersecurity governance willingness indicator constructed via text analysis, we conduct assessments from two perspectives: conceptual relevance and dynamic trends.

First, cybersecurity risk refers to attacks driven by economic or political motives that disrupt IT systems, leading to financial loss and operational failure (Florackis et al., 2023). Such threats heighten uncertainty and increase the likelihood of performance decline and default. Cybersecurity governance addresses these risks by mitigating IT failures caused by attacks. Based on this, we adopt downside risk (DownsideRisk), as defined by Miller and Leiblein (1996), and distance to default (DDBhsh), per Bharath and Shumway (2008), as proxies. A higher DownsideRisk reflects greater exposure to loss, while a higher DDBhsh indicates reduced default risk. Table A2 shows that cybersecurity governance willingness significantly lowers downside risk and increases distance to default, highlighting the indicator's explanatory power for firm-level risk.

Table A2. Cybersecurity governance and business risks, default risks

Variables	(1)	(2)	(3)	(4)	(5)	(6)
	DownsideRiskt	DownsideRiskt+1	DownsideRisk t+2	DDBhsh t	DDBhsh t+1	DDBhsh t+2
lnCyber	–0.004***	–0.003***	–0.002***	0.342***	0.346***	0.331***
	(–3.59)	(–3.72)	(–3.57)	(2.93)	(3.91)	(5.32)
Constant	0.124***	0.092***	0.094***	51.028***	46.711***	45.726***
	(3.71)	(3.53)	(4.17)	(15.47)	(13.19)	(12.31)
Obs	22737	20514	19227	29469	26614	25026
aadj. R2	0.432	0.426	0.524	0.532	0.534	0.534
Controls	YES	YES	YES	YES	YES	YES
Firm	YES	YES	YES	YES	YES	YES
Year	YES	YES	YES	YES	YES	YES

Second, we test dynamic validity by aggregating the indicator annually and comparing its trend with corporate digitalization levels (Figure A1). Following Wu et al. (2022), we measure digitalization via keyword frequency in annual reports. Since 2010, both digitalization and cybersecurity governance willingness have shown an upward trend, consistent with expectations: widespread adoption of AI, big data, and cloud computing has intensified cyber threats, elevating governance to a strategic concern.

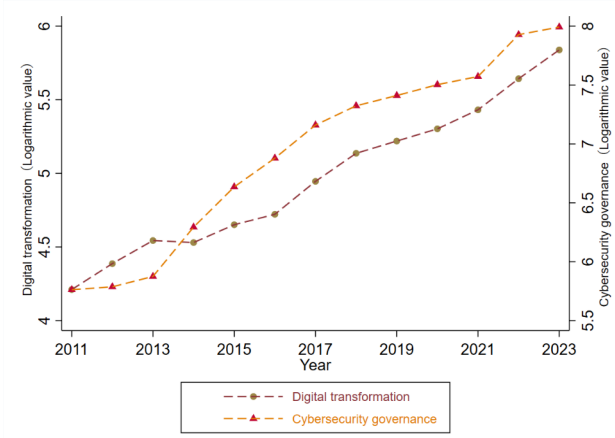

Figure A1. Annual change trends of enterprise cybersecurity governance and digital level

Unlike the stable rise in digitalization, cybersecurity governance willingness fluctuates in some years. In 2015, China's draft Cybersecurity Law – its first comprehensive legislation – was released, prompting a marked increase in firm-level attention. Similarly, following the 2021 enactment of the Data Security Law and the Regulation on Critical Information Infrastructure Protection, the indicator rose again in 2022. These shifts suggest firms respond sensitively to regulatory signals, confirming the indicator's semantic and practical validity.

Overall, the evidence supports the conceptual soundness and empirical robustness of the constructed indicator.