Cybersecurity Threats, Credit Risk, and the Role of Dual Ownership (JMP)*

Mansoor Shekarian†

September 30, 2025

Abstract

I study how corporate bond markets price cybersecurity risk. Ex-post, bond prices decline significantly following cyberattacks—especially for junk bonds. Ex-ante, a one-standard deviation increase in cyber risk exposure is associated with a 4.3 basis point rise in bond yield spreads. Firms with higher cyber risk also issue bonds with more issuer restrictive covenants. Ownership structure matters: dual ownership—when the same institution holds both debt and equity—attenuates the risk premium to cyber-exposed firms. Using mergers among financial institutions as quasi-exogenous shocks to dual ownership, I find that dual holders reduce firm-level cyber risk and mitigate its pricing in the corporate bond market, but interestingly, not in the equity market. These findings have implications for cybersecurity governance, credit contracting, and SEC disclosure rules, highlighting how financial markets internalize operational risks even in the absence of formal regulation.

JEL Classification: G12, G14, G23, G32, G33

Keywords: Corporate Bond Pricing, Cyber Risk, Dual Holders, Bondholders, Shareholders

*I thank Yong Chen, Adam Kolasinski, Marco Rossi, Brady Twedt, Wei Wu, and the seminar audiences at Texas A&M University. There are no conflicts of interest to disclose. Any remaining errors are my own.

†Mays Business School, Texas A&M University. Email: mansoors@tamu.edu

1 Introduction

Cybercrime has emerged as a significant systemic threat to firms and financial markets, with estimated global losses ranging from $1 to $6 trillion in 2020 (Jamilov, Rey, and Tahoun, 2023). Cyberattacks can trigger severe financial losses, reputational damage, and investor repricing of risk.[1] Recent corporate bankruptcies underscore this threat. In March 2025, 23andMe filed for Chapter 11 bankruptcy after a major data breach exposed sensitive genetic data, overwhelming its legal and financial resources.[2] Similar outcomes followed cyber incidents at Stoli Group USA, Petersen Health Care, and Jerico Pictures. These events illustrate how cybersecurity failures can compromise firms' debt repayment capacity and pose broader risks to credit markets.

Despite the rising frequency and severity of cyberattacks, the corporate bond market's response to cybersecurity risk remains underexplored. This is surprising given the asymmetric exposure between equity and debt holders. While shareholders may tolerate or even benefit from upside risk, bondholders are uniquely vulnerable to downside events that impair cash flow and raise default risk. Cyber incidents—through regulatory fines, loss of customer trust, and operational disruptions—can directly threaten a firm's ability to meet debt obligations, making cybersecurity a first-order concern for creditors.

Yet, the incentives to invest in cybersecurity are not evenly shared. From a theoretical standpoint, cybersecurity functions like a maintenance cost: proactive investment today reduces costly failures tomorrow. However, when firms carry risky debt, equity holders may underinvest in cybersecurity because the benefits of downside protection accrue primarily to bondholders (Myers, 1977; Jensen and Meckling, 1976; Merton, 1974). This misalignment

[1] See Kamiya, Kang, Kim, Milidonis, and Stulz (2021); Florackis, Louca, Michaely, and Weber (2023); Eisenbach, Kovner, and Lee (2022); Crosignani, Macchiavelli, and Silva (2023); Jiang, Khanna, Yang, and Zhou (2024).

[2] 23andMe (Nasdaq: ME) reached a $6 billion market cap after its 2021 IPO but collapsed following a 2023 breach.

creates a bondholder-shareholder conflict that can exacerbate firms' cyber vulnerabilities.

I propose that dual ownership—where financial institutions hold both equity and debt claims—can help bridge the divide between shareholders and bondholders. By internalizing both the upside potential of equity and the downside risk borne by debt, dual holders may promote decisions that better align with the interests of both claimholder classes. In the context of cybersecurity, this alignment could lead to more proactive investment in risk prevention, ultimately reducing credit risk and influencing how bond markets price firm-level exposures. Whether and how this mechanism shapes market pricing remains an open empirical question—one that this paper investigates in the case of cybersecurity risk.

This paper asks three core questions: (1) Do bondholders price cybersecurity risk through yield spreads? (2) Does cybersecurity risk affect bond contract design, particularly covenants and collateral requirements? and (3) Does dual ownership mitigate the cybersecurity underinvestment problem, or amplify investor sensitivity to cyber risk?

First, I find that bondholders price cybersecurity risk through bond market reactions to cyber events. Using data breach events linked to cyberattacks reported to the Privacy Rights Clearinghouse (PRC) between 2005 and 2023, I find that affected firms experience an average cumulative abnormal bond return of -0.4% over the 20 trading days following the breach dates. The effect is substantially more pronounced for high-yield (junk) bonds, which decline by an average of -2% over the same window. These bond market reactions are economically comparable to those in equity markets, where the average cumulative abnormal stock return is approximately -1.5% over the same window.

Turning to ex-ante measures, I use a forward-looking proxy for firm-level exposure to cybersecurity risk based on transcripts in earnings conference calls (Jamilov et al., 2023). I find that a one-standard-deviation increase in cyber risk exposure is associated with a 4.3 basis point increase in bond yield spreads, even after controlling for firm and bond

characteristics. Economically, this translates into an annualized cost of approximately $4 million per firm, or around $6 billion when aggregated across all firms in the sample.

Second, I examine how bondholders in the primary market incorporate cybersecurity risk into contractual design—focusing on covenant intensity and collateral requirements. Guided by incomplete contracting theory (Al-Najjar, 1995), I hypothesize that because cyber risk is difficult to specify ex-ante and costly to verify ex-post, investors rely on covenants as preemptive control rights to mitigate agency conflicts. Supporting this hypothesis, I find that firms with higher cybersecurity exposure issue bonds with significantly more covenants—particularly those related to investment restrictions, dividend payouts, subsequent financing, and event risk—while there is no relationship between cyber exposure risk and collateral requirements. This asymmetry likely reflects the flexible and targeted nature of covenants (Chava, Kumar, and Warga, 2010), which can be tailored to constrain risk-taking and enable early intervention. Overall, the results suggest that cyber risk is not only priced in yield spreads but also embedded in bond design—especially through the structure and scope of covenants.

Third, I examine whether dual ownership mitigates the pricing of cyber risk. Drawing on agency theory and the debt-overhang problem (Myers, 1977; Jensen and Meckling, 1976), I hypothesize that dual ownership mitigates cybersecurity underinvestment by aligning incentives across claim types. Supporting this hypothesis, I find that for financially constrained firms, the positive relationship between cybersecurity exposure and bond yield spreads is significantly weaker when dual ownership is high.

A key identification challenge is that firms with lower inherent risk or stronger governance may naturally attract dual holders, confounding the relationship between ownership structure and cyber risk pricing. To address this concern, I exploit plausibly exogenous shocks to dual ownership caused by mergers between financial institutions. For example, consider two asset managers: one that holds a firm's equity and another that holds its bonds.

If these institutions merge, the combined entity becomes a dual holder of the firm, independent of the firm's own fundamentals. These merger-induced shifts in ownership structure allow me to isolate the causal effect of dual ownership on pricing dynamics.

Post-merger, I find that increases in dual ownership causally reduce firms' ex-ante cybersecurity exposure. Supporting the hypothesis of improved incentive alignment, dual ownership also dampens the sensitivity of bond yield spreads to cyber risk: the yield premium associated with an increase in cyber exposure is significantly smaller for firms with high dual ownership than for matched controls. Interestingly, I find no corresponding effect in equity markets—dual ownership does not alter the sensitivity of stock returns to cybersecurity exposure. This asymmetry suggests that dual holders play a targeted role in mitigating bondholder-specific downside risk, without materially influencing equity market perceptions of cyber risk.

This study contributes to several growing strands of literature. First, this is the first study to examine how cyber risk exposure in corporate bond markets is priced through yield spreads using ex-ante measures. While Iyer, Simkins, and Wang (2020) focus on the realized (ex-post) effects of cyber incidents on bond prices, this study identifies cybersecurity as a novel source of priced risk in bond markets. In doing so, it contributes to the literature on operational and intangible risk factors in credit markets.[3]

Second, this is the first study to investigate the role of dual ownership in mitigating cyber risk exposure. While the dual ownership literature presents mixed findings—some studies suggest that dual ownership enhances governance (Jiang, Li, and Shao, 2010; Bodnaruk and Rossi, 2016; Chen, Zhang, and Zhu, 2023; Chava, Wang, and Zou, 2019; Yang, 2021), while

[3]Recent work by Sheneman (2025) shows that private lenders price borrowers' cybersecurity risk into loan spreads and adjust non-price terms such as collateral. However, private lenders often have access to inside information and engage in bilateral monitoring, limiting the generalizability of these findings to the public bond market. Unlike relationship banks, public bondholders rely entirely on public information and contractual terms, making the pricing of cyber risk and the structuring of bond contracts an open empirical question. This paper addresses that gap.

others point to increased risk-taking (Ferreira and Matos, 2012; Gilje, 2016)—this paper provides new evidence that dual ownership helps mitigate the pricing impact of cyber risk exposure. By aligning the incentives of equity and debt holders, dual ownership reduces bondholders' concerns about cybersecurity risk, thereby lowering the bond yield spreads associated with cyber exposure.

Third, by linking firm-level cyber exposure, bond market reactions, and ownership structure, this paper advances our understanding of the nature of cybersecurity risk and the governance mechanisms through which such risk is mitigated or amplified. This complements emerging literature on how cyber threats affect financial stability, investor behavior, firm reputation, and firm financing decisions (Kamiya et al., 2021; Florackis et al., 2023; Crosignani et al., 2023; Andreadis, Kalotychou, Louca, Lundblad, and Makridis, 2025; Eisenbach et al., 2022; Jiang et al., 2024; Sheneman, 2025; Akey, Lewellen, Liskovich, and Schiller, 2023).

Finally, the findings have important implications for financial regulation and cybersecurity disclosure policy. The SEC (2023b) *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule* requires firms to disclose their cyber risk oversight structures, governance practices, and material incidents. My results indicate that bondholders already price cybersecurity risk into yield spreads—even prior to formal disclosure mandates—and that institutional structures, such as dual ownership, play a critical role in shaping how markets respond to these risks. These findings support the SEC's regulatory direction but also suggest that disclosure alone may be insufficient.

The remainder of the paper is organized as follows. Section 2 provides background and hypothesis development. Section 3 describes the data. Section 4 documents how cybersecurity risk is priced in the corporate bond market. Section 5 explores the moderating role of dual ownership. Section 6 concludes.

2 Background and Hypothesis Development

Cybersecurity risk has emerged as a critical concern for financial markets, corporate governance, and regulatory policy. The National Institute of Standards and Technology (NIST) defines cybersecurity risk as the uncertainty related to information technology (IT), particularly involving data breaches, operational disruptions, or unauthorized access to systems and information (NIST, 2023). As firms increasingly depend on digital infrastructure to conduct operations, store sensitive data, and interface with customers, their exposure to cyber threats has become an essential dimension of firm-level risk management and investor decision-making.

Regulatory responses reflect this shift. The U.S. Securities and Exchange Commission (SEC) has issued multiple rounds of cybersecurity disclosure guidance. In 2011, it released Disclosure Guidance Topic No. 2, requiring firms to disclose material cyber risks and incidents under existing securities law (SEC, 2011). This was followed by a 2018 update that broadened the scope to include the role of board oversight, internal control frameworks, and incident response timelines (SEC, 2018). Most recently, the SEC adopted a comprehensive rule in July 2023—*Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*—mandating registrants to disclose their governance structures, risk management processes, and all material cyber incidents within four business days (SEC, 2023b). Additional proposed amendments target investment advisers, broker-dealers, clearing agencies, and transfer agents (SEC, 2023a,c,d).

These regulatory developments underscore a broader recognition: cyber risk is not merely an operational or legal concern, but a financial risk with implications for valuation, capital access, and systemic stability. A growing academic literature supports this view. Text- and disclosure-based measures of cybersecurity exposure have been shown to predict future attacks and are priced in equity and options markets (Florackis et al., 2023;

Jamilov et al., 2023; Jiang et al., 2024). The global economic cost of cyberattacks is estimated to exceed $200 billion annually, with evidence that these risks propagate through supply chains, financial networks, and payment systems (Eisenbach et al., 2022; Kamiya et al., 2021; Crosignani et al., 2023).

Despite this growing literature, most research has focused on the implications of cybersecurity for equity markets or private loans. By contrast, public bond markets—where pricing, monitoring, and enforcement differ substantially—remain understudied. This distinction is important. A large share of external corporate financing comes from public debt markets, where investor protections must be embedded ex ante into prices, collateral structures, and covenants, with enforcement delegated to trustees. These institutional features mean that public bondholders are especially sensitive to downside risks such as operational failure, reputational damage, and loss given default—all plausible outcomes of severe cyber events.

Cyber risk and bond pricing. Cyberattacks can lead to operational disruption, regulatory fines, litigation, and reputational damage—all of which increase credit risk and potential loss given default. Accordingly, bondholders may demand compensation for cyber risk through higher spreads.

H1: *Firms with higher cybersecurity risk have higher bond yield spreads.*

Cyber risk and bond contract design. Bondholders may also respond to cyber risk via non-price mechanisms, including collateral and covenants. Incomplete contracting theory (Al-Najjar, 1995) suggests that when risks are hard to observe or verify ex post—as with cybersecurity—creditors rely on up-front contractual protections. Collateral provides downside protection in default scenarios and can be especially relevant when cyber risk increases the probability of costly operational failures. In addition, covenants offer more flexible, forward-looking protection. They can restrict risk-taking, impose early control rights, and be tailored

to mitigate specific vulnerabilities. Given the evolving and difficult-to-verify nature of cyber risk, covenants may be preferred over rigid collateral structures.

H2: *Firms with higher cybersecurity risk are more likely to issue bonds with collateral requirements.*

H3: *Firms with higher cybersecurity risk are more likely to issue bonds with a greater number and tighter scope of issuer restrictive covenants.*

Dual ownership as a mitigating governance mechanism. Finally, this paper introduces dual ownership—where financial institutions simultaneously hold both equity and debt in a firm—as a governance mechanism within the cybersecurity-credit risk nexus. Agency theory suggests that dual holders internalize the tradeoffs between equity upside and bondholder downside, reducing incentives for excessive risk-taking and encouraging conservative policies. Chen et al. (2023) show that higher dual ownership reduces option-based CEO compensation (vega) and increases inside debt holdings. In M&A settings, dual holders are more likely to support transactions that benefit bondholders at the expense of equity holders (Bodnaruk and Rossi, 2016). These insights suggest that dual ownership may moderate the pricing of cyber risk.

H4: *Dual ownership attenuates the positive relationship between cybersecurity risk and bond yield spreads.*

These hypotheses extend prior work in important ways. While studies have shown that cyber risk is priced in equities and options (Florackis et al., 2023; Jiang et al., 2024), and that lenders adjust loan terms in response to cyber exposure (Sheneman, 2025), this paper tests whether similar dynamics occur in the public bond market, which differs in pricing mechanisms, enforcement institutions, and investor base. The inclusion of dual ownership as a moderating factor provides a novel governance mechanism that may explain heterogeneity in credit market responses to cyber risk.

In sum, cybersecurity risk is economically significant, increasingly regulated, and priced in multiple capital markets. Studying its impact on the public bond market is important for understanding both firm-level financing and systemic risk. This paper contributes by (i) quantifying the ex ante pricing of cybersecurity risk in corporate bonds; (ii) identifying dual ownership as a mitigating governance mechanism; and (iii) documenting how cyber risk alters the structure of bond contracts, particularly in terms of collateral and covenant design.

3 Data

This section describes the datasets utilized in this study and the data construction procedures employed to build the main variables of interest.

3.1 Privacy Rights Clearinghouse (PRC)

The Privacy Rights Clearinghouse (PRC) aggregates publicly disclosed data breach notifications from U.S. government agencies and corporate disclosures. This dataset spans from 2005 through June 2024 and includes critical details on cyberattacks, such as the type of attack, the actual and reported breach dates, and the name of the targeted organization.[4]

In accordance with state-level breach notification laws, firms are required to report incidents of data compromise to affected stakeholders. For the purposes of this study, I focus exclusively on externally initiated cyberattacks that involve personal data loss—such as malware, ransomware, and network intrusions. This filtering reduces the sample to 38,514 cyberattack incidents across 12,926 firms.

[4] https://privacyrights.org/data-breaches

3.1.1 Fuzzy Matching Procedure: Linking PRC with Compustat

The PRC dataset contains numerous variations of company names, which makes direct linkage to firm-level data in Compustat nontrivial. To facilitate matching, I first standardize the company names by converting them to uppercase and removing common legal entity suffixes (e.g., "INC", "LLC", "LTD", "CORP", etc.).

After standardization, I implement a fuzzy matching algorithm (cosine similarity method) using Jaro-Winkler string similarity with a maximum allowable distance of 0.11. This procedure links the PRC data to Compustat, resulting in 3,973 cyberattack incidents involving 597 unique firms (identified by `Permno`). To reduce potential noise, I retain only one cyberattack incident per firm per day, resulting in 2,410 matched incidents. When restricted to one incident per firm per quarter, the dataset includes 1,030 cyberattacks across the same set of 597 firms.

3.1.2 Firm Financials

Firm-level financial and market variables are obtained from the merged CRSP/Compustat database. After applying standard data quality filters, the sample includes 207,351 firm-quarter observations spanning 7,497 unique firms. Variable definitions and construction procedures are detailed in the Appendix. The cyberattack dataset is merged with CRSP/Compustat using gvkey, year, and quarter identifiers. This results in 260 out of the 597 matched firms being successfully merged with financial data.

3.2 Ex-Ante Cyberattack Exposure Measures

To capture firms' baseline exposure to cybersecurity threats, I use the *ex-ante cybersecurity exposure index* developed by Jamilov et al. (2023). This text-based measure is designed to quantify firm-level exposure to cyber risk using computational linguistics and natural language processing (NLP) techniques. Unlike realized cyber risk—based on observed data

breaches—this measure captures firms' perceived or latent exposure to cyber threats, including vulnerability due to digital operations, technological complexity, and sector-specific attack surfaces.

They constructed this measure using a proprietary NLP pipeline applied to earnings conference call transcripts from over 13,000 publicly listed firms across 85 countries spanning April 2002 through September 2021. For each transcript, they first identify passages discussing cybersecurity topics based on a curated dictionary of cyber-related keywords. These keywords are selected to maximize the precision and recall of cyber-related content, including terms such as "data breach," "malware," "ransomware," "cyberattack," "IT infrastructure," and "digital security."

Once cyber-related passages are extracted, the measure is computed at the firm-quarter level by counting the frequency of cyber-related terms and normalizing it relative to the total length of the transcript. Specifically, the exposure scores are defined as:

$$\text{CyberRisk}_{it}^{A} = \text{Number of cyber-related keywords in firm } i\text{'s call at time } t$$

$$\text{CyberRisk}_{it}^{R} = \frac{\text{CyberRisk}_{it}^{A}}{\text{Total number of words in the transcript at time } t}$$

The normalized score (CyberRisk^{R}) ensures comparability across firms and time periods, controlling for transcript length and verbosity. The resulting exposure indices capture not only the frequency of cyber-related discussions but also the intensity with which firms address these risks in their communication with investors. Importantly, these measures are forward-looking and not mechanically tied to breach events. They reflect managerial awareness, investor concern, and firm-specific vulnerabilities before a cyber incident occurs.[5]

[5]One concern with text-based measures is that they may capture not forward-looking exposure, but simply firm characteristics—such as being in the tech sector—or prior breach experience. (Jamilov et al., 2023) explicitly address this issue through a series of robustness tests. Table IA1 in the Appendix shows that these ex-ante measures continue to predict future attacks when industry and time fixed effects are included.

Second, they examine whether the index is mechanically driven by firms that have previously experienced a breach. They find that cyber-related discussions persist and evolve even in firms that have not been

3.3 Corporate Bond Data from TRACE and FISD

Bond-level data are sourced from the Enhanced Trade Reporting and Compliance Engine (TRACE) and the Fixed Income Securities Database (FISD), which together provide comprehensive coverage of U.S. corporate bond transactions and issue characteristics. The Enhanced TRACE dataset is cleaned up following the guidelines in Dick-Nielsen (2009), which involve removing erroneous, reversed, or corrected trades, as well as filtering out trades with special conditions. I consider only senior unsecured bonds (security level = "SEN") and restrict the sample to U.S. corporate bonds that are non-convertible, non-putable, and have fixed coupon structures. Eligible bond types include "CDEB" (Corporate Debt), "CMTN" (Medium-Term Notes), "CZ" (Zero Coupon), and "CMTZ" (Medium-Term Zero Coupon). To ensure market relevance, I impose the following filters: transactions must be at least $100,000 in size, the original offering amount must be at least $100 million, and both time to maturity and time since offering (bond age) must be at least 6 months. The analysis focuses on both investment-grade and high-yield (junk) bonds, as classified by a numerical credit rating scale ranging from 1 (AAA) to 21 (C).

Daily bond-level prices and yields are constructed using volume-weighted averages of intraday transactions. Yield spreads are computed as the difference between the yield of a bond and the yield of a maturity-matched U.S. Treasury security. After applying all filters, the resulting dataset includes 6,312,710 daily bond transactions with 15,909 unique bonds across 1,659 issuing companies between 2004 and September 2021.

The calculation of abnormal bond return closely follows (Bessembinder, Kahle, Maxwell, and Xu, 2008). To compute bond returns for the days with transactions, I require that there

attacked, suggesting that the index captures broader organizational concern rather than backward-looking event response.

Finally, they validate the measure through predictive modeling. Higher values of the cyber exposure index predict a significantly greater likelihood of future cyberattacks—both in- and out-of-sample. The authors also show that the index predicts adverse valuation outcomes, heightened investor sensitivity to cyber-related news, and greater spillover risk to peer firms.

be at least one additional transaction within a 14-day window before the trade date. Bond returns from day $t-1$ to t are calculated using the formula:

$$R_{t-1,t} = log(\frac{P_t + AI_t + C}{P_{t-1} + AI_{t-1}})$$

where P_t is the bond price on day t, AI_t represents the accrued interest, and C is equal to the coupon payment if it falls within the period considered.

Abnormal bond returns (ABR) are calculated by subtracting the return of a benchmark portfolio matched on credit rating and maturity:

$$ABR_{t-1,t} = R_{t-1,t} - BM_{t-1,t}$$

Benchmark portfolios are constructed using 24 groupings: six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Benchmark portfolio return within each group is calculated as the outstanding amount weighted average bond returns. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings (Bindal and Rossi, 2024).

3.4 Institutional Holdings

To measure dual ownership—the extent to which institutional investors simultaneously hold both equity and debt claims on the same firm—I use institutional holdings data from two sources. Equity ownership data are obtained from the SEC Form 13F filings, which report quarterly equity positions held by institutional investors with more than $100 million in assets under management. Corporate bond holdings are sourced from the Lipper eMAXX database, which provides detailed position-level data on fixed-income securities held by mutual funds, insurance companies, and other large institutions.

Following the methodology of Bodnaruk and Rossi (2016), I construct three firm-level

measures of dual ownership:

- **DEO**: The fraction of a firm's total shares outstanding held by dual holders—that is, institutional investors who hold both the firm's equity and its debt in a given quarter:

$$\text{DEO} = \frac{\text{Shares held by dual holders}}{\text{Total shares of the firm}}.$$

- **DEO**^{inst}: The ratio of equity held by dual holders to total institutional equity ownership. This variable captures the relative importance of dual holders among all institutional equity investors:

$$\text{DEO}^{inst} = \frac{\text{Shares held by dual holders}}{\text{Total institutional shares held}}.$$

- **DEO**^{cond}: A conservative dual ownership measure restricting the sample to investors whose ownership share lies between 5% and 95%:

$$\text{DEO}^{cond} = \frac{\text{Shares held by dual holders with equity and debt between 5\% and 95\%}}{\text{Total shares of the firm}}.$$

  This helps exclude noise from marginal holders and avoid distortions from extremely concentrated positions or outliers.

These variables are constructed at the firm-quarter level by matching institutional identities across 13F and eMAXX datasets (matching by their standardized brand names assigned to each financial conglomerate).

3.5 Summary of Statistics

The final sample spans firm financials and corporate bond market transactions from 2004 through September 2021. All continuous variables are winsorized at the 1% and 99% percentiles.

Figure 1 presents the annual distribution of reported cyberattack incidents by industry from 2007 through June 2024. The figure highlights a pronounced upward trend in cyber incidents over time, with a marked acceleration beginning in the mid-2010s and a peak occurring in 2023. This spike coincides with the implementation of the U.S. Securities and Exchange Commission's *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule*, adopted in July 2023 (SEC, 2023b). The rule mandates more rigorous and timely disclosure of material cybersecurity incidents, likely contributing to the surge in reported cases during that period.

Sectoral patterns indicate that the finance, service industries, manufacturing, and wholesale and retail trade sectors bear the highest concentration of incidents. These industries—characterized by high digital integration, customer data sensitivity, and supply chain complexity—collectively account for the majority of reported cyber events, highlighting the systemic nature of cybersecurity risk across key segments of the economy.

Table 1.A presents summary statistics of firm-level quarterly financial characteristics for two groups: firms that never experienced a cyberattack, and firms that experienced a cyberattack—measured in the quarter before the incident. Firms affected by cyberattacks tend to be larger in terms of total assets and market capitalization, older, more levered, more financially constrained, and owned by more institutional investors.

Table 1.B presents summary statistics assessing the relationship between *ex-ante* measures of cybersecurity risk exposure (from Jamilov et al. (2023)) and realized (*ex-post*) cyberattack incidents (from PRC). The results show that firms that are later targeted by cyberattacks exhibit significantly higher levels of ex-ante cyber risk exposure across both the absolute and relative measures. Specifically, the average cyber risk count and relative exposure scores are markedly higher among the attacked firms, with the differences in means and medians statistically significant at the 1% level. These findings support the construct validity of the cyber risk exposure index as a forward-looking proxy for latent vulnerability

to cyber threats.

Table 1.C presents summary statistics assessing the relationship between dual ownership and realized (*ex-post*) cyberattack incidents (from PRC). Across all three constructed measures of dual ownership—DEO (dual equity ownership), DEO^{inst} (dual ownership scaled by institutional ownership), and DEO^{cond} (conservative dual ownership threshold)—firms that are subsequently targeted by cyberattacks exhibit significantly higher levels of dual ownership. The differences in both means and medians are statistically significant at the 1% and 5% levels. These results suggest that dual ownership is more prevalent in firms that are vulnerable to cybersecurity threats. This pattern may arise because these firms tend to be larger and more widely held by institutional investors (Table 1.A). Alternatively, it may reflect institutional investors' strategic preference for holding overlapping claims in firms with heightened operational or cybersecurity risk—either to enhance monitoring capacity, strengthen control over risk management practices, or better align managerial incentives. These findings reinforce the relevance of examining dual ownership as a potential moderating mechanism in how cybersecurity risk is priced in corporate bond markets.

Table 1.D summarizes key characteristics of the corporate bond sample used in this study. On average, bonds in the sample exhibit a yield spread of 2.14% and a yield to maturity of 4.01%. The average credit rating is 8.25, corresponding to investment-grade status. The average bond has a time to maturity of 8.84 years and a face value offering amount of approximately $964 million. Daily trading volume averages $4.78 million, with considerable variation across issues.

4 Findings

4.1 Cyberattacks and Bond Return: Event Study

In this section, I examine the reactions of bond and equity markets to the dates of the cyberattack breaches. To assess the abnormal performance of corporate bonds (stocks), I conduct an event study around the breach date and compute cumulative abnormal returns (CARs) over varying post-event windows.

Figure 2.A presents the results of this analysis for bond returns. The event window spans $[-10, t]$ trading days, where $t = 1, 2, ..., 63$. Abnormal bond returns are computed by subtracting the return of a benchmark portfolio matched on credit rating and maturity. Benchmark portfolios are constructed using 24 combinations of six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Returns are weighted by outstanding par value.

The figure illustrates that bonds of firms affected by cyberattacks experience a statistically significant decline in value. On average, these bonds show a CAR decline of approximately -0.4% over the 20 trading days following the breach. Given that the typical firm in the sample has roughly 10 outstanding bonds, this decline translates to an estimated firm-level loss of $40 million over the 20 trading-day period. Extrapolating these results to the broader sample suggests that cyberattacks in the corporate bond market lead to an aggregate market value loss of approximately $4.5 billion for the affected firms within 20 trading days following the breach.

Next, I examine heterogeneity in market responses by credit quality. Figure 2.B presents CARs for investment-grade bonds, which constitute approximately 83% of the sample. The reaction of these bonds to cyberattack breaches is relatively slow: CARs decline by about -0.3% over the 20-trading day window. The magnitude of the decline suggests that bondhold-

ers in investment-grade firms perceive lower default risk and stronger operational resilience following cyber incidents.

In contrast, Figure 2.C shows that high-yield (junk) bonds exhibit a substantially more severe and protracted response. CARs for junk bonds fall sharply—by roughly -2% over the 20-trading day window. This pronounced decline implies that investors in lower-rated bonds anticipate greater downside risks and higher potential credit losses in the aftermath of a cyberattack. The findings are consistent with the view that high-yield issuers—typically more leveraged and less diversified—are more exposed to operational disruptions, reputational damage, and funding constraints resulting from cybersecurity breaches.

Together, these findings demonstrate that the pricing of cybersecurity risk varies systematically across credit quality. While bondholders of investment-grade firms appear to partially discount the potential consequences of cyber incidents—likely due to stronger fundamentals and greater perceived resilience—investors in speculative-grade debt demand a steeper risk premium. This is reflected in more severe post-event price adjustments and suggests that credit markets differentiate cyber risk exposure based on firms' underlying creditworthiness.

To benchmark these credit market reactions against the equity market, I conduct a parallel event study using daily stock returns for the same set of firms. Figure 2.D shows that the equity market reacts more swiftly and sharply to the breach dates. On average, affected firms experience a -1.5% decline in market capitalization within 20 trading days of the data breach. These effects are economically meaningful: extrapolating to the full sample, I estimate that cyberattacks lead to an aggregate market value loss of approximately $28 billion among publicly traded firms in my sample within 20 trading days following the breach.

Overall, these results highlight the substantial financial impact of cybersecurity breaches across both debt and equity markets. They also reveal heterogeneity in market reactions,

with lower-rated bonds and equities exhibiting greater sensitivity to cyber-related shocks. Taken together, the findings underscore the importance of incorporating cybersecurity risk into models of credit pricing, risk assessment, and asset valuation.[6]

4.2 Cybersecurity exposure and Bond Yield Spread

To quantify the impact of cybersecurity risk exposure on corporate bond pricing, I estimate the following regression model at the bond-quarter level:

$$\text{YieldSpread}_{i,t} = \beta_0 + \beta_1 \cdot \text{CyberRisk}_{i,t} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t} \tag{1}$$

where the dependent variable is the end-of-quarter bond yield spread for bond i in quarter t. The key independent variable is a measure of firm-level cybersecurity exposure. Control variables include bond-level characteristics—such as credit rating, time to maturity, coupon rate, and offering amount—as well as firm-level covariates, including total assets, leverage, firm age, return volatility, return on assets (ROA), and the book-to-market ratio. The specification includes both year-quarter fixed effects and industry fixed effects, with standard errors clustered at the firm and year-quarter levels.

Table 2.A presents the main regression results. Column (1) shows that a one-unit (standard deviation) increase in log-transformed $CyberRisk^A$ is associated with a statistically significant 5.5 bps (4.3 bps) increase in yield spread. Employing a standardized measure of cyber risk exposure, Column (2) shows that a one-unit (standard deviation) increase in $CyberRisk^R$ is associated with a statistically significant 6.1 bps (4.2 bps) increase in yield spread. These results are economically significant. Given that the average firm in the sample issues approximately 10 bonds, the estimated increase in yield spreads translates into an

[6]The PRC dataset does not provide the actual breach date for all firms in the sample (available for 70% of the sample). On average, there is a 151-day latency between the actual breach date and the breach announcement date by firms. Figures IA1.A, IA1.B, IA1.C, and IA1.D in the appendix replicate the same descriptive analysis using the announcement dates of the cyberattacks. The results remain consistent.

annualized cost of roughly $4 million per firm, or $6 billion when aggregated across all firms in the sample.

To test the robustness of these findings, Columns (3) and (4) replace the contemporaneous yield spread with the one-quarter-ahead spread as the dependent variable. The coefficients remain stable in magnitude and significance. Both results support the hypothesis **H1** that cybersecurity exposure is priced into the cost of corporate debt.

As an additional analysis, I examine whether cybersecurity exposure contributes to increases in firms' perceived default risk. I estimate a two-part model of Expected Default Frequency (EDF). For the extensive margin—the likelihood that a firm is perceived as default-immune—I employ a zero-inflated Poisson (ZIP) model. For the intensive margin—variation in EDF conditional on being positive—I use a Tweedie regression, a type of generalized linear model.

Table IA2 presents the results. Columns (1) and (2) report estimates from the ZIP model. The coefficient on $\log(1+\text{CyberRisk}^A)$ is negative and statistically significant at the 1% level, indicating that higher cyber exposure is associated with a lower probability of being classified as risk-free (EDF = 0). Specifically, a one unit (standard deviation) increase in $\log(1+\text{CyberRisk}^A)$ corresponds to a 0.53 (0.38) percentage point decrease in the probability of EDF being a structural zero, holding all other variables at their means.

Columns (3) and (4) report the Tweedie regression results conditional on EDF > 0. Here, the coefficient on CyberRisk^A remains positive and statistically significant, suggesting that among firms already assigned a non-zero default probability, greater cyber exposure is associated with a higher expected intensity of default risk. Economically, a one unit (standard deviation) increase in $\log(1+\text{CyberRisk}^A)$ is associated with a 0.0046 (0.0033) unit increase in EDF. Given a conditional EDF mean of 0.0432, these effects imply a 10.7% (7.6%) increase in EDF.

Taken together, these findings indicate that cybersecurity exposure plays a meaningful role in shaping market perceptions of credit risk—both by increasing the likelihood that a firm transitions from zero to positive default probability (extensive margin) and by raising the expected level of default risk among firms already perceived as risky (intensive margin).

4.3 Cybersecurity exposure and Covenants/Collateral

Bondholders may respond to cyber risk through non-price mechanisms. One such mechanism is collateralization, which provides downside protection in the event of default. Another mechanism is covenant intensity. Tighter covenants allow bondholders to restrict managerial behavior, accelerate control rights, and monitor performance more effectively.

I turn to the primary bond market to examine whether cybersecurity exposure influences bond contract design at the time of issuance. Specifically, I investigate whether bondholders demand stronger contractual protections—such as covenants or collateral—when firms have higher cyber risk exposure. If so, it would suggest that investors preemptively price cyber risk through non-price mechanisms during bond origination.

To test this, I estimate the following regression model:

$$\mathrm{Y}_{i,t+1} = \beta_0 + \beta_1 \cdot \mathrm{CyberRisk}_{i,t} + \beta_2 \cdot \mathrm{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t} \tag{2}$$

where the dependent variable $Y_{i,t+1}$ represents either (i) the number of covenants included in a newly issued bond or (ii) a binary indicator equal to one if the bond is collateralized and zero otherwise. The sample consists of 7,610 unique bonds issued in the primary market between 2004 and 2021 (September).

The covenant variable is constructed from Mergent FISD and captures the presence of 26 covenants, including 8 bondholder-protective and 18 issuer-restrictive clauses. Poisson regression is used to model covenant intensity. As shown in Table 2.B, Column (1) indicates

that a one standard deviation increase in $\log(1+\text{CyberRisk}^A)$ is associated with a statistically significant 0.10-unit increase in the number of covenants. Given the unconditional mean of 4.46 covenants per bond, this implies a 2.25% increase in covenant intensity. Column (2) shows similar results using the relative measure CyberRisk^R.

Columns (3) and (4) report results from logistic regressions where the dependent variable is an indicator for whether the bond is collateralized. While the coefficients on cyber exposure are positive in both specifications, they are not statistically significant. This suggests that, conditional on firm and bond characteristics, cyber risk is not systematically associated with the likelihood of issuing secured debt.

Together, these findings indicate that bondholders incorporate cyber risk into contract design primarily through the inclusion of more covenants rather than collateral requirements(in support of **H2** but not **H3**). The presence of additional covenants may serve as a contractual safeguard against operational, financial, or reputational disruptions stemming from cyber incidents. This highlights the role of bond covenants as an ex ante risk-mitigation mechanism when pricing hard-to-quantify risks such as cybersecurity exposure.

5 Dual Ownership

The presence of dual ownership—when financial institutions hold both debt and equity in the same firm—may moderate the relationship between cybersecurity risk and the cost of debt. By internalizing the trade-off between bondholder protection and equity upside, dual holders have stronger incentives to limit risk-taking and support policies that preserve firm value, particularly in high-risk settings such as cyber-vulnerable firms.

Table 3.A examines the relationship between dual ownership and cybersecurity risk exposure. Columns (1)–(3) use a Tweedie model to estimate the impact of dual ownership on continuous measures of cyber risk. Column (1) shows that a one-standard-deviation increase

in dual equity ownership (DEO) is associated with a 4.7 (0.8) percentage point reduction in cyber exposure, as measured by the relative cyber risk index (CyberRisk^R). This negative relationship is consistent across Columns (5) and (6), indicating that dual ownership is associated with a lower intensity of cyber vulnerability as perceived by markets.

Table 3.B extends these results by interacting dual ownership with firms' expected default risk (EDF). Columns (1)–(3) examine this interaction using ex-ante cyber risk measures. The results indicate that among financially distressed firms (high EDF), dual ownership is more strongly associated with reductions in cyber exposure compared to firms with low EDF. Economically, a one-standard-deviation increase in dual ownership corresponds to roughly 8%–10% lower cyber risk exposure for financially constrained firms.

Taken together, these findings suggest that dual ownership plays a risk-mitigating role by reducing perceived cybersecurity risk—especially among financially constrained firms. By aligning incentives across the capital structure, dual holders encourage stronger cyber risk governance and enhance the perceived resilience of firms facing elevated default risk.

5.1 Identification: M&A Among Financial Institutions

To establish a causal relationship between dual ownership and cybersecurity-related bond pricing, I exploit mergers among financial institutions as a quasi-exogenous source of variation in dual ownership. This strategy addresses key endogeneity concerns—such as the possibility that inherently safer firms attract dual holders or that unobserved firm characteristics jointly influence both cyber risk exposure and investor structure.

Specifically, I identify mergers in which the combining institutions held complementary positions in the equity and debt of the same target firms prior to the merger. A treated firm is defined as one in which, after the merger, the acquiring financial institution holds at least 1% of the bonds outstanding and 1% of the shares outstanding of the target firms. For

example, if institution A held a significant equity stake and institution B held a significant bond position in a firm, their merger results in the creation of a new dual holder for that firm. Importantly, I exclude cases where either institution was already a significant dual holder pre-merger to ensure that the treatment captures a meaningful and new increase in dual ownership.

The identifying assumption underlying this strategy is that the causes of mergers among financial institutions are plausibly unrelated to the cyber risk exposure of the target firms in their portfolios. Thus, this setting offers a valid source of quasi-random variation in dual ownership, enabling identification of its causal effect on cyber risk and bond pricing outcomes.

Following the approach of Chen et al. (2023) and Lewellen and Lowry (2021), I adopt their sample of financial institution mergers between 2006 and 2014. To identify plausibly exogenous increases in dual ownership, I impose the requirement that either party to the merger must hold at least 1% of the target firm's outstanding equity and at least 1% of its outstanding bonds—but that neither party simultaneously holds both positions one quarter prior to the M&A announcement. This restriction ensures that the merger creates a new dual holder, rather than intensifying an already existing one.

Applying this definition reduces the sample to 8 qualifying M&A events, of which 6 have observable bond transactions in the TRACE database during the quarter prior to the merger announcement. After merging with TRACE and Compustat and applying standard filters, the final treatment group consists of 210 unique treated firms and 636 unique treated bonds. If a firm is affected by multiple qualifying M&As, only the first event is retained for identification to avoid confounding overlapping treatments.

Table 4 summarizes the list of M&A transactions, along with the number of treated firms and bonds associated with each merger. The largest event in the sample is the merger

between BlackRock and Barclays Global Investors, which generates 140 treated firms and 396 treated bonds. On average, each M&A event affects 26 treated firms and 80 treated bonds. The average time from the M&A announcement to its completion is approximately two quarters.

By construction, treated firms experience a discrete increase in significant dual holders following the merger. Figure 3 illustrates the evolution of significant dual ownership around the M&A announcement. The number of significant dual holders remains stable in the quarters leading up to the merger, followed by a notable increase starting at the time of announcement. By the end of the second post-announcement quarter, the average treated firm has 0.6 to 1 more significant dual holders than before the merger. This pattern confirms that financial institution mergers serve as a meaningful and persistent shock to dual ownership structure.

To evaluate how dual ownership alters firms' cybersecurity exposure, I employ a stacked difference-in-differences (DID) framework. Control firms are matched to treated firms using propensity score matching (PSM) based on firm size, market-to-book ratio, and return volatility. I require that the control firm characteristics to be within one standard deviation of those of the treated firm. Matching is conducted within SIC2 industries and calendar year-quarters to ensure comparability. In addition, I require that control firms do not have any significant dual holders—defined as institutions holding at least 1% of both equity and bond positions in the firm—during the matching quarter. The baseline regression is specified as follows:

$$\begin{aligned} \text{CyberRisk}_{i,t+1} = \beta_0 + \beta_1(\text{Treated}_{i,t} \times \text{Post}_{i,t}) + \beta_2 \cdot \text{Treated}_{i,t} + \beta_3 \cdot \text{Post}_{i,t} \\ + \beta_4 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t} \end{aligned} \tag{3}$$

In this specification, $\text{Treated}_{i,t}$ is an indicator for firms in which, prior to the merger announcement $(t-1)$, each merging financial institution held at least 1% of the firm's outstand-

ing equity and 1% of its outstanding bonds but that neither party simultaneously held both positions. The $\text{Post}_{i,t}$ period includes quarters $t+1$ through $t+6$, while the pre-treatment period includes $t-4$ through $t-1$. The merger announcement quarter ($t=0$) is excluded from the regression. The fixed effects η_c and η_t capture industry and cohort-by-year-quarter variation to address dynamic treatment effects and merger timing heterogeneity, following Chen et al. (2023) and Gormley and Matsa (2011).

Table 5 reports the results of regression 3, where the dependent variable is CyberRisk^R, estimated using a Tweedie regression model.[7] The coefficient on the interaction term Treated× Post is negative and statistically significant, indicating that cyber risk exposure declines following a merger-induced increase in dual ownership. Specifically, for treated firms, the relative cyber risk measure (CyberRisk^R) decreases by 0.311 units post-merger relative to control firms. Given that the conditional mean of CyberRisk^R is 0.53, this corresponds to a 58% reduction—an economically meaningful decline.

To evaluate how dual ownership impacts the relationship between cyber risk exposure and bond yield spreads, I implement a stacked difference-in-differences (DID) framework. Control bonds are matched to treated bonds using propensity score matching (PSM) based on firm size, market-to-book ratio, return volatility, and bond time to maturity. Matching is restricted to pairs where the control bond characteristics fall within one standard deviation of the treated bond's characteristics. To ensure comparability, matching is also conducted within the same investment-grade status, SIC2 industry classification, and calendar year-quarter. Additionally, I require that control firms have no significant dual holders—defined as institutions holding at least 1% of both the firm's equity and bonds—during the matching

[7] In Table IA3 in the appendix, I use CyberRisk^A as the dependent variable and run a Poisson regression model in Equation 3. The results show that for treated firms, the absolute cyber risk measure (CyberRisk^A) decreases by 0.234 units post-merger relative to control firms. Given that the conditional mean of CyberRisk^A is 1.04, this corresponds to a 23% reduction.

quarter. The baseline regression specification is as follows:

$$\begin{aligned}\text{YieldSpread}_{i,t+1} = \beta_0 &+ \beta_1(\text{Treated}_{i,t} \times \text{Post}_{i,t} \times \text{CyberRisk}_{i,t'}) \\ &+ \beta_2(\text{Treated}_{i,t} \times \text{CyberRisk}_{i,t'}) + \beta_3(\text{Post}_{i,t} \times \text{CyberRisk}_{i,t'}) \\ &+ \beta_4(\text{Treated}_{i,t} \times \text{Post}_{i,t}) + \beta_5 \cdot \text{Treated}_{i,t} + \beta_6 \cdot \text{Post}_{i,t} \\ &+ \beta_7 \cdot \text{CyberRisk}_{i,t'} + \beta_8 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}\end{aligned} \tag{4}$$

Here, $\text{Treated}_{i,t}$ is an indicator for bonds issued by firms where, in quarter $t-1$, each merging financial institution held at least 1% of the firm's outstanding equity and 1% of its outstanding bonds, but neither institution held both simultaneously. The $\text{Post}_{i,t}$ period spans from $t+1$ to $t+6$, while the pre-treatment period includes quarters $t-4$ to $t-1$. The merger announcement quarter ($t = 0$) is excluded from estimation. The variable $\text{CyberRisk}_{i,t'}$ captures the pre-merger level of relative cyber risk exposure (CyberRisk^R), fixed at its value in quarter $t-1$ and held constant in subsequent periods. This approach isolates the impact of pre-existing cyber risk on yield spreads, conditional on changes in dual ownership, and avoids confounding the results with potential changes in cyber risk that may arise after the merger. The specification includes industry fixed effects (η_c) and cohort-by-year-quarter fixed effects (η_t) to control for time-varying industry trends and merger timing heterogeneity.

Table 7 presents the results from the stacked difference-in-differences analysis. The coefficient on the triple interaction term—Treated × Post × CyberRisk—is negative and statistically significant, indicating that, conditional on pre-merger cyber risk exposure, the post-merger increase in dual ownership attenuates the bond market's pricing of cyber-related risk. Specifically, for treated bonds, a one-unit (standard deviation) increase in pre-merger CyberRisk is associated with a 129 (55) basis point smaller increase in yield spread relative to control bonds, suggesting that bondholders demand a lower cyber risk premium after the emergence of significant dual holders.[8]

[8] In Table IA4 in the Appendix, I use CyberRisk^A as a measure of cybersecurity risk exposure and estimate regression 4. The results remain similar.

Figure 5 displays the dynamic DID estimates, which show that this differential pricing effect emerges shortly after the merger announcements and persists for at least six quarters. These findings reinforce the interpretation that dual holders—by aligning equity and debt incentives—can temper market concerns about cyber risk and improve credit market outcomes for cyber-vulnerable firms.

To evaluate how dual ownership impacts the relationship between cyber risk exposure and stock returns, I use the same DID framework in Equation 4 and regress the quarterly stock return ($R_{i,t+1}$) on Treated $\times$ Post $\times$ CyberRisk. Table 7 reports the results. The coefficient of Treated $\times$ Post $\times$ CyberRisk is negative but not statistically significant. These results suggest that the exogenous rise in dual ownership for treated firms does not attenuate the impact of cybersecurity risk exposure on stock returns.

Altogether, the M&A-based identification strategy offers compelling evidence that dual ownership causally reduces cyber exposure and moderates its impact on bond yield spreads, but more interestingly not on equity holders. These findings underscore the importance of investor structure in shaping how markets respond to emerging, non-traditional risk factors such as cybersecurity.

6 Conclusion

This paper provides novel evidence on how cybersecurity risk is priced in the corporate bond market and the role of institutional investor structure—particularly dual ownership—in shaping that pricing. While prior studies have primarily examined the effects of cybersecurity incidents on equity valuation or private loans, this study demonstrates that ex-ante cyber risk is economically meaningful in public debt markets. Specifically, I find that investors demand higher yield spreads when investing in bonds issued by cyber-vulnerable firms. Moreover, firms with greater cyber risk exposure tend to issue bonds with additional

covenants related to investment restrictions, dividend payouts, subsequent financing, and event risk. Cyberattacks result in significant declines in bond value, with the largest effects concentrated in high-yield bonds. Importantly, the magnitude of these impacts is moderated by the identity of the firm's investors—particularly dual holders who simultaneously hold both equity and debt.

The analysis demonstrates that dual ownership plays a critical governance role in mitigating the credit market consequences of cyber risk. Exploiting mergers of financial institutions as a quasi-experimental shock to dual ownership, I show that the emergence of dual holders reduces firm-level cyber risk exposure and lowers the yield spreads that bond markets assign to cyber vulnerability. Controlling for firm characteristics and fixed effects, the results indicate that bondholders price cyber risk less severely when the same institutions internalize incentives across the capital structure. The mechanisms through which cyber risk is mitigated—ex-ante bond design (via stronger covenant intensity) and investor alignment—highlight that cybersecurity is not just an operational or IT issue but a material financing concern.

These findings also carry important policy implications, particularly in light of the SEC's 2023 *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule*. Under the new rule, public companies are now required to disclose their cybersecurity risk management policies, board oversight structure, and material incidents within a four-day window. My findings suggest that bondholders have already been incorporating cybersecurity risks into pricing decisions even in the absence of mandated disclosures. This supports the SEC's initiative, while also suggesting that disclosure alone may not fully substitute for governance-based solutions such as dual ownership alignment. Taken together, this paper contributes to the literature on cybersecurity, credit markets, and institutional governance by demonstrating how emerging non-traditional risks are priced and managed in bond markets. The evidence underscores the growing relevance of cybersecurity in capital allocation,

and the need for regulatory frameworks and investor structures that are equipped to handle operational, reputational, and systemic risk.

References

Akey, P., Lewellen, S., Liskovich, I., Schiller, C., 2023. Hacking corporate reputations. Rotman School of Management Working Paper .

Al-Najjar, N. I., 1995. Incomplete contracts and the governance of complex contractual relationships. The American Economic Review 85, 432–436.

Andreadis, L., Kalotychou, E., Louca, C., Lundblad, C. T., Makridis, C., 2025. From bits to bonds: The economic ripple of local cyberattacks on municipalities. FEB-RN Research Paper .

Bai, J., Bali, T. G., Wen, Q., 2021. Is there a risk-return tradeoff in the corporate bond market? time-series and cross-sectional evidence. Journal of Financial Economics 142, 1017–1037.

Bessembinder, H., Kahle, K. M., Maxwell, W. F., Xu, D., 2008. Measuring abnormal bond performance. The Review of Financial Studies 22, 4219–4258.

Bharath, S. T., Shumway, T., 2008. Forecasting default with the merton distance to default model. The Review of Financial Studies 21, 1339–1369.

Bindal, S., Rossi, M., 2024. Bondholders on the brink: Navigating the threat of hedge fund activism. Available at SSRN 4939841 .

Bodnaruk, A., Rossi, M., 2016. Dual ownership, returns, and voting in mergers. Journal of Financial Economics 120, 58–80.

Chava, S., Kumar, P., Warga, A., 2010. Managerial agency and bond covenants. The Review of Financial Studies 23, 1120–1148.

Chava, S., Wang, R., Zou, H., 2019. Covenants, creditors' simultaneous equity holdings, and firm investment policies. Journal of Financial and Quantitative Analysis 54, 481–512.

Chen, T., Zhang, L., Zhu, Q., 2023. Dual ownership and risk-taking incentives in managerial compensation. Review of Finance 27, 1823–1857.

Crosignani, M., Macchiavelli, M., Silva, A. F., 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. Journal of Financial Economics 147, 432–448.

Dick-Nielsen, J., 2009. Liquidity biases in trace. The Journal of Fixed Income 19, 43.

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, 802–826.

Fama, E. F., MacBeth, J. D., 1973. Risk, return, and equilibrium: Empirical tests. Journal of political economy 81, 607–636.

Ferreira, M. A., Matos, P., 2012. Universal banks and corporate control: Evidence from the global syndicated loan market. The Review of Financial Studies 25, 2703–2744.

Florackis, C., Louca, C., Michaely, R., Weber, M., 2023. Cybersecurity risk. The Review of Financial Studies 36, 351–407.

Gilje, E. P., 2016. Do firms engage in risk-shifting? empirical evidence. The Review of Financial Studies 29, 2925–2954.

Gormley, T. A., Matsa, D. A., 2011. Growing out of trouble? corporate responses to liability risk. The Review of Financial Studies 24, 2781–2821.

Iyer, S. R., Simkins, B. J., Wang, H., 2020. Cyberattacks and impact on bond valuation. Finance Research Letters 33, 101215.

Jamilov, R., Rey, H., Tahoun, A., 2023. The anatomy of cyber risk. Tech. rep., National Bureau of Economic Research.

Jensen, M. C., Meckling, W. H., 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics 3, 305–360.

Jiang, H., Khanna, N., Yang, Q., Zhou, J., 2024. The cyber risk premium. Management Science 70, 8791–8817.

Jiang, W., Li, K., Shao, P., 2010. When shareholders are creditors: Effects of the simultaneous holding of equity and debt by non-commercial banking institutions. The Review of Financial Studies 23, 3595–3637.

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, 719–749.

Lewellen, K., Lowry, M., 2021. Does common ownership really increase firm coordination? Journal of Financial Economics 141, 322–344.

Merton, R. C., 1974. On the pricing of corporate debt: The risk structure of interest rates. The Journal of finance 29, 449–470.

Myers, S. C., 1977. Determinants of corporate borrowing. Journal of financial economics 5, 147–175.

Roll, R., 1984. A simple implicit measure of the effective bid-ask spread in an efficient market. The Journal of finance 39, 1127–1139.

SEC, 2011. CF Disclosure Guidance: Topic No. 2 – Cybersecurity. Division of Corporation Finance.

SEC, 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Release No. 33-10459.

SEC, 2023a. Cybersecurity Risk Management for Investment Advisers and Registered Investment Companies. Release No. IA-6240.

SEC, 2023b. Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Release No. 33-11216.

SEC, 2023c. Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information. Proposed Rule.

SEC, 2023d. Regulation Systems Compliance and Integrity (SCI). Proposed Amendments.

Sheneman, A., 2025. Cybersecurity risk and the cost of debt. Available at SSRN 3406217 .

Titman, S., Wessels, R., 1988. The determinants of capital structure choice. The Journal of finance 43, 1–19.

Whited, T. M., Wu, G., 2006. Financial constraints risk. The review of financial studies 19, 531–559.

Yang, H., 2021. Institutional dual holdings and risk-shifting: Evidence from corporate innovation. Journal of Corporate Finance 70, 102088.

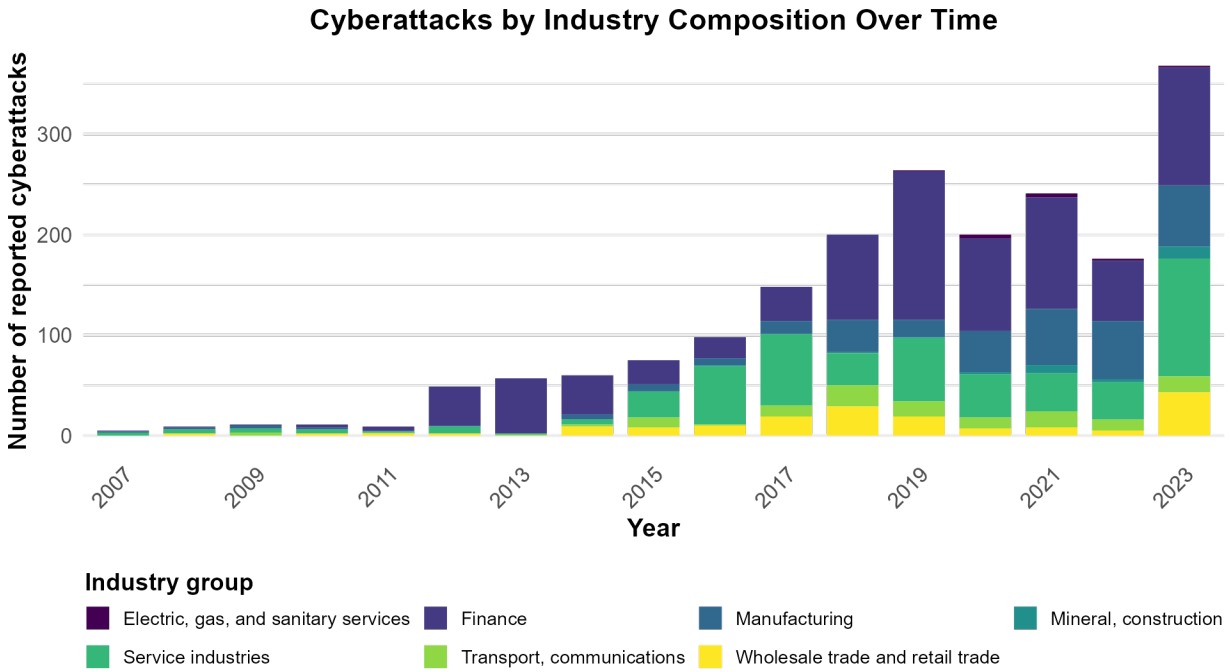


Figure 1: Annual distribution of reported cyberattacks by industry, 2007–2023. This figure shows the number of cyberattack incidents (from PRC) by industry composition over time.

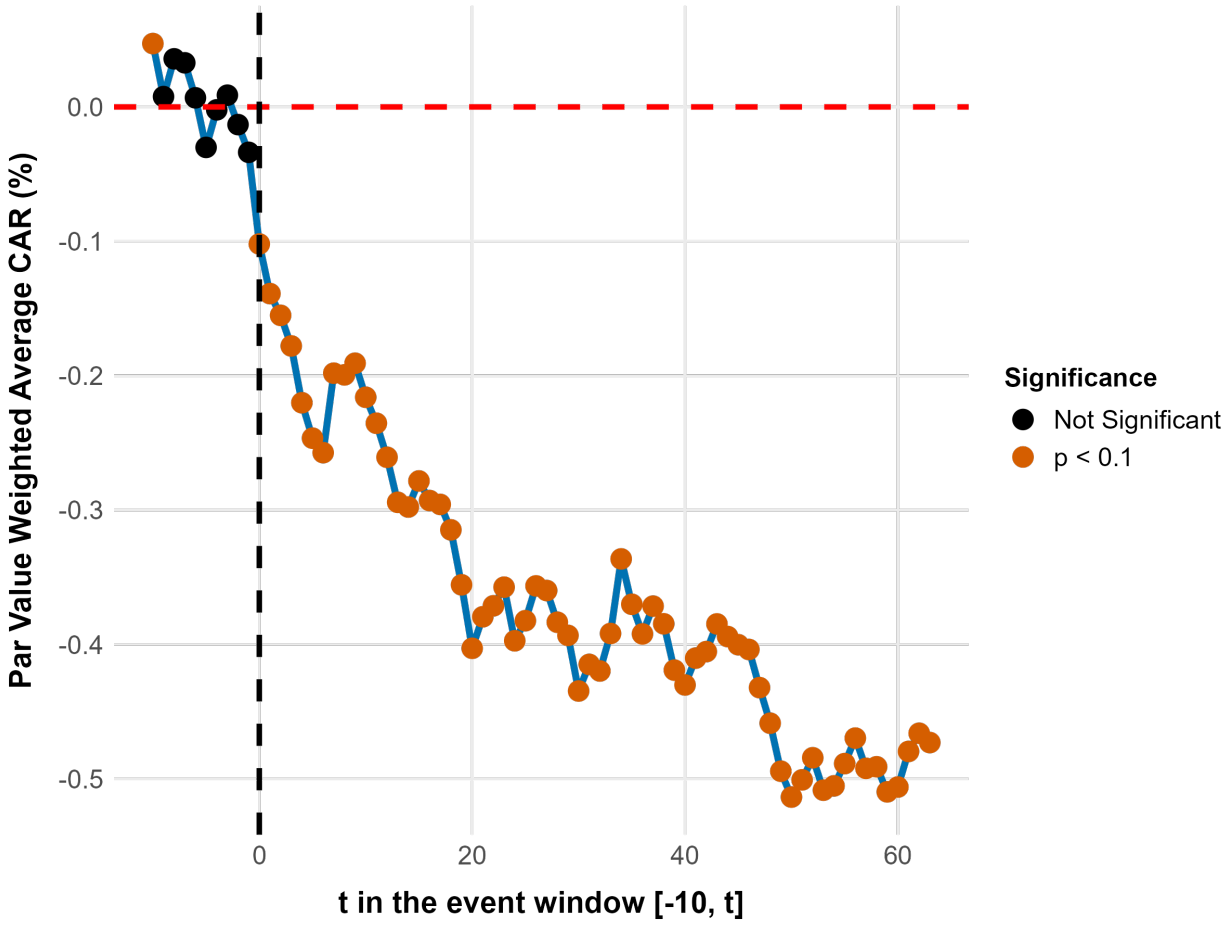


Figure 2.A: Cumulative abnormal bond returns (CARs) around the cyberattack breach dates.

This figure shows cumulative abnormal bond returns around cyberattack event windows. Abnormal bond returns (ABR) are calculated by subtracting the return of a benchmark portfolio matched on credit rating and maturity: $\text{ABR}_{t-1,t} = R_{t-1,t} - BM_{t-1,t}$. Benchmark portfolios are constructed using 24 groupings: six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Returns are weighted by outstanding par value to construct the benchmark portfolio return within each group. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings.

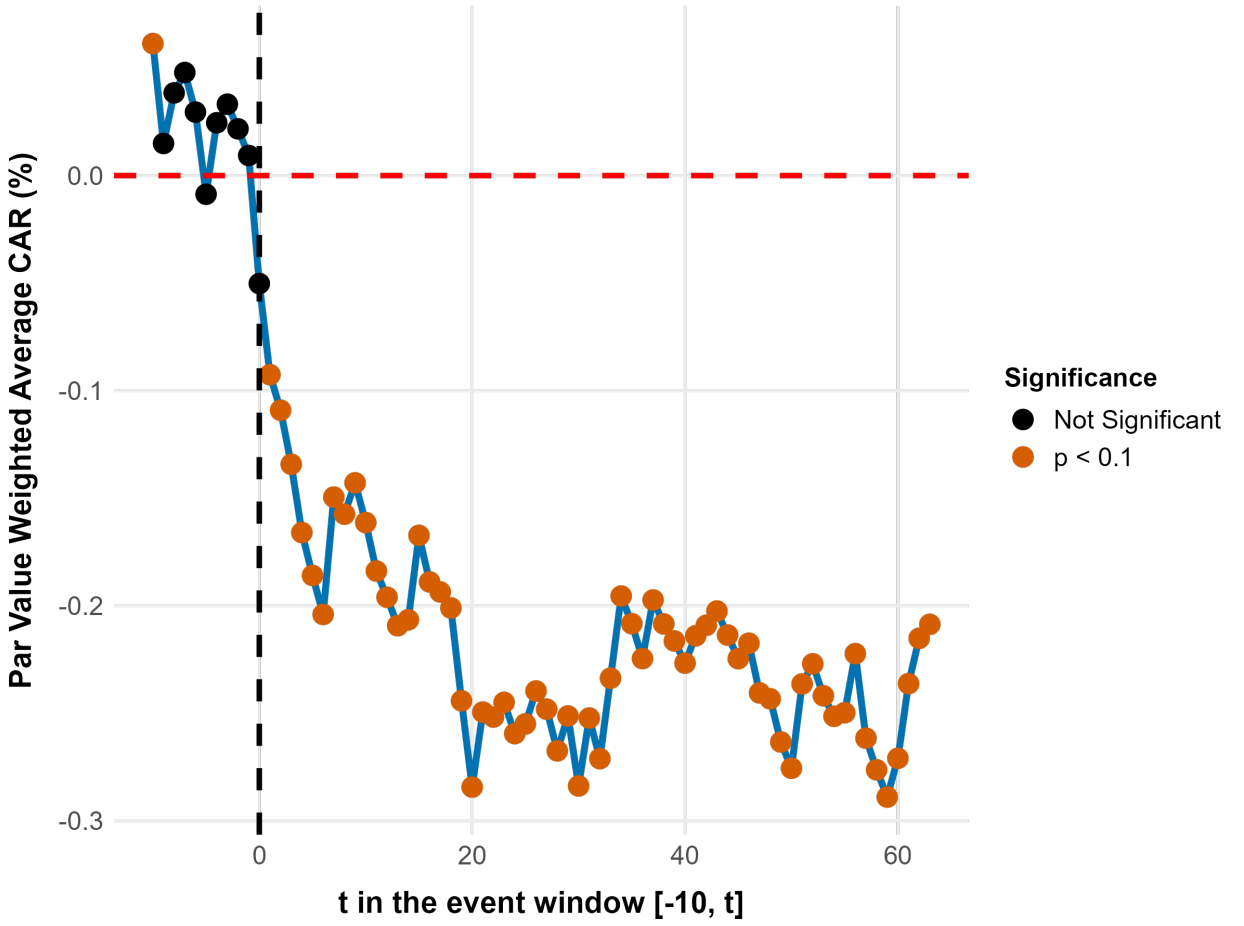


Figure 2.B: Cumulative abnormal bond returns (CARs) around the cyberattack breach dates for investment-grade bonds.
This figure shows cumulative abnormal bond returns around cyberattack event windows for investment-grade bonds. Abnormal bond returns (ABR) are calculated by subtracting the return of a benchmark portfolio matched on credit rating and maturity: $\text{ABR}_{t-1,t} = R_{t-1,t} - BM_{t-1,t}$. Benchmark portfolios are constructed using 24 groupings: six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Returns are weighted by outstanding par value to construct the benchmark portfolio return within each group. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings.

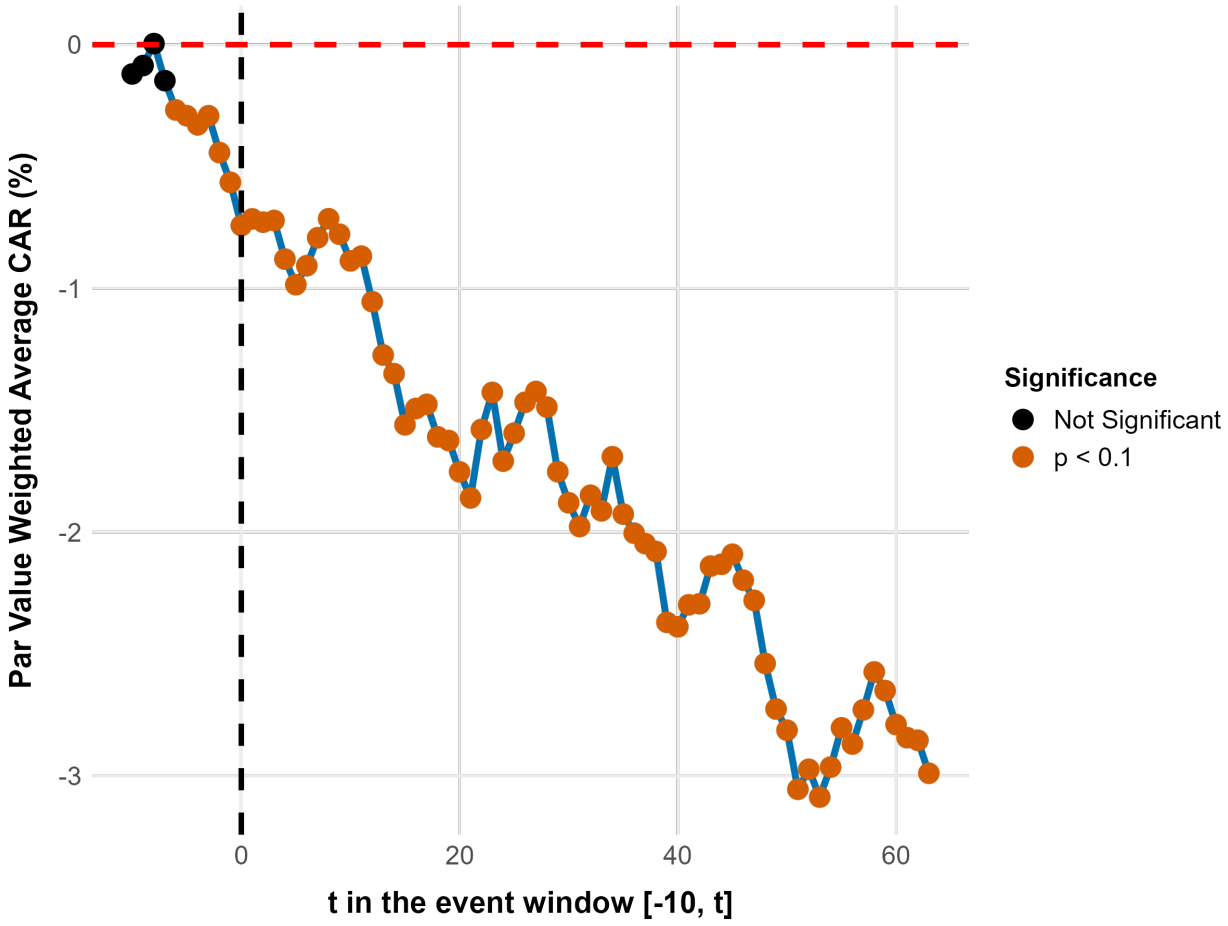


Figure 2.C: Cumulative abnormal bond returns (CARs) around the cyberattack breach dates for junk bonds.

This figure shows cumulative abnormal bond returns around cyberattack event windows for junk bonds. Abnormal bond returns (ABR) are calculated by subtracting the return of a benchmark portfolio matched on credit rating and maturity: $\text{ABR}_{t-1,t} = R_{t-1,t} - BM_{t-1,t}$. Benchmark portfolios are constructed using 24 groupings: six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Returns are weighted by outstanding par value to construct the benchmark portfolio return within each group. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings.

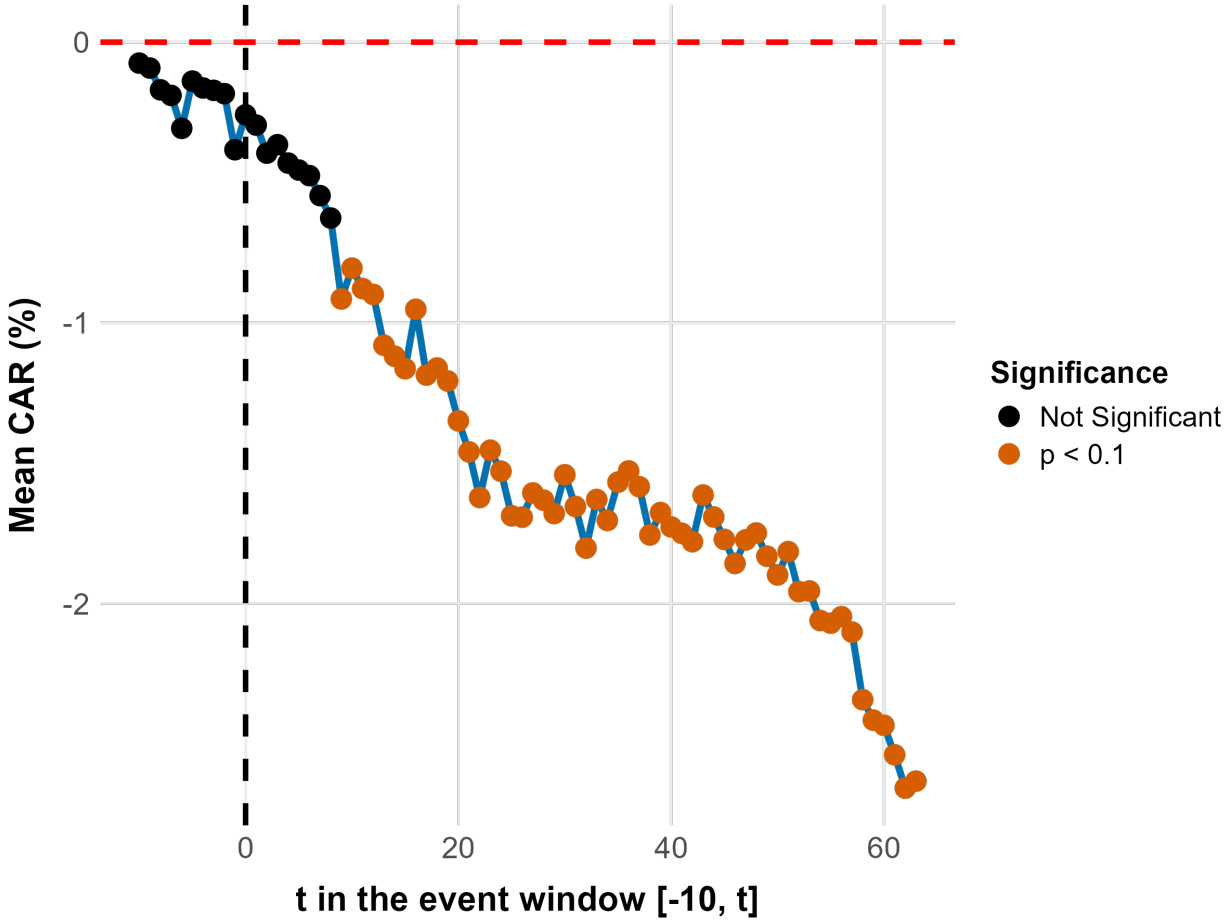


Figure 2.D: Cumulative stock abnormal returns (CARs) around the cyberattack breach dates.

This figure shows cumulative abnormal stock returns around cyberattack event windows. Abnormal stock returns (AR) are calculated by subtracting the market return: $\text{AR}_{t-1,t} = R_{t-1,t} - R^M_{t-1,t}$. Returns are weighted by market capitalization to construct the market return.

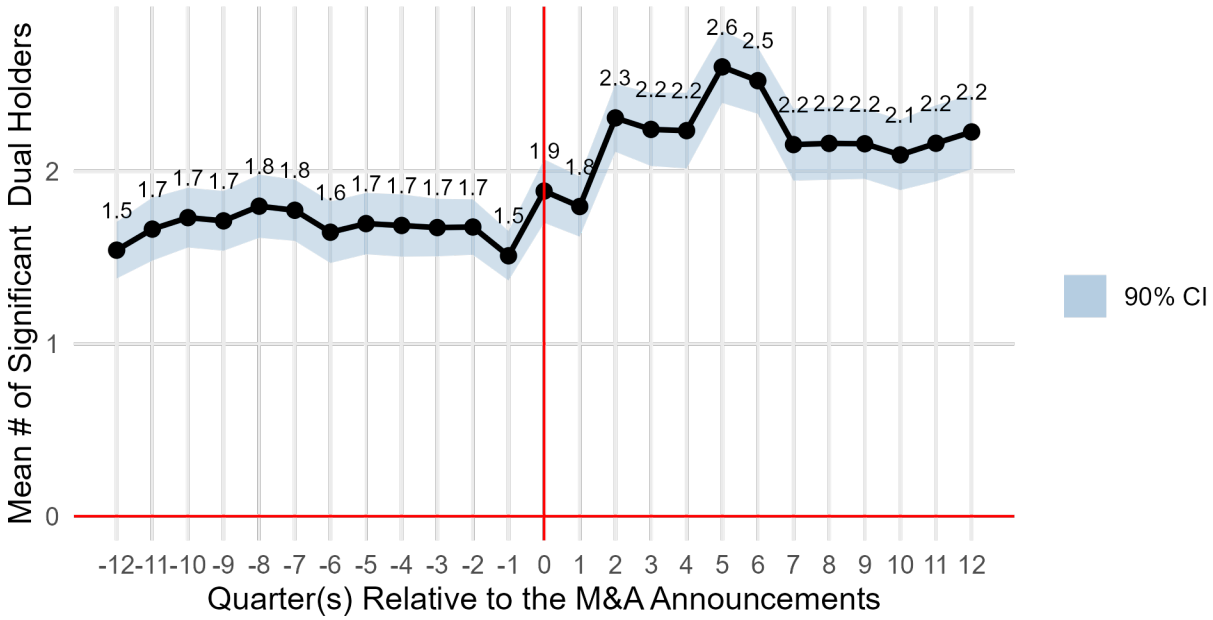


Figure 3: The impact of financial institution mergers on treated firms' significant dual ownership.
This figure shows the impact of financial institution mergers on the level of significant dual ownership for the treated firms. Treated firms are those that, prior to the merger announcement $(q-1)$, each merging financial institution held at least 1% of the firm's outstanding equity and 1% of its outstanding bonds but that neither party simultaneously held both positions. The shaded area represents 90% confidence intervals. A significant dual holder is defined as if a financial institution holds at least 1% equity and 1% bond on a firm.

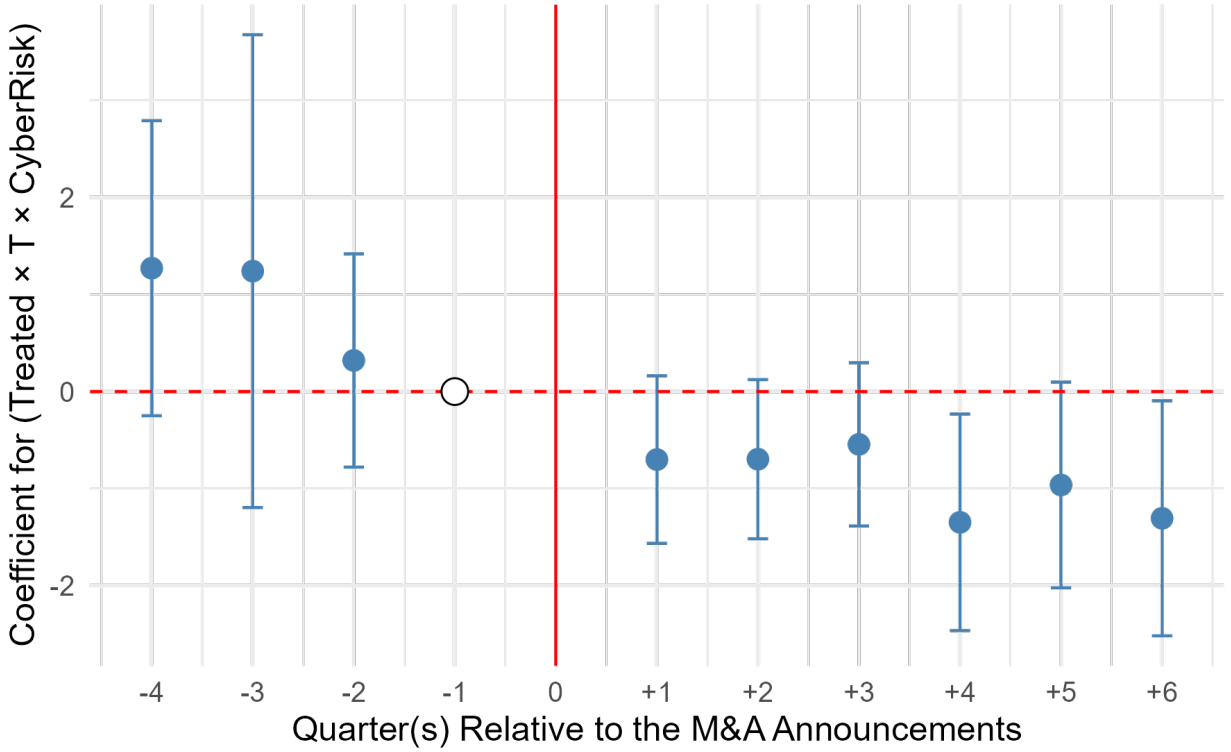


Figure 5: Dynamic treatment effects of financial company mergers on cyber risk exposure and yield spreads.
This figure plots the dynamic effects of financial institution mergers that generate new significant dual holders on firms' cybersecurity exposure and yield spreads. The estimated regression is:

$$\text{Yield Spread}_{i,q+1} = \beta_0 + \beta_1 \cdot \text{Treated}_{i,q} \cdot \text{Quarter}_{t+q} \cdot \text{CyberRisk}^R_{i,q'} + \beta_2 \cdot \text{Controls}_{i,q} + \eta_c + \eta_q + \epsilon_{i,q}$$

where $\text{Treated}_{i,q}$ is an indicator for bonds issued by firms where, in quarter $q-1$, each merging financial institution held at least 1% of the firm's outstanding equity and 1% of its outstanding bonds, but neither institution held both simultaneously. Quarter_{t+q} indicators range from $q = -4$ to $q = +6$, with the merger announcement quarter ($q = 0$) omitted from the regression and $q = -1$ used as the reference period. $\text{CyberRisk}^R_{i,q'}$ captures the pre-merger level of relative cyber risk exposure (CyberRisk^R), fixed at its value in quarter $q-1$ and held constant in subsequent periods. Control bonds are matched to treated bonds using propensity score matching (PSM) based on firm size, market-to-book ratio, return volatility, and time to maturity, requiring covariate similarity within one standard deviation. Matching is performed within investment-grade status, SIC2 industries, and calendar year-quarters. Additionally, I require that control firms have no significant dual holders—defined as institutions holding at least 1% of both the firm's equity and bonds—during the matching quarter. The specification includes industry and cohort-by-year-quarter fixed effects. Point estimates represent the triple interaction coefficients between treated, quarter, and $CyberRisk^R$. The vertical bars indicate 90% confidence intervals.

Table 1.A: Summary of statistics.
This table shows summary statistics for a sample of 260 firm-quarter observations that experience a cyberattack in the following quarter (170 distinct firms) and the remaining 190,925 firm-quarter observations (6,965 distinct firms) that do not experience a cyberattack covered in Compustat over the period 2004 to 2021(September). The appendix provides detailed descriptions of the construction of the variables. ***, **, and * denote that t -tests (Wilcoxon z -tests) for mean (median) differences in firm and industry characteristics between attacked and nonattacked firms are significant at the 1%, 5%, and 10% levels, respectively.

	Firm-quarter followed by: cyberattack (N=260 with 170 firms): A			**Firm-quarter without: cyberattack (N=190,925 with 6,965 firms) : B**			**Test of difference: (A-B)**	
Variable	Mean	Median	SD	Mean	Median	SD	Mean	Median
Total Assets ($B)	15.25	4.00	34.68	5.56	0.67	18.02	9.69***	3.33***
Equity Return	0.21	0.22	0.41	0.21	0.17	0.57	-0.00	0.05
Return Volatility	0.42	0.36	0.21	0.50	0.43	0.27	-0.08***	-0.07***
Market Cap ($B)	17.59	4.77	28.25	5.43	0.72	15.58	12.16***	4.06***
Z Score	0.64	0.79	1.10	-0.10	0.59	3.11	0.74***	0.20***
EDF	0.03	0.00	0.13	0.03	0.00	0.13	-0.00*	0.00*
Firm Age (Years)	24.84	21.96	17.82	19.45	14.59	17.08	5.40***	7.38***
Tobin's Q	2.72	1.83	2.38	2.11	1.58	1.60	0.60***	0.25***
Leverage	0.32	0.30	0.21	0.22	0.19	0.20	0.10***	0.11***
ROA	0.01	0.01	0.03	-0.00	0.01	0.06	0.01	-0.00
EBITDA/TA	0.02	0.03	0.03	0.02	0.03	0.05	0.01	-0.00
R&D/TA	0.01	0.00	0.02	0.01	0.00	0.03	-0.00	0.00
Cash Flow/TA	0.02	0.02	0.03	0.01	0.02	0.06	0.01	0.00
Net Worth/TA	0.39	0.39	0.21	0.50	0.50	0.24	-0.11***	-0.11***
Intangible/TA	0.31	0.30	0.21	0.19	0.11	0.21	0.12***	0.19***
Operational Cost/TA	0.21	0.16	0.16	0.23	0.18	0.18	-0.02**	-0.03**
Turn Over Ratio	0.23	0.18	0.17	0.25	0.20	0.19	-0.01	-0.02
Firm Liquidity	0.18	0.13	0.17	0.21	0.12	0.23	-0.03	0.01
Capex/TA	0.67	0.69	0.16	0.69	0.72	0.16	-0.02***	-0.03***
BTM	0.41	0.32	0.43	0.55	0.43	0.51	-0.14***	-0.11***
PPE/TA	0.21	0.14	0.19	0.26	0.17	0.24	-0.05*	-0.03*
Sales Growth	0.03	0.01	0.32	0.06	0.02	0.32	-0.03*	-0.02*
Industry Sales Growth	0.06	0.05	0.11	0.06	0.06	0.08	0.00	-0.00
WW Index	-0.35	-0.35	0.08	-0.29	-0.28	0.10	-0.07***	-0.07***
Institutional Ownership	0.78	0.86	0.23	0.62	0.71	0.33	0.16***	0.15***

Table 1.B: Summary of statistics.
This table shows summary statistics for the cybersecurity risk exposure variables between a sample of 245 firm-quarter observations that experience a cyberattack in the following quarter (159 distinct firms) and the remaining 141,776 firm-quarter observations (5,248 distinct firms) that do not experience a cyberattack covered in Compustat over the period 2004 to 2021(September). The appendix provides detailed descriptions of the construction of the variables. ***, **, and * denote that t -tests (Wilcoxon z -tests) for mean (median) differences in firm and industry characteristics between attacked and nonattacked firms are significant at the 1%, 5%, and 10% levels, respectively.

	Firm-quarter followed by: cyberattack (N=245 with 159 firms): A			**Firm-quarter without: cyberattack (N=141,776 with 5,248 firms) : B**			**Test of difference: (A-B)**	
Variable	Mean	Median	SD	Mean	Median	SD	Mean	Median
$CyberRisk^A$	2.24	1.00	4.15	1.44	0.00	3.30	0.81***	1.00***
$CyberRisk^R$	0.49	0.21	0.83	0.41	0.00	1.00	0.08***	0.21***

Table 1.C: Summary of statistics.
This table shows summary statistics for the dual ownership variables between a sample of 127 firm-quarter observations that experience a cyberattack in the following quarter (86 distinct firms) and the remaining 57,090 firm-quarter observations (2,118 distinct firms) that do not experience a cyberattack covered in Compustat over the period 2004 to 2021(September). The appendix provides detailed descriptions of the construction of the variables. ***, **, and * denote that t -tests (Wilcoxon z -tests) for mean (median) differences in firm and industry characteristics between attacked and nonattacked firms are significant at the 1%, 5%, and 10% levels, respectively.

	Firm-quarter followed by: cyberattack (N=127 with 86 firms): A			**Firm-quarter without: cyberattack (N=57,090 with 2,118 firms) : B**			**Test of difference: (A-B)**	
Variable	Mean	Median	SD	Mean	Median	SD	Mean	Median
DEO	0.28	0.29	0.17	0.20	0.17	0.17	0.08***	0.12***
DEO^{inst}	0.35	0.35	0.20	0.26	0.24	0.21	0.08***	0.11***
DEO^{cond}	0.09	0.06	0.09	0.08	0.04	0.09	0.01**	0.02**

Table 1.D: Summary of statistics.
This table shows summary statistics for 6,312,710 daily bond transactions across 15,909 unique bonds issued by 1,659 unique firms over the period 2004 to 2021 (September). Price (Yield to maturity) is calculated as the volume-weighted average of intraday transactions for each bond. Yield spreads are computed as the difference between the yield and maturity-matched treasury securities. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings, where 1 corresponds to AAA and 21 corresponds to C; higher numerical scores indicate greater credit risk. Covenants is a count variable that includes 8 bondholder protective covenants and 18 issuer restrictive covenants. Collateral is a dummy variable indicating whether there is collateral pledged for the underlying security. The appendix provides detailed descriptions of the construction of the variables

Variable	Mean	Median	SD	Min	Max	Q1	Q3
Price (% of Par)	104.75	103.57	10.69	50.00	142.69	99.90	109.15
Yield to Maturity (%)	4.01	3.64	2.79	0.29	27.88	2.30	5.15
Yield Spread (%)	1.94	1.24	2.42	0.04	24.34	0.68	2.28
Rating	8.25	8.00	3.30	1.00	21.00	6.00	10.00
Maturity (Years)	8.84	5.73	8.85	0.50	99.51	3.06	9.09
Offering Amount ($M)	964.10	750.00	810.75	100.00	15000.00	500.00	1250.00
Daily Trading Volume ($M)	4.78	1.32	21.00	0.10	10090.23	0.43	4.51
Coupon (%)	4.98	4.95	1.90	0.12	15.00	3.55	6.25
Covenant Intensity	4.46	4.00	2.76	0.00	14.00	3.00	6.00
Collateral Indicator	0.21	0.00	0.41	0.00	1.00	0.00	0.00

Table 2.A: The effect of ex-ante cyber risk exposure on quarterly bonds yield spreads.
This table shows the results of regressing the end of quarter bond yield spread on cyber risk exposure and control variables over the period 2004 to September 2021 (Equation 1):

$$\text{YieldSprea}_{i,t} = \beta_0 + \beta_1 \cdot \text{CyberRisk}_{i,t} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

The appendix provides detailed descriptions of the construction of the variables. Clustered standard errors at the quarter and firm level are reported in parentheses. *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: Yield Spread$_t$		**Dependent Variable: Yield Spread$_{t+1}$**	
	(1)	(2)	(3)	(4)
$\log(1 + CyberRisk^A)$	0.055***		0.054**	
	(0.018)		(0.020)	
$CyberRisk^R$		0.061***		0.057***
		(0.018)		(0.020)
Rating	0.229***	0.229***	0.224***	0.224***
	(0.020)	(0.020)	(0.018)	(0.018)
Maturity (Years)	0.028***	0.028***	0.029***	0.029***
	(0.002)	(0.002)	(0.002)	(0.002)
Coupon	0.120***	0.120***	0.122***	0.122***
	(0.011)	(0.011)	(0.011)	(0.011)
log(Offering Amount)	−0.079***	−0.079***	−0.080***	−0.080***
	(0.026)	(0.026)	(0.027)	(0.027)
log(Total Assets)	−0.061**	−0.058**	−0.075***	−0.072***
	(0.026)	(0.026)	(0.026)	(0.026)
Leverage	1.667***	1.663***	1.854***	1.851***
	(0.161)	(0.162)	(0.193)	(0.194)
log(Firm Age)	0.086***	0.087***	0.065**	0.066**
	(0.025)	(0.025)	(0.028)	(0.028)
Return Volatility	4.167***	4.171***	3.511***	3.515***
	(0.450)	(0.451)	(0.486)	(0.487)
ROA	−7.235***	−7.220***	−8.586***	−8.572***
	(1.045)	(1.046)	(1.206)	(1.208)
BTM	0.688***	0.686***	0.753***	0.752***
	(0.084)	(0.084)	(0.099)	(0.099)
Firm Liquidity	0.624**	0.632**	0.589**	0.597**
	(0.287)	(0.285)	(0.286)	(0.285)
Industry Fixed Effects	Y	Y	Y	Y
Year-Quarter Fixed Effects	Y	Y	Y	Y
Observations	213,496	213,496	213,496	213,496
Adjusted R^2	0.647	0.647	0.591	0.591

Table 2.B: Cybersecurity risk and collateral or covenants requirements in the primary bond market.
This table shows the results of regressing covenant intensity (collateral) on cyber risk exposure and control variables over 2004 to September 2021 (Equation 2):

$$\mathrm{Y}_{i,t+1} = \beta_0 + \beta_1 \cdot \mathrm{CyberRisk}_{i,t} + \beta_2 \cdot \mathrm{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where the dependent variable $Y_{i,t+1}$ represents either (i) the number of covenants in a newly issued bond (including 8 bondholder-protective covenants and 18 issuer-restrictive covenants), or (ii) a binary indicator equal to one if collateral is pledged for the underlying security, and zero otherwise. Columns (1)–(2) employ a Poisson regression model, while Columns (3)–(4) use a logit regression model. The appendix provides detailed descriptions of the variable constructions. Heteroscedasticity-robust and clustered standard errors at the firm and quarter levels are reported in parentheses. *p<0.10; **p<0.05; ***p<0.01.

	Dependent Variable: Covenant Intensity$_{t+1}$		**Dependent Variable: Collateral$_{t+1}$**	
	(1)	(2)	(3)	(4)
log(1 + $CyberRisk^A$)	0.021***		0.105	
	(0.007)		(0.115)	
$CyberRisk^R$		0.018**		0.081
		(0.008)		(0.008)
Rating	0.056***	0.053***	−0.492***	−0.493***
	(0.004)	(0.004)	(0.059)	(0.059)
Maturity (Years)	0.026**	0.026**	0.038	0.034
	(0.012)	(0.011)	(0.150)	(0.150)
Coupon	−0.031***	−0.033***	0.525***	0.528***
	(0.009)	(0.008)	(0.119)	(0.120)
log(Offering Amount)	0.040***	0.040***	−1.061***	−1.065***
	(0.013)	(0.013)	(0.169)	(0.170)
log(Total Assets)	−0.071***	−0.070***	0.309***	0.316***
	(0.007)	(0.007)	(0.097)	(0.097)
Leverage	−0.217***	−0.216***	4.930***	4.899***
	(0.049)	(0.049)	(0.910)	(0.917)
log(Firm Age)	−0.005	−0.007	0.175	0.175
	(0.008)	(0.008)	(0.111)	(0.112)
Return Volatility	−0.243***	−0.180**	3.143***	3.116***
	(0.078)	(0.072)	(0.915)	(0.923)
ROA	0.853**	0.886**	−11.974***	−11.957***
	(0.339)	(0.353)	(3.450)	(3.451)
BTM	−0.084***	−0.078***	0.352	0.343
	(0.023)	(0.023)	(0.296)	(0.298)
Firm Liquidity	−0.110**	−0.120**	−2.967*	−2.949*
	(0.054)	(0.055)	(1.703)	(1.703)
Industry Fixed Effects	Y	Y	Y	Y
Year-Quarter Fixed Effects	Y	Y	Y	Y
Observations	7,610	7,610	7,610	7,610
Pseudo R^2	0.292	0.271	0.485	0.485

Table 3.A: Cyber risk and dual ownership

This table presents the results of regressing the ex-ante cyber risk measure on dual ownership and control variables over the period 2004 to September 2021:

$$\mathrm{Y}_{i,t+1} = \beta_0 + \beta_1 \cdot \mathrm{DO}_{i,t} + \beta_2 \cdot \mathrm{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where the dependent variable $Y_{i,t+1}$ represents the measure of cyber risk. The variable $DO_{i,t+1}$ represents each measure of dual ownership: *DEO* (dual equity ownership), DEO^{inst} (dual ownership scaled by institutional ownership), and DEO^{cond} (conservative dual ownership threshold). Models (1)–(3) estimate a Tweedie regression (a type of GLM), where the dependent variable corresponds to the ratio of the relative frequency of cybersecurity-related keywords, $\mathrm{CyberRisk}^R_{t+1}$. The appendix provides detailed descriptions of the variable constructions. Heteroscedasticity-robust and clustered standard errors at the firm and quarter levels are reported in parentheses. *p<0.10; **p<0.05; ***p<0.01.

Dependent Variable:	**CyberRisk$^R_{t+1}$**		
	(1)	(2)	(3)
DEO_t	-0.135^*		
	(0.071)		
DEO^{inst}_t		-0.106^*	
		(0.060)	
DEO^{cond}_t			-0.240^{**}
			(0.119)
Firm Controls	Y	Y	Y
Industry FEs	Y	Y	Y
Year-Quarter FEs	Y	Y	Y
Observations	54,823	54,823	54,823
Pseudo R^2	0.169	0.169	0.169

Table 3.B: Cyber risk and dual ownership interacting with high EDF indicator
This table presents the results of regressing the ex-ante cyber risk measure on dual ownership, interacted with a high expected default frequency (EDF) indicator, along with control variables, over the period 2004 to September 2021.

$$\mathrm{Y}_{i,t+1} = \beta_0 + \beta_1 \cdot \mathrm{DO}_{i,t} \cdot \text{High EDF}_{i,t} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where the dependent variable $Y_{i,t+1}$ represents the measure of cyber risk. The variable $DO_{i,t+1}$ represents each measure of dual ownership: DEO (dual equity ownership), DEO^{inst} (dual ownership scaled by institutional ownership), and DEO^{cond} (conservative dual ownership threshold). Firms classified as having a high EDF are those with EDF values above the quarterly median across all firms. Models (1)–(3) estimate a Tweedie regression (a type of GLM), where the dependent variable corresponds to the ratio of the relative frequency of cybersecurity-related keywords, CyberRisk^R_{t+1}. The appendix provides detailed descriptions of the variable constructions. Heteroscedasticity-robust and clustered standard errors at the firm and quarter levels are reported in parentheses. *p<0.10; **p<0.05; ***p<0.01.

Dependent Variable:	**CyberRisk$^R_{t+1}$**		
	(1)	(2)	(3)
$\text{DEO}_t \times High_EDF_t$	−0.397***		
	(0.100)		
$\text{DEO}^{inst}_t \times High_EDF_t$		−0.388***	
		(0.078)	
$\text{DEO}^{cond}_t \times High_EDF_t$			−0.451**
			(0.185)
DEO_t	0.074		
	(0.089)		
DEO^{inst}_t		0.100	
		(0.073)	
DEO^{cond}_t			0.027
			(0.170)
High_EDF_t	0.178***	0.196***	0.131***
	(0.034)	(0.034)	(0.029)
Firm Controls	Y	Y	Y
Industry FEs	Y	Y	Y
Year-Quarter FEs	Y	Y	Y
Observations	54,823	54,823	54,823
Pseudo R^2	0.170	0.170	0.170

Table 4: Distribution of M&A events and treated firms

This table reports mergers and acquisitions (M&As) among financial institutions that create new significant dual holders, thereby increasing the number of treated firms in the sample. A significant dual holder is defined as if a financial institution holds at least 1% equity and 1% bond on a firm. Treated firms are those that, prior to the merger announcement $(q-1)$, each merging financial institution held at least 1% of the firm's outstanding equity and 1% of its outstanding bonds but that neither party simultaneously held both positions. Column (5) reports the number of treated firms associated with each merger, and Column (6) reports the number of bonds issued by each treated firm.

Announcement Date	Completion Date	Acquirer	Target	# of Treated Firms	# of Treated Bonds
02/15/2006	09/29/2006	BlackRock	Merrill Lynch Investment Managers	42	196
10/10/2005	04/03/2006	Lincoln National	Jefferson-Pilot	0	0
07/24/2006	12/31/2006	Principal Financial Group	WM Advisors	0	0
02/01/2007	08/03/2007	Great-West Lifeco Inc	Putnam Investments	17	30
03/16/2008	05/30/2008	JPMorgan Chase	Bear Stearns	3	0
06/11/2009	12/01/2009	BlackRock	Barclays Global Investors	140	396
09/30/2009	05/30/2010	Ameriprise Financial	Columbia Management Group	0	0
07/29/2010	12/31/2010	Nuveen Investments	FAF Advisors	0	0
04/18/2012	06/29/2012	Affiliated Managers Group	Yacktman Asset Management	0	0
04/14/2014	10/01/2014	TIAA-CREF	Nuveen Investments	0	0
02/16/2010	02/16/2010	Guggenheim	Security Benefit	0	0
10/16/2012	10/16/2012	Natixis	McDonnell Investment Management	0	0
10/06/2008	05/12/2009	BNP Paribas	Fortis Banque France	2	14
09/15/2008	01/01/2009	Bank of America	Merrill Lynch & Co.	1	0
04/02/2010	04/06/2010	Goldman Sachs Group Inc.	Level Global Investors LP	0	0
04/23/2008	09/30/2008	Lehman Brothers Holdings Inc	David J Greene & Co LLC	1	0
10/31/2006	12/4/2006	Morgan Stanley	FrontPoint Partners LLC	0	0
10/03/2008	12/31/2008	Wells Fargo & Co	Wachovia Corp, Charlotte, NC	4	0
			Total	**210**	**636**

Table 5: Diff-in-diff regression of cyber risk exposure and dual ownership.
This table shows the results from difference-in-differences regressions around the mergers of financial conglomerates, which increase the number of significant dual holders for treated firms. The estimated Tweedie model (Equation 3) is:

$$\text{CyberRisk}^{R}_{i,t+1} = \beta_0 + \beta_1 \cdot \text{Treated}_{i,t} \cdot \text{Post}_{i,t} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where $\text{Treated}_{i,t}$ is an indicator for firms in which, one quarter prior to the merger announcement $(t-1)$, each merging financial institution held at least 1% of the firm's equity and 1% of its outstanding bonds—but neither institution held both positions. $\text{Post}_{i,t}$ includes quarters $t+1$ through $t+6$, while the pre-treatment period includes $t-4$ through $t-1$. The merger announcement quarter $(t=0)$ is excluded from the regression. Control firms are matched to treated firms using propensity score matching (PSM) based on firm size, market-to-book ratio, and return volatility, requiring covariate similarity within one standard deviation. Matching is performed within SIC2 industries and calendar year-quarters. Additionally, I require that control firms have no significant dual holders—defined as institutions holding at least 1% of both the firm's equity and bonds—during the matching quarter. The appendix provides detailed descriptions of the construction of the variables. Heteroscedastic robust and clustered standard errors at the cohort-year-quarter level are reported in parentheses *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: $\textbf{CyberRisk}^{R}_{t+1}$
	(1)
Treated	−0.100
	(0.138)
Post	−1.039
	(2.452)
Treated × Post	−0.311*
	(0.170)
Firms Controls	Y
Industry Fixed Effects	Y
Cohort-Year-Quarter Fixed Effects	Y
Observations	1,566
Number of Treated Firms	88
Number of Control Firms	88
Pseudo R^2	0.399

Table 6: Diff-in-diff regression of yield spread on dual ownership and cyber risk exposure.

This table shows the results from triple difference-in-differences regressions of yield spread on cyber risk exposure around the mergers of financial conglomerates, which increase the number of significant dual holders for treated firms. The estimated regression model (Equation 4) is:

$$\text{Yield Spread}_{i,t+1} = \beta_0 + \beta_1 \cdot \text{Treated}_{i,t} \cdot \text{Post}_{i,t} \cdot \text{CyberRisk}^R_{i,t'} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where $\text{Treated}_{i,t}$ is an indicator for firms in which, one quarter prior to the merger announcement $(t-1)$, each merging financial institution held at least 1% of the firm's equity and 1% of its outstanding bonds—but neither institution held both positions. $\text{Post}_{i,t}$ includes quarters $t+1$ through $t+6$, while the pre-treatment period includes $t-4$ through $t-1$. The merger announcement quarter $(t=0)$ is excluded from the regression. $\text{CyberRisk}^R_{i,t'}$ captures the pre-merger level of relative cyber risk exposure (CyberRisk^R), fixed at its value in quarter $t-1$ and held constant in subsequent periods. Control bonds are matched to treated bonds using propensity score matching (PSM) based on firm size, market-to-book ratio, return volatility, and time to maturity, requiring covariate similarity within one standard deviation. Matching is performed within investment-grade status, SIC2 industries, and calendar year-quarters. Additionally, I require that control firms have no significant dual holders—defined as institutions holding at least 1% of both the firm's equity and bonds—during the matching quarter. The appendix provides detailed descriptions of the construction of the variables. Clustered standard errors at the quarter and firm level are reported in parentheses. *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: Yield Spread$_{t+1}$	
	(1)	(2)
Treated	0.081	−0.088
	(0.249)	(0.258)
Post	2.456	2.327
	(2.690)	(2.680)
Treated × Post	−0.194	0.135
	(0.259)	(0.259)
CyberRisk^R		0.011
		(0.194)
Treated × CyberRisk^R		0.668
		(0.549)
Post × CyberRisk^R		0.420
		(0.277)
Treated × Post × CyberRisk^R		−1.293*
		(0.766)
Bond Controls	Y	Y
Firms Controls	Y	Y
Industry Fixed Effects	Y	Y
Cohort-Year-Quarter Fixed Effects	Y	Y
Observations	7,578	7,578
Number of Treated Firms	73	73
Number of Treated Bonds	344	344
Number of Control Firms	154	154
Number of Control Bonds	587	587
Adjusted R^2	0.702	0.705

Table 7: Diff-in-diff regression of stock return on dual ownership and cyber risk exposure.

This table shows the results from triple difference-in-differences regressions of stock return on cyber risk exposure around the mergers of financial conglomerates, which increase the number of significant dual holders for treated firms. The estimated regression model (Equation 4) is:

$$\mathrm{R}_{i,t+1} = \beta_0 + \beta_1 \cdot \mathrm{Treated}_{i,t} \cdot \mathrm{Post}_{i,t} \cdot \mathrm{CyberRisk}^{R}_{i,t'} + \beta_2 \cdot \mathrm{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where $\mathrm{Treated}_{i,t}$ is an indicator for firms in which, one quarter prior to the merger announcement ($t-1$), each merging financial institution held at least 1% of the firm's equity and 1% of its outstanding bonds—but neither institution held both positions. $\mathrm{Post}_{i,t}$ includes quarters $t+1$ through $t+6$, while the pre-treatment period includes $t-4$ through $t-1$. The merger announcement quarter ($t=0$) is excluded from the regression. $\mathrm{CyberRisk}^{R}_{i,t'}$ captures the pre-merger level of relative cyber risk exposure ($\mathrm{CyberRisk}^{R}$), fixed at its value in quarter $t-1$ and held constant in subsequent periods. Control firms are matched to treated firms using propensity score matching (PSM) based on firm size, market-to-book ratio, and return volatility, requiring covariate similarity within one standard deviation. Matching is performed within SIC2 industries and calendar year-quarters. Additionally, I require that control firms have no significant dual holders—defined as institutions holding at least 1% of both the firm's equity and bonds—during the matching quarter. The appendix provides detailed descriptions of the construction of the variables. Heteroscedastic robust and clustered standard errors at the cohort-year-quarter level are reported in parentheses *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: $\mathbf{R}_{t+1}$	
	(1)	(2)
Treated	0.006	0.007
	(0.010)	(0.011)
Post	−0.040	−0.037
	(0.081)	(0.083)
Treated × Post	−0.004	0.003
	(0.014)	(0.015)
$\mathrm{CyberRisk}^{R}$		−0.009
		(0.009)
Treated × $\mathrm{CyberRisk}^{R}$		−0.004
		(0.017)
Post × $\mathrm{CyberRisk}^{R}$		0.018
		(0.016)
Treated × Post × $\mathrm{CyberRisk}^{R}$		−0.021
		(0.022)
Firms Controls	Y	Y
Industry Fixed Effects	Y	Y
Cohort-Year-Quarter Fixed Effects	Y	Y
Observations	3,569	3,569
Number of Treated Firms	134	134
Number of Control Firms	248	248
Adjusted R^2	0.392	0.392

IA Appendix

IA1 Variable Definitions

- **Asset Intangibility:** $1 - \texttt{ppentq}/\texttt{atq}$, where `ppentq` is total property, plant, and equipment, and `atq` is total assets.
- **CAPX / Assets:** Capital expenditures (`capxq`) divided by total assets (`atq`).
- **Cash Flow / Assets:** $[\texttt{ibq} + \texttt{dpq}]/\texttt{atq}$, where `ibq` is income before extraordinary items and `dpq` is depreciation and amortization. Observations with values greater than 1 or less than –1 are dropped.
- **Cyberattack (Indicator):** Equals 1 if a firm experiences hacking, malware, spyware, or similar cyber events in a given quarter, and 0 otherwise.
- **Durable Goods Industries (Indicator):** Equals 1 for firms with SIC codes between 3400 and 3999, and 0 otherwise (Titman and Wessels, 1988).
- **Financial Constraint (Indicator):** Equals 1 if a firm's Whited–Wu index (Whited and Wu, 2006) is in the top tercile in a given quarter.
- **Financial Industry (Indicator):** Equals 1 for firms with SIC codes between 6000 and 6999, and 0 otherwise.
- **Financial Information Loss (Indicator):** Equals 1 if a cyberattack results in the loss of sensitive financial information (e.g., SSNs, credit card data), and 0 otherwise.
- **Firm Size:** Natural logarithm of total assets (`atq`).
- **Firm Age:** Natural logarithm of the number of years a firm appears in CRSP.
- **Leverage:** $[\texttt{dlttq} + \texttt{dlcq}]/\texttt{atq}$, where `dlttq` is long-term debt and `dlcq` is current liabilities. Observations with values greater than 1 are dropped.
- **Liquidity:** Cash and short-term investments (`cheq`) divided by total assets (`atq`).
- **Intangibles / Assets:** Intangible assets (`intanq`) divided by total assets (`atq`). Observations with values greater than 1 are dropped.

- **Net Worth:** Stockholders' equity (`seqq`) divided by total assets (`atq`).
- **R&D / Assets:** $\max(0, \texttt{xrdq})/\texttt{atq}$, where `xrdq` is R&D expenditure.
- **Repeated Cyberattacks Within One Year (Indicator):** Equals 1 if a firm experiences multiple cyberattacks within a one-year window, and 0 otherwise.
- **Retail Industry (Indicator):** Equals 1 for firms with SIC codes between 5200 and 5999, and 0 otherwise.
- **ROA (Return on Assets):** Net income (`niq`) divided by total assets (`atq`).
- **Sales Growth:** $\texttt{saleq}_t/\texttt{saleq}_{t-1}$. Observations with $\texttt{saleq}_t < 0$ are dropped.
- **Tobin's Q:** $[\texttt{atq} - \texttt{ceqq} + (\texttt{prccq} \times \texttt{cshoq})]/\texttt{atq}$, where `ceqq` is common equity, `prccq` is share price, and `cshoq` is shares outstanding. Observations with $\texttt{prccq} \leq 1$ or > 1000, and with Tobin's Q > 1000, are dropped.
- **Expected Default Frequency (EDF):** Computed based on the Merton distance-to-default framework (Merton, 1974), following Bharath and Shumway (2008):

$$\text{EDF} = \Phi(-\text{DD}) \tag{5}$$

$$\text{DD} = \frac{\ln\left(\frac{V_A}{D}\right) + \left(\mu - \frac{1}{2}\sigma_V^2\right) T}{\sigma_V \sqrt{T}} \tag{6}$$

$$\sigma_V = \left(\frac{\text{MarketCap}}{\text{FirmValue}}\right) \cdot \sigma_E + \left(\frac{\text{TotalDebt}}{\text{FirmValue}}\right) \cdot \left(\frac{0.05}{\sqrt{12}} + 0.25 \cdot \sigma_E\right) \tag{7}$$

V_A: Market value of assets

σ_V: Estimated asset volatility

μ: Expected asset return

σ_E: Equity return volatility (1-year rolling window)

- **CyberRisk^A:** Absolute frequency of cybersecurity-related keywords, as defined by Jamilov et al. (2023), in each earnings call transcript.
- **CyberRisk^R:** Ratio of cybersecurity-related keyword count to total words in the transcript (range: 0–1), as defined by Jamilov et al. (2023).

- **Cyber^{ind}:** Equals 1 if the absolute count of cybersecurity-related keywords (Cyber Risk) is greater than 0, and 0 otherwise.
- **DEO:** Fraction of a firm's total shares held by dual holders (investors who hold both equity and debt), as defined by Bodnaruk and Rossi (2016).
- **DEO^{inst}:** Fraction of total shares held by dual holders, scaled by total institutional ownership, as defined by Bodnaruk and Rossi (2016).
- **DEO^{cond}:** Fraction of total shares held by dual holders whose equity and debt ownership stakes each lie between 5% and 95%, as defined by Bodnaruk and Rossi (2016). A financial conglomerate is classified as a dual holder if, through its affiliates, it simultaneously holds both equity and bonds of the same firm, and the par value of its bond position represents between 5% and 95% of its total position in the firm.
- **Covenants:** A count variable constructed from Mergent FISD that captures the number of bond covenants intended to protect bondholders or restrict issuer behavior. It includes 26 indicators: 8 bondholder protective covenants and 18 issuer restrictive covenants.

  The bondholder protective covenants comprise: *Negative Pledge Covenant*, *Cross Default*, *Cross Acceleration*, *Change of Control Put Provision*, *Rating Decline Trigger Put*, *Declining Net Worth*, *After-Acquired Property Clause*, and *Asset Sale Clause*.

  The issuer restrictive covenants include: *Consolidation or Merger Restrictions*, *Dividends and Related Payments*, *Funded Debt*, *Indebtedness*, *Investments*, *Liens*, *Maintenance of Net Worth*, *Restricted Payments*, *Sales and Leasebacks*, *Sale of Assets*, *Senior Debt Issuance*, *Stock Issuance by the Issuer*, *Stock Transfer or Sale Restrictions*, *Subordinated Debt Issuance*, *Transactions with Affiliates*, *Net Earnings Test*, *Fixed Charge Coverage*, and *Leverage Test*.

IA2 Cyber risk and bond returns

IA2.1 Univariate portfolio analysis

I begin by examining the significance of cyber risk exposure in corporate bond returns using a portfolio-level analysis. Portfolios are formed monthly from July 2002 to June 2023 based on firm-level CyberRisk^R, measured in the previous quarter. At the end of each quarter, bond-issuing firms are sorted in ascending order of their prior-quarter cyber risk and allocated into three portfolios: low, medium, and high cyber-risk firms. Firms with zero cyber exposure are assigned to the low-risk portfolio (tercile 1), while the remaining firms are evenly split into the medium (tercile 2) and high (tercile 3) portfolios. Portfolios are rebalanced quarterly, and their performance is tracked over the subsequent quarter. Following Florackis et al. (2023) to ensure robustness, the analysis excludes firms that appear in the sample for fewer than 30 months or that have zero cyber-related disclosures throughout the sample period. Portfolios are value-weighted based on the amount outstanding of each bond.

IA5 reports the results. Moving from tercile 1 to tercile 3, the average excess return of the cyber-risk-sorted portfolios increases from 0.45% to 0.52% per month. However, the monthly average return difference between tercile 3 and 1 is 0.06%, with a Newey-West t-statistic that is not statistically significant.

Next, I test whether the return differences between high- and low-risk exposure bonds can be explained by prominent bond market factors. Following Bai, Bali, and Wen (2021), I use a four-factor model that includes the aggregate corporate bond market, downside risk, credit risk, and liquidity risk factors. The excess bond market return ($MKT\ Bond$) is proxied by the Merrill Lynch Aggregate Bond Market Index returns in excess of the one-month Treasury bill return. Illiquidity ($ILLIQ$) is calculated as the autocovariance of price changes, following Roll (1984). The downside risk factor (DRF) is defined as the

value-weighted average return difference between the highest-value-at-risk portfolio minus the lowest-value-at-risk portfolio within each rating portfolio. The liquidity risk factor (LRF) is generated based on the monthly change (i.e., innovations) in aggregate illiquidity, and the credit risk factor (CRF) is the value-weighted average return difference between the highest- and lowest-rating portfolios within each illiquidity portfolio.

While the long-short portfolio in tercile 3 and tercile 1 generates a monthly alpha of 0.09% when using the bond market factor model, this alpha decreases to 0.01% when using the four-factor bond model, suggesting that bond market factors explain a substantial portion of the return differences.

IA2.2 Fama–MacBeth regressions

So far, I have tested the significance of cyber risk exposure at the portfolio level. I now examine the cross-sectional relationship between cyber risk exposure and expected returns at the bond level using Fama and MacBeth (1973) regressions. I present the time-series averages of the slope coefficients from regressions of one-month-ahead excess bond returns on cyber risk exposure and control variables, including bond momentum (MOM), bond market beta (β^{Bond}), default beta (β^{DEF}), term beta (β^{TERM}), credit rating, year to maturity (MAT), bond amount outstanding (SIZE), and illiquidity (ILLIQ). Monthly cross-sectional regressions are run for the following time-series regression:

$$R_{i,t+1} = \lambda_{0,t} + \lambda_{1,t} \cdot \text{CyberRisk}^{R}_{i,t} + \sum_{k=1}^{K} \lambda_{i,k} \cdot \text{Controls}_{k,t} + \epsilon_{i,t+1}, \tag{2}$$

where $R_{i,t+1}$ is the excess return on bond i in month $t+1$.

IA6 reports the time-series average of the intercepts, the slope coefficients (λ's), and the adjusted R^2 values over the 252 months from July 2002 to June 2023. The Newey-West adjusted t-statistics are reported in parentheses. After controlling for bond characteristics

such as MOM Bond, β^{Bond}, β^{DEF}, β^{TERM}, credit rating, maturity, size, and illiquidity, the average slope coefficient for cyber risk remains positive but statistically insignificant. This suggests that while cyber risk exposure is priced at the portfolio level, its impact on individual bond returns is weaker when accounting for other bond-specific characteristics.

IA3 Appendix Figures

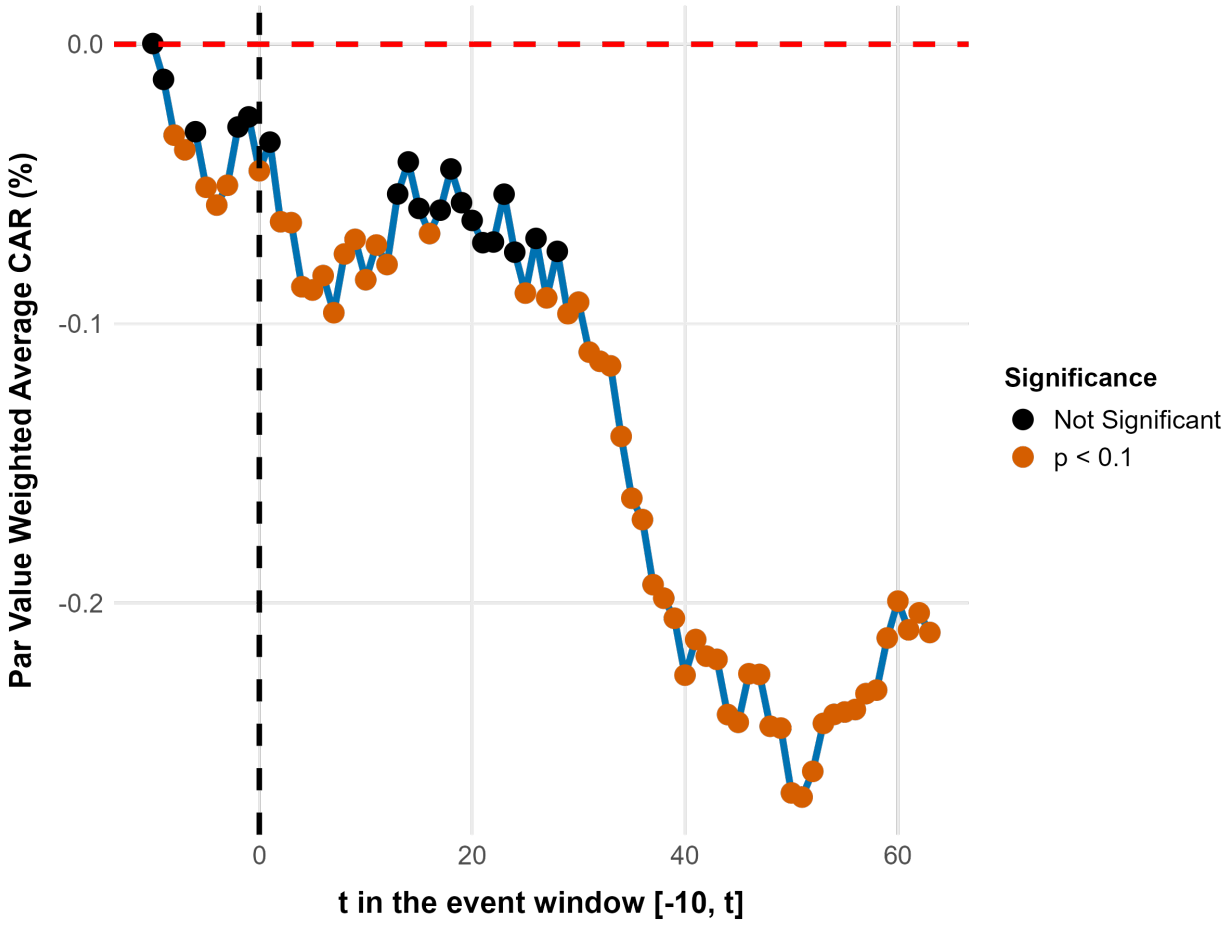


Figure IA1.A: Cumulative abnormal bond returns (CARs) around the cyberattack announcement dates.

This figure shows cumulative abnormal bond returns around cyberattack event windows. Abnormal bond returns (ABR) are calculated by subtracting the return of a benchmark portfolio matched on credit rating and maturity: $\text{ABR}_{t-1,t} = R_{t-1,t} - BM_{t-1,t}$. Benchmark portfolios are constructed using 24 groupings: six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Returns are weighted by outstanding par value to construct the benchmark portfolio return within each group. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings.

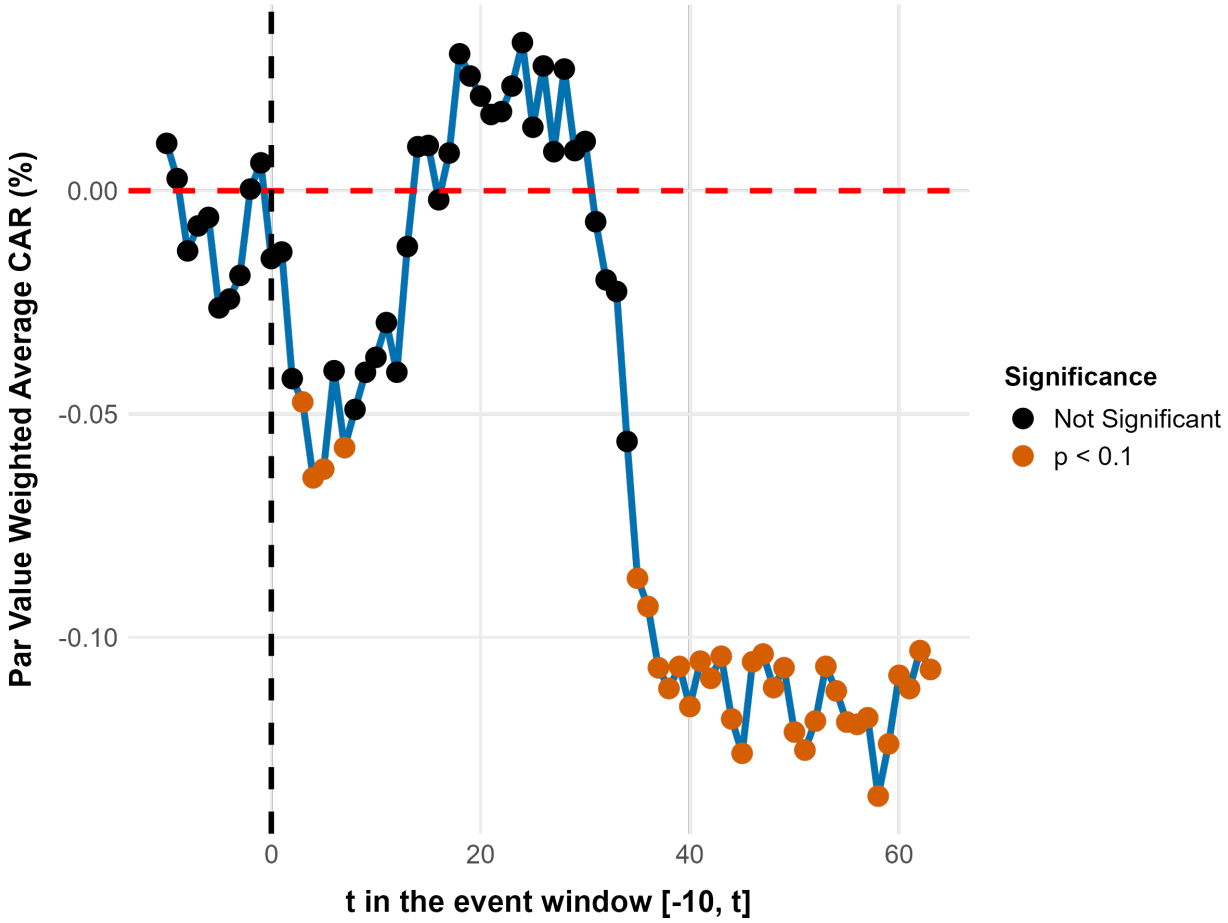


Figure IA1.B: Cumulative abnormal bond returns (CARs) around the cyberattack announcement dates for investment-grade bonds.
This figure shows cumulative abnormal bond returns around cyberattack event windows for investment-grade bonds. Abnormal bond returns (ABR) are calculated by subtracting the return of a benchmark portfolio matched on credit rating and maturity: $\text{ABR}_{t-1,t} = R_{t-1,t} - BM_{t-1,t}$. Benchmark portfolios are constructed using 24 groupings: six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Returns are weighted by outstanding par value to construct the benchmark portfolio return within each group. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings.

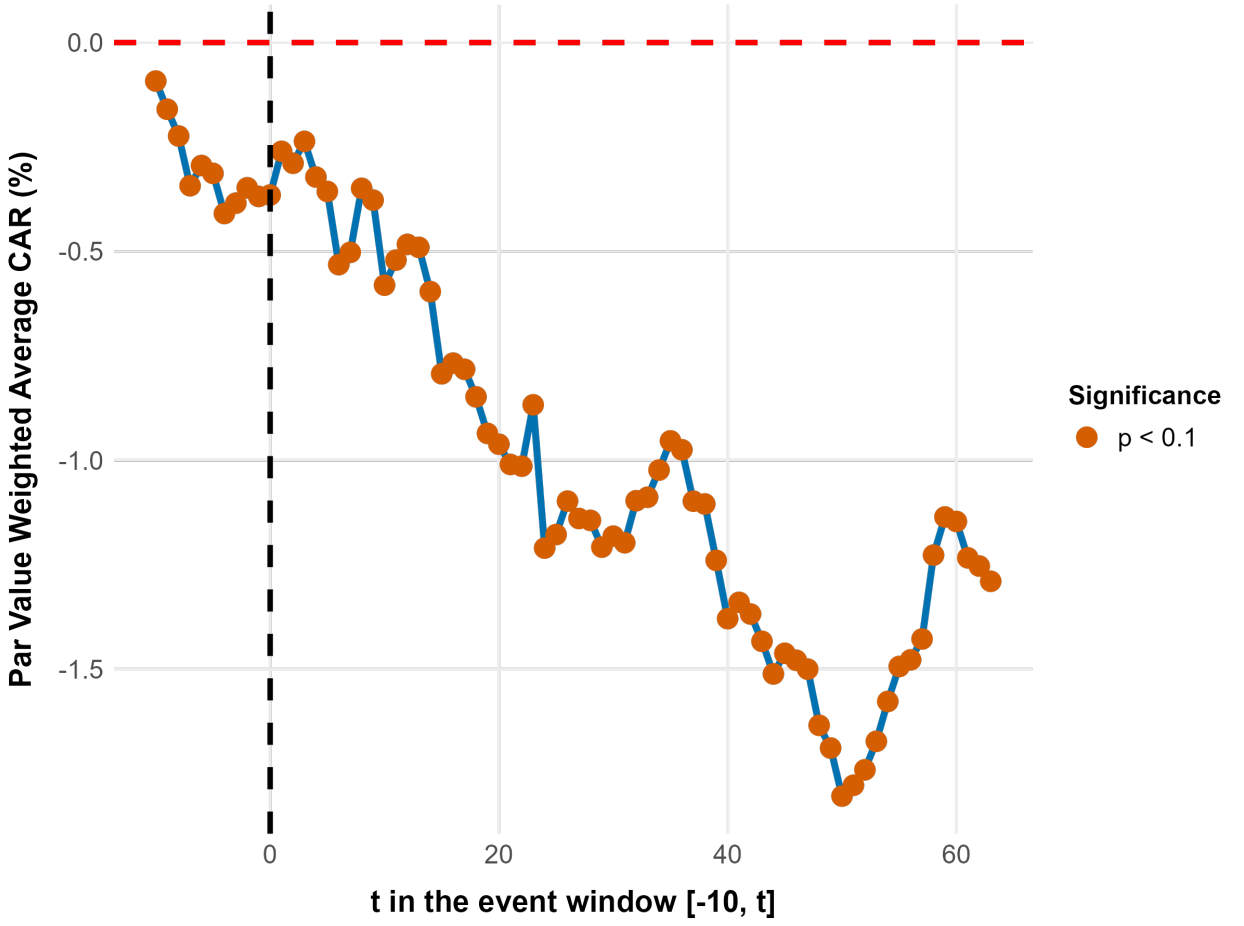


Figure IA1.C: Cumulative abnormal bond returns (CARs) around the cyberattack announcement dates for junk bonds.

This figure shows cumulative abnormal bond returns around cyberattack event windows for junk bonds. Abnormal bond returns (ABR) are calculated by subtracting the return of a benchmark portfolio matched on credit rating and maturity: $\text{ABR}_{t-1,t} = R_{t-1,t} - BM_{t-1,t}$. Benchmark portfolios are constructed using 24 groupings: six credit rating categories (Aaa/Aa, A, Baa, Ba, B, and below B) and four maturity buckets (0–3 years, 3–5 years, 5–10 years, and over 10 years). Returns are weighted by outstanding par value to construct the benchmark portfolio return within each group. Credit ratings are taken as the median of Moody's, S&P, and Fitch ratings.

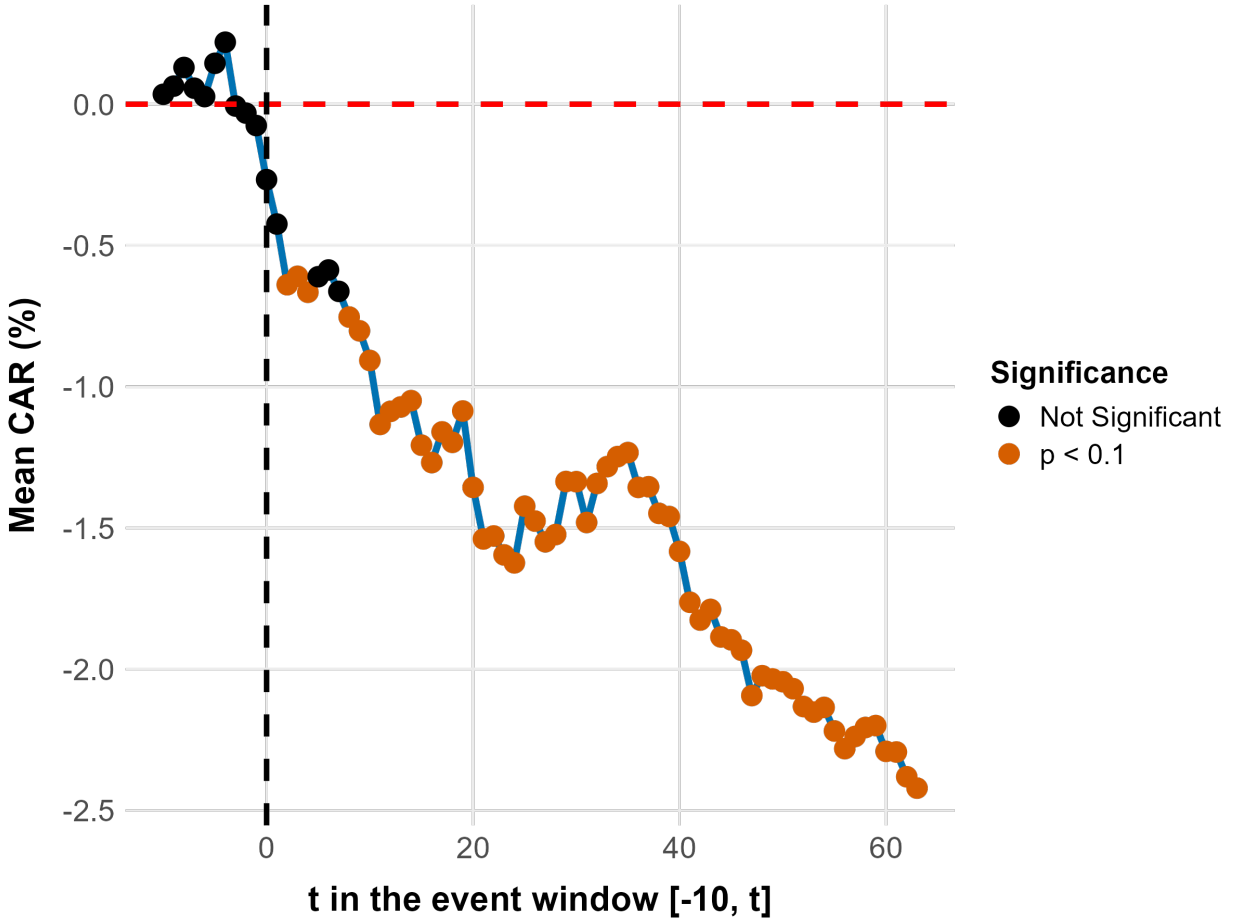


Figure IA1.D: Cumulative stock abnormal returns (CARs) around the cyberattack announcement dates.
This figure shows cumulative abnormal stock returns around cyberattack event windows. Abnormal stock returns (AR) are calculated by subtracting the market return: $\text{AR}_{t-1,t} = R_{t-1,t} - R^M_{t-1,t}$. Returns are weighted by market capitalization to construct the market return.

IA4 Appendix Tables

Table IA1: Predicting cyberattacks.
This table shows the results of regressing the firm's future cyberattacks (indicator) on cyber risk exposure and control variables over 2005 to 2021(September) using a logit model.

$$\text{FutureCyberattack}_{i,t+1} = \beta_0 + \beta_1 \cdot \text{CyberRisk}_{i,t} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

The appendix provides detailed descriptions of the construction of the variables. Heteroscedastic robust standard errors are clustered at the quarter and firm level. Standard errors are reported in parentheses. *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: FutureCyberattack$_{t+1}$	
	(1)	(2)
$\log(1 + CyberRisk^A)$	0.202**	
	(0.091)	
$CyberRisk^R$		0.068*
		(0.040)
Firm Controls	Y	Y
Industry Fixed Effects	Y	Y
Year-Quarter Fixed Effects	Y	Y
Observations	56,391	56,391
Pseudo R^2	0.236	0.235

Table IA2: The effect of ex-ante cyber risk on firm's EDF.
This table shows the results of regressing the firm's EDF (Equation 5) on cyber risk exposure and control variables over 2005 to 2021(September) using a zero-inflated Poisson model (extensive margin) in columns 1-2 and a Tweedie regression (type of GLM) conditioning on non-zero EDF (intensive margin) in columns 3-4.

$$\text{EDF}_{i,t} = \beta_0 + \beta_1 \cdot \text{CyberRisk}_{i,t} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

The appendix provides detailed descriptions of the construction of the variables. Heteroscedastic robust standard errors are clustered at the quarter and firm level. T-stats are reported in parentheses. *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: $\Pr(\mathbf{EDF}_{it} = 0)$		**Dependent Variable:** $\mathbb{E}[\mathbf{EDF}_{it} \mid \mathbf{EDF}_{it} > 0]$	
	(1)	(2)	(3)	(4)
$\log(1 + CyberRisk^A)$	-0.071^{***}		0.065^{***}	
	(-4.49)		(3.86)	
$CyberRisk^R$		-0.010		0.021
		(-0.62)		(1.46)
Firm Controls	Y	Y	Y	Y
Industry Fixed Effects	Y	Y	Y	Y
Year-Quarter Fixed Effects	Y	Y	Y	Y
Observations	179,086	179,086	155,858	155,858
Pseudo R^2	0.405	0.405	0.597	0.597

Table IA3: Diff-in-diff regression of cyber risk exposure and dual ownership. This table shows the results from difference-in-differences regressions around the mergers of financial conglomerates, which increase the number of significant dual holders for treated firms. The estimated Poisson regression (Equation 3) is:

$$\text{CyberRisk}^{A}_{i,t+1} = \beta_0 + \beta_1 \cdot \text{Treated}_{i,t} \cdot \text{Post}_{i,t} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where $\text{Treated}_{i,t}$ is an indicator for firms in which, one quarter prior to the merger announcement $(t-1)$, each merging financial institution held at least 1% of the firm's equity and 1% of its outstanding bonds—but neither institution held both positions. $\text{Post}_{i,t}$ includes quarters $t+1$ through $t+6$, while the pre-treatment period includes $t-4$ through $t-1$. The merger announcement quarter $(t=0)$ is excluded from the regression. Control firms are matched to treated firms using propensity score matching (PSM) based on firm size, market-to-book ratio, and return volatility, requiring covariate similarity within one standard deviation. Matching is performed within SIC2 industries and calendar year-quarters. Additionally, I require that control firms have no significant dual holders—defined as institutions holding at least 1% of both the firm's equity and bonds—during the matching quarter. The appendix provides detailed descriptions of the construction of the variables. Heteroscedastic robust and clustered standard errors at the cohort-year-quarter level are reported in parentheses *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: CyberRisk$^{A}_{t+1}$
	(1)
Treated	−0.021
	(0.152)
Post	−0.278
	(0.766)
Treated × Post	−0.267*
	(0.156)
Firms Controls	Y
Industry Fixed Effects	Y
Cohort-Year-Quarter Fixed Effects	Y
Observations	1,566
Number of Treated Firms	88
Number of Control Firms	88
Pseudo R^2	0.447

Table IA4: Diff-in-diff regression of yield spread on dual ownership and cyber risk exposure.

This table shows the results from triple difference-in-differences regressions of yield spread on cyber risk exposure around the mergers of financial conglomerates, which increase the number of significant dual holders for treated firms. The estimated regression model (Equation 4) is:

$$\text{Yield Spread}_{i,t+1} = \beta_0 + \beta_1 \cdot \text{Treated}_{i,t} \cdot \text{Post}_{i,t} \cdot \text{CyberRisk}^{A}_{i,t'} + \beta_2 \cdot \text{Controls}_{i,t} + \eta_c + \eta_t + \epsilon_{i,t}$$

where $\text{Treated}_{i,t}$ is an indicator for firms in which, one quarter prior to the merger announcement $(t-1)$, each merging financial institution held at least 1% of the firm's equity and 1% of its outstanding bonds—but neither institution held both positions. $\text{Post}_{i,t}$ includes quarters $t+1$ through $t+6$, while the pre-treatment period includes $t-4$ through $t-1$. The merger announcement quarter $(t=0)$ is excluded from the regression. $\text{CyberRisk}^{A}_{i,t'}$ captures the pre-merger level of absolute cyber risk exposure (CyberRisk^{A}), fixed at its value in quarter $t-1$ and held constant in subsequent periods. Control bonds are matched to treated bonds using propensity score matching (PSM) based on firm size, market-to-book ratio, return volatility, and time to maturity, requiring covariate similarity within one standard deviation. Matching is performed within investment-grade status, SIC2 industries, and calendar year-quarters. Additionally, I require that control firms have no significant dual holders—defined as institutions holding at least 1% of both the firm's equity and bonds—during the matching quarter. The appendix provides detailed descriptions of the construction of the variables. Clustered standard errors at the quarter and firm level are reported in parentheses. *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable: Yield Spread$_{t+1}$	
	(1)	(2)
Treated	0.081	−0.165
	(0.249)	(0.293)
Post	2.456	2.307
	(2.690)	(2.716)
Treated × Post	−0.194	0.217
	(0.259)	(0.303)
CyberRisk^{A}		0.046
		(0.177)
Treated × CyberRisk^{A}		0.478
		(0.416)
Post × CyberRisk^{A}		0.251
		(0.193)
Treated × Post × CyberRisk^{A}		−0.769*
		(0.461)
Bond Controls	Y	Y
Firms Controls	Y	Y
Industry Fixed Effects	Y	Y
Cohort-Year-Quarter Fixed Effects	Y	Y
Observations	7,578	7,578
Number of Treated Firms	73	73
Number of Treated Bonds	344	344
Number of Control Firms	154	154
Number of Control Bonds	587	587
Adjusted R^2	0.702	0.705

Table IA5: Univariate portfolios of corporate bonds sorted by cyber risk exposure.

Tercile portfolios are formed monthly from July 2002 to June 2023 based on firm-level CyberRisk^R measured in the previous quarter. At the end of each quarter, bond-issuing firms are sorted in ascending order of their prior-quarter cyber risk and allocated into three portfolios: low, medium, and high cyber-risk firms. Firms with zero cyber exposure are assigned to the low-cyber-risk portfolio (tercile 1), while the remaining firms are split evenly into the medium (tercile 2) and high (tercile 3) portfolios. Portfolios are rebalanced quarterly, and their performance is tracked over the subsequent quarter. Following (Florackis et al., 2023) and to ensure robustness, the analysis excludes firms that appear in the sample for fewer than 30 months or that have zero cyber-related disclosures throughout the sample period. Portfolios are value-weighted using the amount outstanding of each bond. Table reports, for each tercile, the average $CyberRisk^R$, next-month average excess return, the one-factor (bond market) alpha, and the four-factor alpha estimated from bond market factors. The final six columns summarize portfolio characteristics: bond beta (β^{MKT}), illiquidity (ILLIQ), downside risk (VaR), credit rating, time-to-maturity (in years), and size measured as total amount outstanding in billions of dollars. The last row reports the differences in monthly average returns and differences in alphas across quintiles. The four-factor bond market model includes the excess bond market return (MKT), the downside risk factor (DRF), the credit risk factor (CRF), and the liquidity risk factor (LRF). Average excess returns and alphas are expressed in monthly percentage terms. Newey-West adjusted t-statistics are reported in parentheses. Significance levels are denoted by *p<0.1; **p<0.05; ***p<0.01.

Terciles	Average	Average	1-factor bond	4-factor bond	Average portfolio characteristics					
	$CyberRisk^R$	excess return (%)	alpha (%)	alpha (%)	β^{MKT}	ILLIQ	VaR	Rating	Maturity	Size
Low $CyberRisk^R$	0.00	0.45***	0.40***	0.35**	1.12	0.37	0.03	7.62	9.30	0.82
		(3.76)	(3.71)	(2.46)						
Medium $CyberRisk^R$	0.41	0.46***	0.41***	0.34**	1.09	0.34	0.03	7.35	9.55	0.92
		(3.92)	(3.54)	(2.08)						
High $CyberRisk^R$	1.75	0.52***	0.49***	0.36**	1.08	0.30	0.03	7.41	10.48	0.95
		(4.14)	(4.06)	(2.52)						
High - Low		0.06	0.09*	0.01						
		(1.17)	(1.78)	(0.50)						

Table IA6: Fama-MacBeth cross-sectional regressions.
This table reports the average intercept and slope coefficients from the (Fama and MacBeth, 1973) cross-sectional regressions of one-month-ahead corporate bond excess returns on the $CyberRisk^R$ with additional controls:

$$\mathrm{R}_{i,t+1} = \lambda_{0,t} + \lambda_{1,t} \cdot \mathrm{CyberRisk}^R_{i,t} + \sum_{k=1}^{K} \lambda_{i,k} \cdot \mathrm{Controls}_{k,t} + \epsilon_{i,t+1}$$

Bond-level control variables include credit rating, time to maturity (in years), and amount outstanding (size, in billions of dollars). Credit ratings are expressed numerically, where 1 corresponds to AAA and 21 corresponds to C; higher numerical scores indicate greater credit risk. The bond market beta (β_{MKT}), default beta (β_{DEF}), and term beta (β_{TERM}) measure the exposures of individual bonds to the aggregate bond market factor, the default factor (as the difference between the return on a market portfolio of long-term corporate bonds and the long-term government bond return), and the term factor (as the difference between the monthly long-term government bond return and the one-month Treasury bill rate), respectively. These betas are estimated using a 36-month rolling window. Additional bond characteristics include ILLIQ, (Roll, 1984) measure of bond-level illiquidity; and MOM, the bond momentum factor, defined as the cumulative past 11-month return from $t-12$ to $t-2$, skipping month $t-1$. The Fama-MacBeth regressions are estimated each month over the period July 2002 to September 2021. Newey-West adjusted t-statistics are reported in parentheses. Significance levels are denoted by *p<0.1; **p<0.05; ***p<0.01.

	Dependent Variable:
	R_{t+1}
	(1)
$CyberRisk^R$	0.0002
	(1.05)
β^{MKT}	0.0005
	(0.67)
β^{DEF}	0.0000
	(-0.33)
β^{TERM}	0.0001
	(0.73)
Rating	0.0003
	(1.14)
Maturity	0.0001
	(1.49)
Size	0.0011 ***
	(3.16)
ILLIQ	0.0009 **
	(2.14)
MOM	0.0089
	(1.26)
(Intercept)	-0.0073 **
	(-3.03)
Number of Bonds	8,022
Adjusted R^2	0.289