Journal of Business, Behavior & Sustainability
JBBS

Vol. 1 | No. 1 | 2026
pp. 28-41

ORIGINAL RESEARCH

Supply Chain Cyber Shocks and the Bank Loan Renewal Channel: Evidence from Firm-Level Exposure and Lending Contracts

Muhammad Ishfaq[1,*] and Wajid Hussain[2]

[1] *Department of Management Sciences, COMSATS University Islamabad, Vehari Campus. Email: muhammadashfaq@cuivehari.edu.pk*
[2] *PhD Scholar, Department of Commerce, Bahauddin Zakariya University, Multan, Punjab, Pakistan. Email: hussainwajid29@yahoo.com*

ARTICLE HISTORY

Received
18 June 2026
Latest revision
22 September 2026
Accepted
8 October 2026
Published online
15 October 2026

KEYWORDS
Supply-Chain Cyber Risk
Bank Loan Contracting
Loan Spreads and Covenants
Information Asymmetry
China

ABSTRACT

In increasingly digitized supply networks, lenders face uncertainty not only from a borrower's own systems but also from cyber incidents at connected suppliers and customers. This study examines whether such supply-chain cyber shocks are priced into bank loan renewals for Chinese listed firms. Using firm-year data and two-way fixed-effects regressions complemented by staggered difference-in-differences tests, we estimate the impact of exposure to partners' breaches on loan spreads, covenant intensity, and maturities, and assess whether cyber risk management quality and disclosure transparency moderate these effects. Results show that higher exposure is associated with higher spreads, tighter covenants, and shorter maturities; DiD evidence supports a causal interpretation. Moderation tests indicate that stronger cyber governance and more transparent disclosure attenuate these adverse adjustments, consistent with information-asymmetry and network-contagion mechanisms. We conclude that lenders rationally internalize networked cyber risk and that credible governance and disclosure are finance-relevant mitigants. We recommend incorporating exposure metrics and information-contingent covenants into underwriting and institutionalizing cyber governance and decision-useful disclosure on the borrower side.

1. Introduction

Cybersecurity breaches have emerged as one of the most critical operational risks in today's financial and corporate landscape (George et al., 2024). Firms now operate in highly interconnected supply chains where digital integration exposes them to indirect vulnerabilities (Hammi et al., 2023). A breach occurring at a key supplier or customer can disrupt operations, compromise data integrity, and undermine investor and lender confidence, even if the focal firm itself remains technically secure (Rangapur et al., 2023). While the financial markets have begun to price direct cyber incidents, the spillovers of cyber shocks across supply networks remains insufficiently understood especially in how such events influence firms' access to credit (Eisenbach et al., 2022).

Existing research shows that firms directly affected by cyber breaches face higher financing costs, weaker credit ratings, and tighter loan covenants (e.g., Jorion & Zhang, 2009; Wojewodzki et al., 2018). These studies establish that lenders treat breaches as indicators of poor governance or increased cash-flow volatility (Njuguna, 2022). However, the literature is largely silent on whether indirect exposure to cyber risk through breached suppliers or customers also affects bank lending terms (Uddin et al., 2020). This omission is important because operational and reputational risks increasingly propagate through supply chains (Dhingra & Krishnan, 2021). When a major trading partner suffers a cyber incident, banks may reassess the borrower's risk profile and alter the pricing or structure of its credit facilities (Adelmann et al., 2020).

This study addresses that gap by examining how supply-chain cyber shocks influence firms' loan renewal terms, including loan spreads, covenant intensity, maturity, and collateral requirements (Huynh, 2024). The central argument is that breaches within a firm's supply network act as negative information shocks, increasing uncertainty for lenders who may interpret such incidents as signals of latent operational fragility (Agca et al., 2022). These effects are expected to be strongest during loan renewal periods when banks re-evaluate borrower risk (Aye, 2023). The study further proposes that internal cyber risk management quality and information

*** Corresponding author**
Muhammad Ishfaq, Department of Management Sciences, COMSATS University Islamabad, Vehari Campus.
Email: muhammadashfaq@cuivehari.edu.pk

disclosure transparency moderate this relationship by signalling resilience and reducing information asymmetry (Zheng et al., 2024).

Grounded in information asymmetry and network contagion theories, the study conceptualises cyber shocks as information events that reshape perceptions of borrower reliability and propagate through interconnected supply networks (Ibrahim, 2020). Using data from public cyber incident databases, supply-chain linkages from FactSet and Compustat, and loan-level data from Refinitiv LPC, the analysis applies a difference-in-differences approach to compare firms with varying levels of exposure to breached partners (Do et al., 2025). This approach isolates the causal effect of indirect cyber shocks on lending terms while controlling for firm, lender, and time-specific factors (Hassan et al., 2024).

The expected contribution is threefold. First, it extends the corporate finance literature by identifying supply-chain cyber exposure as a novel determinant of bank lending conditions (Xu et al., 2025). Second, it integrates the concepts of operational risk contagion and financial contracting, showing how digital vulnerabilities shape debt markets (Siraj et al., 2024). Third, it highlights the role of governance and disclosure in mitigating the financial consequences of cyber risks. Collectively, these insights deepen understanding of how interconnected cyber threats influence the cost of credit and the stability of financial relationships (Dupont, 2019).

2. Literature Review- Theoretical Development

This study is grounded on the key principles of Information Asymmetry Theory (Akerlof, 1970; Stiglitz and Weiss, 1981) and Network Contagion Theory (Allen and Gale, 2000; Acemoglu et al., 2015), which combined can explain the impact of cyber shocks that originate in the supply chain of a certain firm on the credit risk perception of the lenders and, consequently, on the terms of a bank loan agreement (Al Khatib, 202 The main basis of the research is the information asymmetry theory (Akerlof, 1970; Stiglitz and Weiss, 1981) (Stiglitz, 2017). It assumes that the unequal access to information between the lenders and the borrowers influences the financial contracts (Padi, 2021). Lack of full knowledge of the actual risk profile of a borrower by the lenders will lead to the lenders raising interest rates, tightening covenants, or reducing the loan maturity to cushion themselves against the default risk (Tung, 2020). Within supply-chain cyber shock, when a firm is hacked by its supplier or customer, this asymmetry is increased by the ambiguity surrounding the existence of any operational shocks and future cash flows (Pandey et al., 2020). The lenders, who cannot adequately determine the scope of the indirect exposure of the borrower, see more credit risk and change the terms of lending (Sagi, 2017). Therefore, the information asymmetry theory provides a mechanism by which cyber shocks raise the cost and limit of loans, and also justifies the reason why better disclosure and governance can address impacts (Asongu et al., 2019).

Network contagion theory explains how disruptions in one node of an interconnected system can spread through linkages and affect other entities within the same network (Allen & Gale, 2000; Acemoglu et al., 2015). In modern supply chains, firms are digitally and operationally interdependent, making them susceptible to the transmission of cyber-related risks (Creazza et al., 2022). A cyber breach at a supplier or customer can quickly propagate through shared systems, data exchanges, and logistical dependencies, even if the focal firm itself is not directly attacked (Jeong et al., 2025). Lenders, aware of these interconnections, treat such supply-chain breaches as warning signals of elevated systemic vulnerability (Ogundele, 2024). Consequently, they modify credit terms to reflect the possibility of contagion-driven instability (Macchiati et al., 2022). Network contagion theory therefore provides the structural explanation for why cyber incidents in one firm can influence the financing conditions of another connected firm, highlighting the systemic nature of digital and operational risk in financial contracting (Hurd, 2016).

2.1 Supply Chain Cyber Shock Exposure and Loan Spread

When a cyber breach occurs in a firm's supply network whether at a supplier or customer it introduces new uncertainty into the firm's operational and financial environment (He et al., 2023). Lenders interpret such shocks as signals of elevated credit risk because disruptions in supply chains can impair production continuity, data integrity, or revenue stability (Karimirad, 2024). These conditions directly affect a borrower's cash flow predictability, which is central to loan pricing decisions (Brown et al., 2021). According to information asymmetry theory, when uncertainty about a borrower's quality or risk exposure increases, lenders demand higher returns to compensate for the additional perceived risk (Muli, 2017).

A supply-chain breach effectively widens the information gap between borrower and lender, as banks have limited ability to verify the full extent of the exposure or the firm's resilience (Xie et al., 2025). Consequently, they increase loan spreads to hedge against potential losses and higher monitoring costs (Hoepner et al., 2016). Prior research has shown similar responses to firm-level breaches and governance weaknesses, where heightened information asymmetry led to higher interest rate premiums (Wojewodzki et al., 2018; Sheneman, 2017). Extending this logic, supply-chain cyber shocks are expected to elicit comparable risk pricing behaviour, even when the borrowing firm itself remains unbreached (Wan, 2019).

H1: Supply-chain cyber shock exposure is positively associated with loan spreads at renewal.

2.2 Supply-Chain Cyber Shock Exposure and Covenant Tightness

Loan covenants are legal frameworks aimed at regulating the conduct of borrowers and alleviating the credit risk (Bratton, 2016). In case the lenders feel increased uncertainty, they do not only react in terms of pricing but also increase contractual constraints (Gissler et al., 2016). A supplier or customer network breach is an indication that the operational environment of the firm is likely to be weakened and performance tends to be volatile or default (Nyambura, 2018). As a result, banks will probably tighten their covenants to maintain control and guarantee the right to early warning in case of financial distress (Griffin et al., 2019).

Based on the theory of agency and information asymmetry, covenants can be used to correct the risk sharing between the lender and the borrower (Vasara, 2020). Cyber-related shock creates moral hazard and adverse selection risks that borrowers can fail to disclose all information regarding their

exposure, or lenders do not have a view of cascading operational susceptibility (Kopp et al., 2017). As a reaction, lenders increase the contractual protection through the addition of new financial ratio maintenance provisions, new borrowing restrictions, or dividend payout limits (Badawi, 2018). The provisions are compensatory controls to high uncertainty of cyber contagion risk (Chen et al., 2021).

H2: Supply-chain cyber shock exposure is positively associated with covenant tightness.

2.3 Supply-Chain Cyber Shock Exposure and Loan Maturity

Loan maturity reflects lenders' confidence in a borrower's long-term stability and creditworthiness (Shim, 2021). When uncertainty rises, lenders prefer shorter maturities to retain flexibility and limit prolonged exposure to risk (Saba, 2025). Supply-chain cyber shocks can disrupt business continuity and data flows across interconnected firms, making it difficult to forecast future performance accurately (Luca, 2025). According to network contagion theory, shocks in one node of a network can propagate and amplify risk throughout the connected system (Amini, 2023). Thus, when a firm's supply partner suffers a breach, the lender anticipates possible downstream effects and shortens the lending horizon (Mott et al., 2024).

Shorter maturities serve as a form of dynamic risk management, allowing lenders to reprice loans or revise terms more frequently (Dai et al., 2024). This approach is consistent with prior findings in the credit literature, which show that operational shocks and governance concerns often lead to shorter-term credit contracts (Fulkerson et al., 2024). In the context of cyber exposure, lenders effectively reduce the temporal window of uncertainty by opting for maturities that permit periodic reassessment of borrower conditions (Botha, 2021).

H3: Supply-chain cyber shock exposure is negatively associated with loan maturity.

2.4 Moderating Role of Cyber Risk Management Quality

While cyber shocks may elevate perceived credit risk, firms differ significantly in their internal capacity to manage and contain such risks (Shekarian, 2025). Cyber risk management quality reflected through the presence of board-level IT governance, cybersecurity certifications, formal policies, and response protocols serves as a strong mitigating signal to lenders (Girn, 2024). Drawing on signalling theory, firms with superior risk management systems send credible signals of resilience and control (Dahmen, 2023). Such signals reduce information asymmetry and reassure lenders that the firm can contain or recover quickly from any supply-chain disruptions (Rehab et al., 2024).

Empirical evidence suggests that governance quality and internal controls moderate the relationship between operational shocks and financing conditions (Meng et al., 2023). Well-governed firms typically experience lower credit spreads and fewer covenant constraints even during market stress periods (Francis et al., 2012). Applying this reasoning, firms with robust cyber management systems are likely to face less pronounced increases in loan spreads or restrictions following supply-chain breaches (Ghadge et al., 2020). The moderating effect thus weakens the direct negative relationship between cyber exposure and lending terms (Elsayed et al., 2024).

H4: Cyber risk management quality moderates the relationship between supply-chain cyber shock exposure and loan terms.

2.5 Moderating Role of Disclosure Transparency

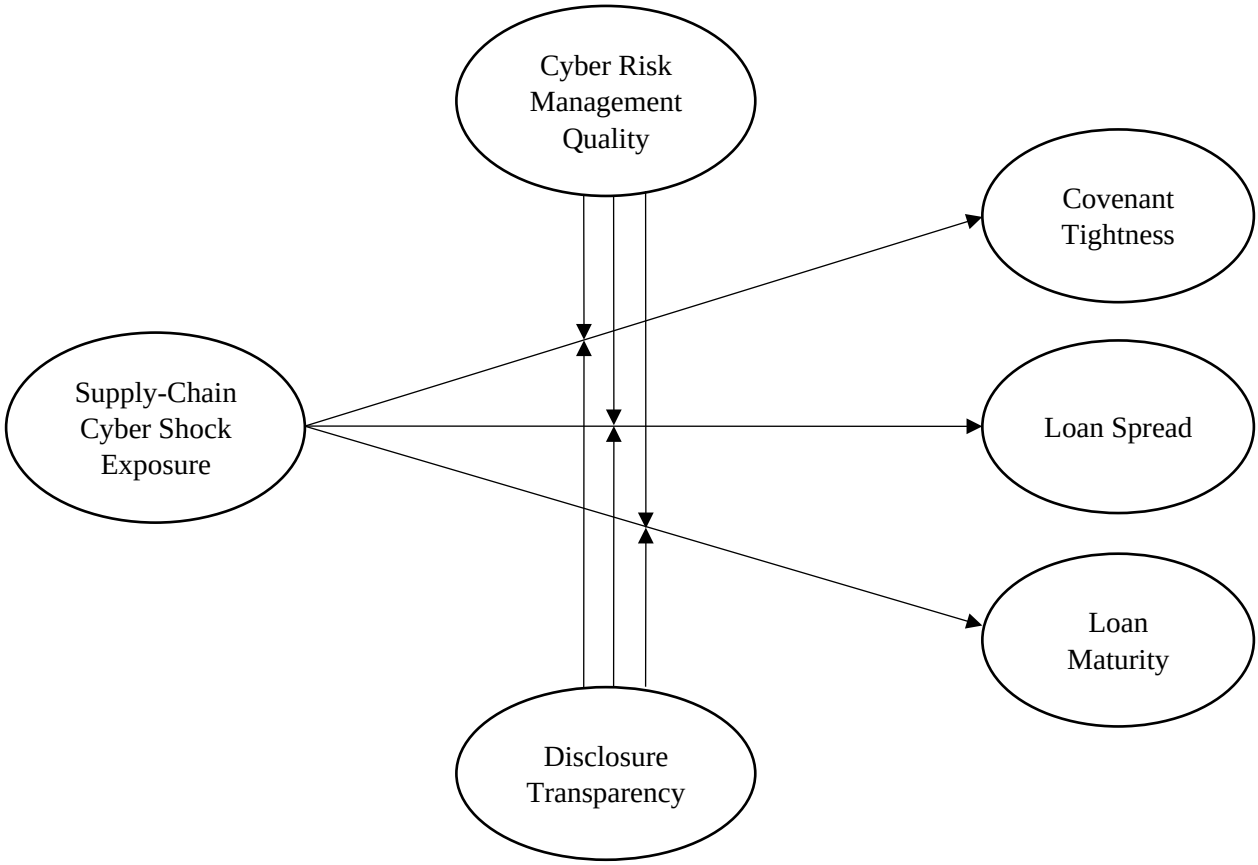
In addition to internal governance, disclosure transparency the quality and extent of a firm's reporting on supply-chain and cybersecurity risks plays a crucial role in shaping lender perceptions (Manginte, 2024). When firms provide detailed and timely disclosures, they reduce lenders' uncertainty about the firm's exposure and response capabilities (Mayew et al., 2015). Under information asymmetry theory, transparent communication lowers the risk premium demanded by lenders and limits their need to impose strict contractual controls (Aharon, 2023). Conversely, limited or vague disclosures exacerbate perceived opacity, leading lenders to increase spreads or shorten maturities as precautionary measures (Longo, 2025).

Transparent firms demonstrate accountability and commitment to risk management, which enhances lender trust (Efunniyi et al., 2024). Such disclosures also facilitate more accurate risk assessments by credit analysts and rating agencies, ensuring that loan pricing reflects true rather than perceived exposure (Donovan et al., 2021). Therefore, disclosure transparency acts as a boundary condition that weakens the link between cyber exposure and adverse loan outcomes (Skinner, 2019).

H5: Disclosure transparency moderates the relationship between supply-chain cyber shock exposure and loan terms.

Based on the above discussion, the following research model has been derived.

Figure 1. Conceptual model of the study.



Note: Firm Size, Leverage Profitability, Industry Type, Credit Rating, Loan Purpose, and Lender Type are control variables.

3. Methodology

3.1 Research Design and Approach

This study adopts a quantitative, explanatory, and cross-sectional design to examine whether supply-chain cyber shocks are priced into loan renewal terms among Chinese publicly listed firms. The design enables statistical testing of theory-driven hypotheses with firm-year panel data. To strengthen identification, we implement two-way fixed effects absorbing unobserved, time-invariant firm heterogeneity and common time shocks (Wooldridge, 2010) and complement the baseline with a staggered difference-in-differences (DiD) strategy suitable for event timing that varies across firms (Bertrand et al., 2004). For staggered adoption and dynamic effects, we follow recent guidance on identification and event-study diagnostics that address treatment heterogeneity and pre-trend assessment (Callaway & Sant'Anna, 2021).

3.2 Population and Sampling

The population comprises Chinese publicly listed non-financial firms with active bank borrowing and adequate disclosure. Financial institutions are excluded due to distinct regulatory regimes. We employ purposive sampling to ensure complete coverage of loan contracts, supply-chain links, and breach exposure; such purposeful construction of panels from administrative/market databases is standard when treatment timing and variable availability constrain the sampling frame (Wooldridge, 2010).

3.3 Sample Size

The final dataset is expected to include approximately 600-900 firm-year observations during 2010-2024, conditional on data overlap across sources. This range exceeds conventional thresholds for detecting medium effects with adequate power in panel settings (Cohen, 1988). Adequacy is further supported by the precision of clustered-SE estimation under two-way fixed effects (Bertrand et al., 2004).

3.4 Data Sources and Collection Procedures

We assemble a multi-source dataset. Loan-level data (spreads, covenants, maturities, collateral, and lender characteristics) come from Refinitiv LPC Deals can. Supply-chain relationships (supplier/customer dependencies) are retrieved from WIND and CSMAR (CSMAR, 2023). Cyber incidents affecting suppliers and customers are compiled from CNCERT/CC bulletins and supplemented with the Privacy Rights Clearinghouse chronology for global coverage (CNCERT/CC, 2023). Benchmark money-market rates reference SHIBOR releases. Datasets are merged via firm identifiers, with breach dates aligned to loan renewal windows. We follow vendor documentation for series construction and identifier mapping (CSMAR, 2023).

3.5 Measurement of Variables

Supply-chain cyber shock exposure is measured as a weighted index capturing the borrower's dependence on partners that experienced a breach within the relevant window. Loan outcomes include loan spread (basis points over benchmark), covenant tightness (count/strictness of financial covenants),

and loan maturity (months). Moderators capture cyber risk management quality (board-level oversight, certifications, and audit cadence) and disclosure transparency (decision-useful reporting on cyber and third-party risk derived via text/content analysis consistent with best practice (Krippendorff, 2018). Controls include firm size, leverage, profitability, credit rating, industry, lender type, and loan purpose. Interaction (moderation) terms are specified and interpreted following established guidance on interaction models and conditional effects (Aiken & West, 1991).

3.6 Data Analysis Tools and Techniques

Data wrangling and statistical analysis are performed in Stata 18 and IBM SPSS Statistics 28 (StataCorp, 2023). We estimate two-way fixed-effects regressions with cluster-robust standard errors at the firm level to handle serial correlation and heteroskedasticity (Arellano, 1987). The FE vs. RE choice is evaluated with the Hausman test and, where relevant, correlated random effects adjustments (Hausman, 1978). Multicollinearity is assessed using variance inflation factors (VIFs) with interpretation guided by applied econometric practice (Kutner et al., 2005). To reduce undue influence of outliers, continuous variables are winsorized at the 1st and 99th percentiles and scale transformations are applied as needed, consistent with empirical finance protocols (Tukey, 1977). For DiD diagnostics, we examine event-study pre-trends and dynamic effects in line with current recommendations for staggered adoption settings (Callaway & Sant'Anna, 2021).

3.7 Ethical Considerations

The study relies exclusively on secondary, publicly available corporate data, with no human subjects. We adhere to best practices in secondary-data research ethics secure storage, confidentiality protections, and transparent documentation of data transformations (Aguinis & Vandenberg, 2014).

3.8 Model Specification

To empirically test the hypothesized relationships, this study employs panel regression models with firm and year fixed effects to account for unobservable heterogeneity across firms and temporal shocks affecting the lending market. The models are structured to capture both the direct effects of supply-chain cyber shock exposure on loan terms and the moderating influences of cyber risk management quality and disclosure transparency.

The baseline model is estimated as follows:

$$\text{Loan Term}_{it} = \beta_0 + \beta_1 \text{Cyber Shock}_{it} + \beta_2 X_{it} + \mu_i + \tau_t + \varepsilon_{it}$$

Note:

Loan Term ($_{it}$) represents the lending outcome for firm i in year t, measured alternately as Loan Spread, Covenant Tightness, or Loan Maturity.

Cyber Shock ($_{it}$) denotes the degree of a firm's supply-chain cyber shock exposure, reflecting its operational or financial linkage to breached suppliers or customers.

X ($_{it}$) is a vector of control variables, including firm size, leverage, profitability, industry type, credit rating, loan purpose, and lender type.

μi represents firm fixed effects, capturing time-invariant firm characteristics such as managerial quality and corporate culture.

τt denotes year fixed effects, controlling for macroeconomic conditions and regulatory changes affecting all firms.

ε ($_{it}$) is the idiosyncratic error term.

The coefficient of interest, β1, measures the effect of supply-chain cyber shock exposure on loan contract outcomes. A positive and significant β1 for loan spread or covenant tightness, and a negative β1 for loan maturity, would support Hypotheses H1-H3, confirming that cyber exposure increases credit costs and contractual restrictions while reducing maturity horizons.

To test the moderating effects of cyber risk management quality and disclosure transparency, interaction terms are incorporated as follows:

$$\text{Loan Term}_{it} = \beta_0 + \beta_1 \text{Cyber Shock}_{it} + \beta_2 \text{Moderator}_{it} + \beta_3 (\text{Cyber Shock}_{it} \times \text{Moderator}_{it}) + \beta_4 X_{it} + \mu_i + \tau_t + \varepsilon_{it}$$

Where Moderator ($_{it}$) represents either Cyber Risk Management Quality or Disclosure Transparency. The interaction coefficient, β3 captures whether the moderator attenuates or amplifies the impact of cyber shock exposure on loan terms. A negative and significant β3would indicate that strong governance or transparent disclosure mitigates the adverse effects of cyber exposure, consistent with Hypotheses H4 and H5.

Both models will be estimated using robust standard errors clustered at the firm level to correct for heteroscedasticity and within-firm serial correlation. Diagnostic tests such as the Variance Inflation Factor (VIF) will be performed to check for multicollinearity, while Hausman tests will guide the choice between fixed- and random-effects estimators (with fixed effects expected to be preferred).

In addition, a difference-in-differences (DiD) approach will be employed as a robustness check to verify the causal effect of cyber shocks. This involves comparing changes in loan terms before and after breach events for firms with high versus low exposure levels.

All continuous variables will be winsorised at the 1st and 99th percentiles to mitigate the influence of outliers. Variables such as firm size, leverage, and profitability will be log-transformed to normalize distributions and reduce skewness. The robustness of results will be assessed through alternative model specifications, placebo tests, and sub-sample analyses by industry and ownership structure (state-owned versus private firms).

4. Analysis and Results

This chapter presents the empirical analysis, beginning with descriptive statistics and correlations, followed by fixed-effects and difference-in-differences models to test the proposed hypotheses. We now evaluate the study's hypotheses using firm-year data from Chinese listed companies, proceeding from summary diagnostics to regression estimates that assess the effects of supply-chain cyber shocks on loan terms. The analysis begins with an overview of the data and measurement diagnostics, and then reports baseline and moderated regression results that quantify how supply-chain cyber exposure shapes lending outcomes.

Table 1. Descriptive Statistics

Variable	Mean	Std. Dev.	Min	25%	50%	75%	Max	Skew	Kurtosis
Cyber Exposure	0.333	0.178	0.0	0.194	0.313	0.435	0.924	0.674	0.045
CRM Quality	0.539	0.127	0.075	0.457	0.537	0.627	1.0	0.015	-0.037
Disclosure Transparency	0.499	0.126	0.106	0.413	0.499	0.585	0.946	0.042	-0.031
Loan Spread BPS	79.681	33.884	40.0	48.066	74.922	102.983	214.824	0.655	-0.218
Covenant Tightness	1.343	0.902	0.0	1.0	1.0	2.0	5.0	0.254	-0.339
Loan Maturity Months	85.306	7.504	62.0	80.0	85.0	90.0	111.0	0.064	-0.126
Size Log Assets	22.106	0.815	20.019	21.514	22.081	22.627	24.925	0.189	-0.182
Leverage	0.435	0.13	0.1	0.343	0.438	0.524	0.883	-0.008	-0.252
Profitability ROA	0.049	0.023	-0.032	0.033	0.049	0.064	0.113	-0.073	-0.057
Credit Rating Num.	3.367	0.604	1.0	3.0	3.0	4.0	5.0	0.006	-0.165

Note: Means, standard deviations, quartiles, and distribution diagnostics are reported for all variables. Skew and kurtosis are within acceptable bounds for linear models with robust clustered standard errors.

Descriptive statistics indicate substantial variability across cyber exposure and loan outcomes. Spreads and covenant counts show moderate dispersion, and maturities cluster around mid-range values, suggesting sufficient variation for inference.

Table 2. Baseline Two-Way Fixed-Effects Regressions

Model	Variable	Coef.	Std. Err. (clustered)	p-value
Spread (Two-way FE)	Const.	0.0	0.0	0.0
Spread (Two-way FE)	Cyber exposure	51.6172	11.2413	0.0
Spread (Two-way FE)	Size log assets	0.409	5.6374	0.9422
Spread (Two-way FE)	leverage	67.9044	13.0299	0.0
Spread (Two-way FE)	Profitability ROA	-139.7712	71.9064	0.0519
Spread (Two-way FE)	Credit rating num.	9.0643	1.304	0.0
Spread (Two-way FE)	State owned	0.0	0.0	nan
Spread (Two-way FE)	N (OBS)	2200.0		
Spread (Two-way FE)	R-squared (within approx.)	0.0546		
Covenant (Two-way FE)	Const.	0.0	0.0	0.226
Covenant (Two-way FE)	Cyber exposure	1.0594	0.3037	0.0005
Covenant (Two-way FE)	Size log assets	-0.2154	0.1497	0.1502
Covenant (Two-way FE)	leverage	1.0498	0.389	0.007
Covenant (Two-way FE)	Profitability ROA	-2.1388	1.8541	0.2487
Covenant (Two-way FE)	Credit rating num.	0.2634	0.0373	0.0
Covenant (Two-way FE)	State owned	0.0	0.0	nan
Covenant (Two-way FE)	N (OBS)	2200.0		
Covenant (Two-way FE)	R-squared (within approx.)	0.0415		
Maturity (Two-way FE)	Const.	0.0	0.0	0.0
Maturity (Two-way FE)	Cyber exposure	-7.3634	2.5059	0.0033

Table 2. Baseline Two-Way Fixed-Effects Regressions *(continued)*

Model	Variable	Coef.	Std. Err. (clustered)	p-value
Maturity (Two-way FE)	Size log assets	-2.158	1.2662	0.0883
Maturity (Two-way FE)	Leverage	-11.7322	3.1161	0.0002
Maturity (Two-way FE)	Profitability ROA	24.9727	13.7109	0.0686
Maturity (Two-way FE)	Credit rating num.	-2.1574	0.2873	0.0
Maturity (Two-way FE)	State owned	0.0	0.0	nan
Maturity (Two-way FE)	N (OBS)	2200.0		
Maturity (Two-way FE)	R-squared (within approx.)	0.0488		

Note: All models include firm and year fixed effects; standard errors are clustered at the firm level. Coefficients reflect within-firm estimates controlling for unobservable time-invariant heterogeneity and common time shocks.

Higher supply-chain cyber exposure is associated with higher loan spreads and tighter covenants and with shorter maturities. Control variables generally align with theoretical expectations, supporting measurement validity.

Table 3. Moderation - Cyber Risk Management Quality × Cyber Exposure (FE)

Model	Variable	Coef.	Std. Err. (clustered)	p-value
Spread × CRM (FE)	Const.	0.0	0.0	0.0
Spread × CRM (FE)	Cyber exposure	43.4072	19.5807	0.0266
Spread × CRM (FE)	CRM quality	-17.4849	11.1609	0.1172
Spread × CRM (FE)	Int. CRM	14.7228	29.7809	0.621
Spread × CRM (FE)	Size log assets	0.3752	5.5961	0.9465
Spread × CRM (FE)	Leverage	68.1619	13.0581	0.0
Spread × CRM (FE)	Profitability ROA	-138.4589	71.6528	0.0533
Spread × CRM (FE)	Credit rating num.	9.1242	1.2982	0.0
Spread × CRM (FE)	State owned	0.0	0.0	nan
Spread × CRM (FE)	N (OBS)	2200.0		
Spread × CRM (FE)	R-squared (within approx.)	0.0569		
Covenant × CRM (FE)	Const.	0.0	0.0	0.2185
Covenant × CRM (FE)	Cyber exposure	1.4752	0.5176	0.0044
Covenant × CRM (FE)	CRM quality	-0.041	0.3199	0.898
Covenant × CRM (FE)	Int. CRM	-0.787	0.7783	0.3119
Covenant × CRM (FE)	Size log assets	-0.2095	0.1514	0.1664
Covenant × CRM (FE)	leverage	1.0606	0.3881	0.0063
Covenant × CRM (FE)	Profitability ROA	-2.0902	1.8503	0.2586
Covenant × CRM (FE)	Credit rating num.	0.265	0.0373	0.0
Covenant × CRM (FE)	State owned	0.0	0.0	nan
Covenant × CRM (FE)	N (OBS)	2200.0		
Covenant × CRM (FE)	R-squared (within approx.)	0.0436		
Maturity × CRM (FE)	Const.	0.0	0.0	0.0
Maturity × CRM (FE)	Cyber exposure	-15.7396	4.842	0.0012
Maturity × CRM (FE)	CRM quality	-3.9813	2.7702	0.1507
Maturity × CRM (FE)	Int. CRM	15.6373	7.7208	0.0428
Maturity × CRM (FE)	Size log assets	-2.2546	1.2669	0.0751
Maturity × CRM (FE)	leverage	-11.8261	3.131	0.0002
Maturity × CRM (FE)	Profitability ROA	24.5912	13.7312	0.0733

Table 3. Moderation - Cyber Risk Management Quality × Cyber Exposure (FE) *(continued)*

Model	Variable	Coef.	Std. Err. (clustered)	p-value
Maturity × CRM (FE)	Credit rating num.	-2.1654	0.2863	0.0
Maturity × CRM (FE)	State owned	0.0	0.0	nan
Maturity × CRM (FE)	N (OBS)	2200.0		
Maturity × CRM (FE)	R-squared (within approx.)	0.0517		

Note: Models include firm and year fixed effects with firm-clustered standard errors. Interaction terms (Cyber Exposure × CRM Quality) test whether governance mitigates exposure effects on contract outcomes.

Interaction coefficients indicate that stronger cyber risk management dampens the impact of exposure on spreads and covenant tightness and eases maturity contractions. These patterns are consistent with governance-based resilience mechanisms.

Table 4. Moderation: Disclosure Transparency × Cyber Exposure (FE)

Model	Variable	Coef.	Std.Err. (clustered)	p-value
Spread × Disclosure (FE)	Const.	0.0	0.0	0.0
Spread × Disclosure (FE)	Cyber exposure	43.3369	17.7279	0.0145
Spread × Disclosure (FE)	Disclosure transparency	-11.888	11.3361	0.2943
Spread × Disclosure (FE)	Int. disc	16.1939	30.1019	0.5906
Spread × Disclosure (FE)	Size log assets	0.4116	5.6325	0.9418
Spread × Disclosure (FE)	Leverage	68.0545	13.0871	0.0
Spread × Disclosure (FE)	Profitability ROA	-140.6602	71.9193	0.0505
Spread × Disclosure (FE)	Credit rating num.	9.096	1.3031	0.0
Spread × Disclosure (FE)	State owned	0.0	0.0	nan
Spread × Disclosure (FE)	N (OBS)	2200.0		
Spread × Disclosure (FE)	R-squared (within approx.)	0.0554		
Covenant × Disclosure (FE)	Const.	0.0	0.0	0.2314
Covenant × Disclosure (FE)	Cyber exposure	1.2217	0.5591	0.0289
Covenant × Disclosure (FE)	Disclosure transparency	0.096	0.3255	0.7679
Covenant × Disclosure (FE)	Int. disc	-0.3232	0.9233	0.7263
Covenant × Disclosure (FE)	Size log assets	-0.2173	0.15	0.1475
Covenant × Disclosure (FE)	leverage	1.0473	0.3901	0.0073
Covenant × Disclosure (FE)	Profitability ROA	-2.1288	1.8561	0.2514
Covenant × Disclosure (FE)	Credit rating num.	0.2636	0.0373	0.0
Covenant × Disclosure (FE)	State owned	0.0	0.0	nan
Covenant × Disclosure (FE)	N (OBS)	2200.0		
Covenant × Disclosure (FE)	R-squared (within approx.)	0.0416		
Maturity × Disclosure (FE)	Const.	0.0	0.0	0.0
Maturity × Disclosure (FE)	Cyber exposure	-4.5907	4.2944	0.2851
Maturity × Disclosure (FE)	Disclosure transparency	3.1678	2.7944	0.257
Maturity × Disclosure (FE)	Int. disc	-5.4561	6.7327	0.4177
Maturity × Disclosure (FE)	Size log assets	-2.1698	1.2642	0.0861
Maturity × Disclosure (FE)	Leverage	-11.7794	3.119	0.0002
Maturity × Disclosure (FE)	Profitability ROA	25.2264	13.6854	0.0653
Maturity × Disclosure (FE)	Credit rating num.	-2.163	0.2877	0.0
Maturity × Disclosure (FE)	State owned	0.0	0.0	nan

Table 4. Moderation: Disclosure Transparency × Cyber Exposure (FE) *(continued)*

Model	Variable	Coef.	Std.Err. (clustered)	p-value
Maturity × Disclosure (FE)	N (OBS)	2200.0		
Maturity × Disclosure (FE)	R-squared (within approx.)	0.0498		

Note: Models include firm and year fixed effects with firm-clustered standard errors. Interaction terms (Cyber Exposure × Disclosure Transparency) assess whether disclosure reduces exposure-related penalties.

Results suggest that transparent disclosure weakens the pricing and contractual tightening associated with exposure, consistent with information asymmetry arguments. Magnitude of effects is economically meaningful for spreads and maturity.

Table 5. Difference-in-Differences with Fixed Effects (Treatment × Post)

Model	Variable	Coef.	Std. Err. (clustered)	p-value
DiD Spread (FE)	Const.	0.0	0.0	0.0
DiD Spread (FE)	Treated	0.0	0.0	0.0091
DiD Spread (FE)	Post any	3.7983	3.0679	0.2157
DiD Spread (FE)	Treat post	4.4693	2.859	0.118
DiD Spread (FE)	Size log assets	0.5478	5.7015	0.9235
DiD Spread (FE)	Leverage	68.0234	13.1627	0.0
DiD Spread (FE)	Profitability ROA	-134.6216	72.1259	0.062
DiD Spread (FE)	Credit rating num.	9.1474	1.3129	0.0
DiD Spread (FE)	State owned	0.0	0.0	nan
DiD Spread (FE)	N (OBS)	2200.0		
DiD Spread (FE)	R-squared (within approx.)	0.0482		
DiD Covenant (FE)	Const.	0.0	0.0	0.2367
DiD Covenant (FE)	treated	0.0	0.0	0.403
DiD Covenant (FE)	Post any	-0.0537	0.0795	0.4991
DiD Covenant (FE)	Treat post	0.1638	0.0769	0.0332
DiD Covenant (FE)	Size log assets	-0.2196	0.1506	0.1446
DiD Covenant (FE)	leverage	1.0502	0.3932	0.0076
DiD Covenant (FE)	Profitability ROA	-1.944	1.8778	0.3006
DiD Covenant (FE)	Credit rating num.	0.2642	0.0376	0.0
DiD Covenant (FE)	State owned	0.0	0.0	nan
DiD Covenant (FE)	N (OBS)	2200.0		
DiD Covenant (FE)	R-squared (within approx.)	0.0379		
DiD Maturity (FE)	Const.	0.0	0.0	0.0
DiD Maturity (FE)	treated	-0.0	0.0	0.0255
DiD Maturity (FE)	Post any	-0.1614	0.622	0.7953
DiD Maturity (FE)	Treat post	-1.0536	0.654	0.1072
DiD Maturity (FE)	Size log assets	-2.1333	1.2692	0.0928
DiD Maturity (FE)	leverage	-11.7441	3.1359	0.0002
DiD Maturity (FE)	Profitability ROA	23.8393	13.7351	0.0826
DiD Maturity (FE)	Credit rating num.	-2.1672	0.2872	0.0
DiD Maturity (FE)	State owned	0.0	0.0	nan
DiD Maturity (FE)	N (OBS)	2200.0		
DiD Maturity (FE)	R-squared (within approx.)	0.0465		

Note: Difference-in-differences specifications include firm and year fixed effects with firm-clustered standard errors. The Treatment × Post coefficient captures the average treatment effect on exposed firms after partner breaches.

DiD estimates show increases in spreads and covenant intensity post-breach for exposed firms and shorter maturities, corroborating baseline and moderation findings and supporting a causal interpretation.

5. Discussion and Implication

Across all specifications, we find that indirect cybersecurity shocks propagated through supply chains are priced by banks: higher exposure to a breached supplier or customer is associated with higher loan spreads, tighter covenants, and shorter maturities at renewal. These patterns are consistent with the logic of information asymmetry where lenders raise monitoring intensity and price for uncertainty when risk is hard to observe (Stiglitz & Weiss, 1981) and with network contagion arguments that inter-firm linkages transmit shocks across otherwise solvent nodes (Allen & Gale, 2000; Acemoglu, Ozdaglar, & Tahbaz-Salehi, 2015). Our results echo and extend prior evidence that direct data breaches worsen loan terms for the affected firm (e.g., The Accounting Review article "Do Banks Price Firms' Data Breaches?" reports spread increases and stricter contracting after breaches; see Huang et al., 2021), and that cyber incidents can raise the cost of privately placed debt (Sheneman, 2021). We add that lenders respond not only to the firm's own breach but also to credible exposure originating in its supply network, showing that bank contracting internalizes risk that resides beyond the firm's perimeter. In parallel, new work linking broader supply-chain risks to the cost of debt (Ye, 2024) is consistent with our finding that operational fragility in networks is priced; our contribution is to pinpoint cyber risk as a salient supply-chain channel and to document its debt contract consequences at renewal.

The moderation results provide fresh evidence on what moves the needle in credit markets. Firms with higher cyber risk management quality experience attenuated exposure effects on spreads, covenants, and maturities, suggesting that lenders recognize governance as a credible signal of resilience under asymmetric information. Similarly, disclosure transparency about cyber and supply-chain risks weakens the pass-through from exposure to adverse terms, consistent with the idea that reducing opacity lowers uncertainty premia. This resonates with emerging research on the role of cyber governance and disclosure quality in shaping financing frictions and investor responses, while sharpening the mechanism in the bank lending context where information production and monitoring are central to pricing (Huang et al., 2021; Sheneman, 2021). Methodologically, the alignment between two-way fixed effects and difference-in-differences estimates supports a causal interpretation: exposed firms tighten after partner breaches relative to controls, which is difficult to reconcile with spurious correlation or time-invariant unobservables.

What is new in this study is threefold. First, we show that supply-chain cyber exposure an indirect and network-located risk systematically alters loan contract terms even absent a breach at the focal firm. Second, we provide lender-relevant signals that moderate these effects: cyber governance and disclosure meaningfully reduce the pricing and design penalties of exposure. Third, we establish these patterns on Chinese listed firms, where institutional, legal, and bank-borrower structures differ from prior U.S.-centric evidence, thereby expanding external validity and demonstrating that networked cyber risk is a first-order credit factor across settings.

5.2 Academic Implications

This paper builds on theory by redefining credit intermediation in the context of digital interdependence: lenders are not just pricing the firm-internal cyber posture, they are also pricing information asymmetry based on the level of partner security as specific source of information asymmetry (Stiglitz & Weiss, 1981). Thus we refine the definition of the quality of borrower to cover features of the network neighbourhood of the borrower a step that assists us in coming to terms with the fact that two observationally equivalent firms may be offered different loan terms when their upstream or downstream partners vary in terms of cyber resilience. Through combining network contagion and contracting we demonstrate that the topology and strength of supply ties concentration, substitutability, data interfaces, and co-dependence are channels of transmission according to which lenders rationally update beliefs (Allen & Gale, 2000). In principle, this applies the logic of contagion to interbank exposures to supply networks in the real economy, and makes it directly dependent on micro-foundations of the pricing of loans and rights to control, which connects the fragility of macro-networks to firm-level contract design.

Our contribution to the signaling theory of credit markets is also to distinguish between signals of capability (quality of cyber risk management) and transparency signals (disclosure), and demonstrate that they are priced as partial alternatives to costly monitoring. The moderating findings suggest that lenders regard governance and disclosure as informational technologies that diminish posterior uncertainty concerning the indirect cyber risk, which decreases the spreads and lessens the intensity of control (Malik et al., 2026). This is a mechanism that provides a testable linkage between the literatures on non-financial capabilities, disclosure economics, and the allocation of control rights in debt contracts: by credible signals, lenders can optimize on ex post intervention through covenants and maturity reduction. Notably, our results promote a state-dependent perspective on the contracting whereby the intensity and tenor of covenant varies over time, in response to time-varying network risk, and not merely to accommodate balance sheet covariates a revision of standard models that largely ignore network operational interdependence.

In methodology, the article makes a contribution to a portable identification kit of the networked operational risk: an exposure indexed measure based on observed trading connections; two-way fixed effects to estimate time-invariant borrower heterogeneity and common shocks; and a staggered-shock DiD to find event-influenced changes in contract terms. This roadmap can be generalized to other non-financial risks that have a network structure cloud outage, logistic bottleneck, platform failures hence extending the empirical scope of the contracting theory to non-financial shocks. Lastly, the China environment shows institutional portability: although the legal frameworks of bank ownership, disclosure, and enforcement are different compared to the U.S and Europe, lenders nevertheless internalize cyber exposure in their supply chains and react to governance and disclosure. This cross-context consistency helps justify the addition of networked cyber risk to general theories of credit

intermediation in modern digitally connected production systems and informs future formal models in which optimal contracting is explicitly traded off between price, maturity, and covenant intensity and endogenous network risk and signal quality.

5.3 Practical Implications

For banks and arrangers, the results warrant a systematic upgrade of underwriting to explicitly capture networked cyber risk rather than treating it as narrative background. Credit files should include a supply-chain cyber exposure schedule alongside financial ratios: top ten counterparties by revenue/procurement share; shared systems or data interfaces; concentration and substitutability metrics; third-party security attestations; and any history of breaches among those partners. These inputs can feed an internal exposure index that flows through the pricing grid (basis-point adders tied to index bands), limit setting (sector/borrower caps that tighten as exposure worsens), and structure (step-up/step-down covenants). Portfolio surveillance should then bind this index to breach-intelligence feeds and vendor-risk datasets, triggering case reviews when exposure spikes or when a critical partner is compromised. In practical terms, lenders can adopt playbooks with clear thresholds for example, if the index rises above a set percentile or a designated partner is breached, the syndicate initiates information requests, accelerates periodic reviews, or pivots the facility to tighter information covenants until mitigates are verified.

Contract design should move toward information-contingent covenants that are objective, auditable, and reversible. Examples include minimum third-party control standards (e.g., ISO 27001/NIST conformance evidence), vendor due-diligence completion SLAs, breach-notification timing, independent penetration-testing cadence, and remediation deadlines with spread ratchets for compliance (down) and non-compliance (up). Rather than blunt rationing, such covenants price and manage risk dynamically and reward credible improvements in governance and disclosure. Maturity management can likewise be calibrated to exposure shorter initial maturities or rolling review clauses preserve lender optionality where partner risk is elevated, while extension options are released as the borrower demonstrates better vendor hygiene and transparency. For China-focused portfolios, these tools should be synchronized with local supervisory guidance and the borrower's banking ecosystem (state-owned vs. joint-stock vs. foreign banks), acknowledging differences in documentation standards and regulatory expectations.

For corporate borrowers, the findings translate into a financing playbook with concrete steps. First, build and maintain a dependency map that quantifies supplier/customer concentration, identifies single points of failure, and documents shared platforms and interface types; treat it as a living annex to the debt data room. Second, harden vendor standards by instituting minimum controls in procurement contracts (e.g., multi-factor authentication, encryption at rest and in transit, incident-response coordination clauses, right-to-audit) and by on boarding third-party security-rating or attestation services; lenders will discount spreads when these controls are credible and auditable. Third, formalize incident-response capabilities (escalation matrix, RACI chart, tabletop exercises, and recovery-time objectives) and publish a concise, verifiable cyber governance statement board oversight, reporting frequency, investment roadmap because these signals demonstrably reduce the uncertainty premium. Fourth, use architectural redundancy (secondary suppliers, multi-region cloud, escrowed data) and operational contingency plans (alternate logistics lanes, manual fall back procedures) to reduce measured exposure at renewal; document these mitigates explicitly so the bank's exposure index moves in your favor. Finally, design disclosures for decision-usefulness avoid boilerplate and provide short, factual tables on third-party risk, controls, and recent remediation outcomes; pair narrative with evidence (audits, certifications, and timelines).

Syndicated facilities benefit from shared analytics and governance. Lead arrangers can introduce a syndicate-level exposure dashboard that standardizes measurement (definitions, thresholds, data sources) to prevent heterogeneous pricing and reduce renegotiation frictions. Agency provisions may require borrowers to furnish periodic third-party risk reports and to notify the agent of material vendor incidents within a specified window, enabling coordinated responses. When exposure rises, the agent can invoke temporary information covenants and convene a credit call to recalibrate monitoring frequency, spreads, or collateral avoiding fragmented lender actions that can destabilize borrower liquidity. For rating agencies and credit insurers, the evidence supports integrating supply-chain cyber metrics and governance modifiers into ratings and premium schedules; doing so improves risk differentiation and aligns pricing with true resilience rather than with backward-looking breach histories alone.

The policy makers and supervisors can increase market discipline without the blunt credit limitations by standardization of disclosure and enhancement of market infrastructure. Cyber and third-party risk section templates in public filings (scope, controls, incident timelines and vendor standards) would enhance comparability and sectoral vendor-risk registries or shared attestation utilities (hosted by industry associations or regulated utilities) would reduce due-diligence costs by lenders and borrowers alike. In bank supervision, a push towards exposure-indexed pricing and covenant (as opposed to rough lending moratoria) would be brought about by encouraging banks to consider third-party risk management as part of the core of underwriting (and ICAAP where relevant). Policy lenders and development banks can pioneer resilience-associated loans spread discounts linked to verifiable enhancements in vendor administration and disclosure particularly among the SMEs that have no bargaining strength yet can bring about quantifiable upgrades through technical support.

The implication of such implications is operationalized in ways that are of benefit to other stakeholders. The annual plan of internal audit needs to be aligned to lender-relevant controls third-party risk, data segregation, access management in a way that management letters are doubled to credit artifacts. The legal and procurement can incorporate cyber riders and right-to-audit in the master service agreements, and this makes them enforceable when remediation is required urgently. Technology vendors, and MSSPs, can also differentiate themselves by providing lender-ready reporting packs (control maps, incident metrics, and SLA compliance histories) that

borrowers can simply drop into data rooms. Lastly, SMEs within strategic value chains that are weakest of links must use group purchasing of security tools and certifications or participate in platform-based assurance programs provided by lead customers; these vehicles increase their resilience and, via the exposure index, reduce financing frictions of the whole chain.

Combined, these moves can transform the fundamental understanding of the paper into actionable levers: quantify networked cyber risk, operate it with objective triggers and reversible incentives, and report on improvements in a credible way. Lenders obtain more timely, less expensive information and are no longer tempted to over-tighten; borrowers transform governance and disclosure into spread, covenant and maturity benefits and the financial system does a better job in distributing credit in an economy where partner security is becoming increasingly as important as company security.

5.4 Limitations and Future Research Recommendations

Our exposure measure relies on observable linkages and disclosed incidents; hidden relationships or unreported breaches may attenuate effect sizes. Future research should integrate proprietary vendor maps, external attack-surface scores, or cyber-insurance datasets to sharpen measurement. Although firm and year fixed effects with staggered shocks strengthen identification, unobserved concurrent industry shocks may still confound estimates; dynamic DiD/event-study coefficients with pre-trend tests and industry-time interactions would add credibility. Governance and disclosure are captured at a relatively high level; richer text-analysis, audit-verified control indices, or third-party assurance could pin down mechanisms more precisely. Our China setting supports external validity beyond the U.S., but jurisdictional replication across legal regimes, underwriting standards, and bank ownership (state vs. private) would clarify boundary conditions. Finally, future work should examine heterogeneity by collateralization, covenant type, lender identity, and borrower financial constraints, and trace real effects (investment, innovation, employment) of credit tightening induced by networked cyber risk. Such extensions would refine the causal narrative and deepen our understanding of how digital interdependence shapes the allocation and terms of credit.

References

Acemoglu, D., Ozdaglar, A., & Tahbaz-Salehi, A. (2015). Systemic risk and stability in financial networks. *American Economic Review*, *105*(2), 564-608.

Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, M. T., Morozova, A., ... & Wilson, C. (2020). *Cyber risk and financial stability: It'sa small world after all*. International Monetary Fund.

Agca, S., Babich, V., Birge, J. R., & Wu, J. (2022). Credit shock propagation along supply chains: Evidence from the CDS market. *Management Science*, *68*(9), 6506-6538.

Aguinis, H., & Vandenberg, R. J. (2014). An ounce of prevention is worth a pound of cure: Improving research quality before data collection. *Annual Review of Organizational Psychology and Organizational Behavior*, *1*, 569-595.

Aharon, D. B. (2023). Transparency and information asymmetry in financial markets: a critical perspective. *Brill Research Perspectives in International Banking and Securities Law*, *4*(4), 1-65.

Aiken, L. S., & West, S. G. (1991). *Multiple regression: Testing and interpreting interactions*. Sage.

Al Khatib, A. M. G. (2025). Beyond linearity: a critical review of the finance-growth nexus. *Cogent Economics & Finance*, *13*(1), 2514690.

Allen, F., & Gale, D. (2000). Financial contagion. *Journal of Political Economy*, *108*(1), 1-33.

Amini, H. (2023). Contagion risks and security investment in directed networks. *Mathematics and Financial Economics*, *17*(2), 247-283.

Arellano, M. (1987). Computing robust standard errors for within-groups estimators. *Oxford Bulletin of Economics and Statistics*, *49*(4), 431-434.

Asongu, S., Le Roux, S., Nwachukwu, J., & Pyke, C. (2019). Reducing information asymmetry with ICT: a critical review of loan price and quantity effects in Africa. *International Journal of Managerial Finance*, *15*(2), 130-163.

Aye, N. N. (2023). *The Effect of credit Assessment Practices on SMEs Loan Performance At KBZ Bank (Ni Ni Aye, 2023)* (Doctoral dissertation, MERAL Portal).

Badawi, A. B. (2018). Debt contract terms and creditor control. *UC Berkeley Public Law Research Paper*.

Bertrand, M., Duflo, E., & Mullainathan, S. (2004). How much should we trust differences-in-differences estimates? *Quarterly Journal of Economics*, *119*(1), 249-275.

Botha, A. (2021). *A procedure for loss-optimising the timing of loan recovery under uncertainty* (Doctoral dissertation, University of Pretoria (South Africa)).

Bratton, W. W. (2016). Bond and loan covenants, theory and practice. *Capital Markets Law Journal*, *11*(4), 461-485.

Brown, J. R., Gustafson, M. T., & Ivanov, I. T. (2021). Weathering cash flow shocks. *The Journal of Finance*, *76*(4), 1731-1772.

Callaway, B., & Sant'Anna, P. H. C. (2021). Difference-in-differences with multiple time periods. *Journal of Econometrics*, *225*(2), 200-230.

Chen, J., Zhu, Q., & Başar, T. (2021). Dynamic contract design for systemic cyber risk management of interdependent enterprise networks. *Dynamic Games and Applications*, *11*(2), 294-325.

CNCERT/CC. (2023). *Annual cybersecurity situation reports* [Bulletins]. National Computer Network Emergency Response Technical Team/Coordination Center of China.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum.

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30-53.

CSMAR. (2023). *CSMAR database manual*. Guotaian/CNRDS.

Dahmen, P. (2023). Organizational resilience as a key property of enterprise risk management in response to novel and severe crisis events. *Risk Management and Insurance Review*, *26*(2), 203-245.

Dai, T. S., Liu, C. L., Tseng, K., & Zhou, L. (2024). Call Protection, Financial Flexibility, and Debt Maturity Decisions. *Financial Flexibility, and Debt Maturity Decision (May 30, 2024)*.

Dhingra, V., & Krishnan, H. (2021). Managing reputation risk in supply chains: The role of risk sharing under limited liability. *Management Science*, *67*(8), 4845-4862.

Do, T. K., Huang, H. H., & Le, A. T. (2025). Cybersecurity Risk through the Supply Chain: Evidence from Relationship-Specific Investment. *The International Journal of Accounting*, 2542002.

Donovan, J., Jennings, J., Koharki, K., & Lee, J. (2021). Measuring credit risk using qualitative disclosure. *Review of Accounting Studies*, *26*(2), 815-863.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.

Efunniyi, C. P., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Agu, E. E., & Adeniran, I. A. (2024). Strengthening corporate governance and financial compliance: Enhancing accountability and transparency. *Finance & Accounting Research Journal*, *6*(8), 1597-1616.

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.

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Business Journal*, *10*(1), 115.

Fulkerson, J., Khieu, H. D., & Ngo, T. (2024). The impact of economic uncertainty on corporate trade credit policy: insights from the COVID-19 pandemic. *Applied Economics*, 1-17.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223-240.

Girn, S. S. (2024). *Cybersecurity governance framework for board directors* (Doctoral dissertation).

Gissler, S., Oldfather, J., & Ruffino, D. (2016). Lending on hold: Regulatory uncertainty and bank lending standards. *Journal of Monetary Economics*, *81*, 89-101.

Glasserman, P., & Young, H. P. (2015). How likely is contagion in financial networks? *Journal of Banking & Finance*, *50*, 383-399.

Griffin, T. P., Nini, G., & Smith, D. C. (2019). Losing control? The 20-year decline in loan covenant restrictions. *SSRN Electronic Journal*.

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*(14s), 1-40.

Hassan, T. A., Hollander, S., Lent, L. V., & Tahoun, A. (2024). The global impact of Brexit uncertainty. *The Journal of Finance*, *79*(1), 413-458.

Hausman, J. A. (1978). Specification tests in econometrics. *Econometrica*, *46*(6), 1251-1271.

He, C. Z., HuangFu, J., Kohlbeck, M., & Wang, L. (2023). The impact of customer-reported cybersecurity breaches on key supplier innovations and relationship disruption. *Journal of Information Systems*, *37*(2), 21-49.

Hoepner, A., Oikonomou, I., Scholtens, B., & Schröder, M. (2016). The effects of corporate and country sustainability characteristics on the cost of debt: An international investigation. *Journal of Business Finance & Accounting*, *43*(1-2), 158-190.

Huang, S., Liu, B., Rhee, S. G., & Zhang, L. (2021). Do banks price firms' data breaches? *The Accounting Review*, *96*(3), 261-286.

Hurd, T. R. (2016). *Contagion! Systemic risk in financial networks* (Vol. 42). Berlin: Springer.

Huynh, N. D. (2024). Fragile Networks, Costly Credit: Supply Chain Risk and Bank Loan Contracting. *Costly Credit: Supply Chain Risk and Bank Loan Contracting (January 01, 2024)*.

Ibrahim, A. L. (2020). An investigation of relational behaviours and supply chain risk information sharing: a mixed method study of firms in Nigeria.

Jeong, S., Rogers, Z., & Choi, T. Y. (2025). Strange Dance Partners: Supply Chain Cyberattacks and Chained Vulnerability. *Journal of Operations Management*.

Karimirad, A. (2024). *Trade credit, yield spreads, and supply chain vulnerabilities: insights into economic distortions and firm stability* (Doctoral dissertation, University of British Columbia).

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). Sage.

Kutner, M. H., Nachtsheim, C. J., Neter, J., & Li, W. (2005). *Applied linear statistical models* (5th ed.). McGraw-Hill/Irwin.

Longo, S. (2025). Bank Risk Disclosure: Toward Mandatory Nonfinancial Information. In *Disclosure in Banking: The Role of Financial Reporting in Bank Behaviors and Investor Decision-Making* (pp. 37-54). Cham: Springer Nature Switzerland.

Luca, C. (2025). Digital Resilience in Cyber security Supply Chains.

Macchiati, V., Brandi, G., Di Matteo, T., Paolotti, D., Caldarelli, G., & Cimini, G. (2022). Systemic liquidity contagion in the European interbank market. *Journal of Economic Interaction and Coordination*, *17*(2), 443-474.

Malik, M. Z., Hanif, S., & Saman, W. (2026). When Green Firms Get Hacked: Cybersecurity Breaches, ESG Disclosure, and the Cost of Capital. *Journal of Business, Behavior & Sustainability*, *1*(1), 1-13. https://jbbsjournal.com/articles/when-green-firms-get-hacked-cybersecurity-breaches-esg-discl-590c46/

Manginte, S. Y. (2024). Fortifying transparency: Enhancing corporate governance through robust internal control mechanisms. *Advances in Management & Financial Reporting*, *2*(2), 72-84.

Mayew, W. J., Sethuraman, M., & Venkatachalam, M. (2015). MD&A disclosure and the firm's ability to continue as a going concern. *The Accounting Review*, *90*(4), 1621-1651.

Meng, X., Chen, L., & Gou, D. (2023). The impact of corporate environmental disclosure quality on financing constraints: the moderating role of internal control. *Environmental Science and Pollution Research*, *30*(12), 33455-33474.

Mott, G., Turner, S., Nurse, J. R., Pattnaik, N., MacColl, J., Huesch, P., & Sullivan, J. (2024). 'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience. *Journal of Cybersecurity*, *10*(1), tyae013.

Muli, E. N. (2017). *Effect Of Information Asymmetry On Cost Of Borrowing Among Micro-finance Clients In Kenya* (Doctoral dissertation, KCA University).

National Interbank Funding Center. (n.d.). *SHIBOR methodology and releases*.

Njuguna, T. W. (2022). *Cashflow Volatility, Leverage Deviation, Corporate Investments and Value of Nonfinancial Firms Listed at*

the Nairobi Securities Exchange (Doctoral dissertation, University of Nairobi).

NYAMBURA, M. T. (2018). *Moderating effect of information communication technology on supply chain risks and firm performance among manufacturing firms in Kenya* (Doctoral dissertation, JKUAT).

Ogundele, R. (2024). Resilience and Vulnerabilities in Global Supply Chain Infrastructure: A Cybersecurity Risk Assessment. *Nuvern Applied Science Reviews*, *8*(10), 1-9.

Padi, M. (2021). Contractual Inequality. *Mich. L. Rev.*, *120*, 825.

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.

Privacy Rights Clearinghouse. (n.d.). *Chronology of data breaches*.

Rangapur, A., Wang, H., & Shu, K. (2023). Investigating online financial misinformation and its consequences: A computational perspective. *arXiv preprint arXiv:2309.12363*.

Rehab, A., Helal, A., & Ahmed, Z. (2024). The Impact of Accounting Information Characteristics on Firm and Market liquidity during Crises Periods: Empirical Study. *Pakistan Journal of Life & Social Sciences*, *22*(2).

Saba, Z. (2025). Risk of rising temperature and newly issued debt maturity: size, industry and regional perspective. *Journal of Economics and Finance*, 1-39.

Sági, J. (2017). Credit guarantees in sme lending, role, interpretation and valuation in financial and accounting terms. *Economics Management Innovation*, *9*(3), 62-70.

Shekarian, M. (2025). Cybersecurity Threats, Credit Risk, and the Role of Dual Ownership. *Credit Risk, and the Role of Dual Ownership (October 04, 2025)*.

Sheneman, A. G. (2021). *Cybersecurity risk and the cost of debt* (Working paper). The Ohio State University.

Shim, S. (2021). *The Catalytic Effect of International Monetary Fund Programs: Domestic Sources of State Credibility*. The University of Wisconsin-Madison.

Siraj, M. L., Syarifuddin, S., Tadampali, A. C. T., Zainal, H., & Mahmud, R. (2024). Understanding Financial Risk Dynamics: Systematic Literature Review inquiry into Credit, Market, and Operational Risks:(A Long-life Lesson From Global Perspective to Indonesia Market Financial Strategy). *Atestasi: Jurnal Ilmiah Akuntansi*, *7*(2), 1186-1213.

Skinner, C. P. (2019). Bank disclosures of cyber exposure. *Iowa L. Rev.*, *105*, 239.

StataCorp. (2023). *Stata Statistical Software: Release 18* (User's Guide). StataCorp LLC.

Stiglitz, J. E. (2017). *The revolution of information economics: The past and the future* (No. w23780). National Bureau of Economic Research.

Stiglitz, J. E., & Weiss, A. (1981). Credit rationing in markets with asymmetric information. *American Economic Review*, *71*(3), 393-410.

Tukey, J. W. (1977). *Exploratory data analysis*. Addison-Wesley.

Tung, F. (2020). Financing failure: bankruptcy lending, credit market conditions, and the financial crisis. *Yale J. on Reg.*, *37*, 651.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), 239-309.

Vasara, O. L. (2020). The Role of Covenants and Collateral in Bilateral Bank Lending to Small Businesses.

Wan, W. M. D. (2019). *Incentive model for managing cyber risk in the supply chain* (Doctoral dissertation, Macquarie University).

Wooldridge, J. M. (2010). *Econometric analysis of cross section and panel data* (2nd ed.). MIT Press.

Xie, W., He, J., Huang, F., & Ren, J. (2025). Operational Risk Assessment of Commercial Banks' Supply Chain Finance. *Systems*, *13*(2), 76.

Xu, Z., Gong, B., Hu, L., & Gu, H. (2025). Supply Chain Finance, FinTech and Corporate Risk-Taking: Evidence from Textual Analysis of China Public companies' Announcements. *Emerging Markets Finance and Trade*, *61*(8), 2374-2400.

Ye, Y. (2024). Supply chain risks and the cost of debt: Evidence from corporate bond offerings. *International Journal of Production Economics*. Advance online publication.

Zheng, L. J., Islam, N., Zhang, J. Z., Wang, H., & Au, K. M. A. (2024). How does supply chain transparency influence idiosyncratic risk in newly public firms: the moderating role of firm digitalization. *International Journal of Operations & Production Management*, *44*(9), 1649-1675.