NBER WORKING PAPER SERIES

THE ANATOMY OF CYBER RISK

Rustam Jamilov
Hélène Rey
Ahmed Tahoun

Working Paper 28906
http://www.nber.org/papers/w28906

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
June 2021, Revised December 2025

For useful comments and feedback we thank our discussants Christodoulos Louca, Jinfei Sheng, Ishita Sen, and Emily Williams as well as Marie Briere, Matteo Crosignani, Tom Ferguson, Chris Florackis, Linda Goldberg, Jason Healey, Ralph Koijen, Anna Kovner, Marco Macchiavelli, Emanuel Moench, Patricia Mosser, Richard Portes, Elias Papaioannou, Zacharias Sautner, Andre Silva, Laurence van Lent, Grigory Vilkov and seminar participants at numerous venues. Mahammad Ahmadli, Luis Alonso Armesto, Haotian Bai, Marco Bellifemine, Zeta Chai, Aakash Kalyani, Maiwand Nangyal, Ruilang Qin, Giovanni Rosso, Markus Schwedeler, Daoyu Sun, and André Gonçalves Veiga provided excellent research assistance. We thank Chris Florackis for sharing their data. Jamilov gratefully acknowledges financial support from the Wheeler Institute for Business and Development and the John Fell Fund (CUD00490). Tahoun sincerely appreciates support from the Institute for New Economic Thinking (INET). Send correspondence to Hélène Rey. The paper does not represent the views of the French Macroprudential Authority or the National Bureau of Economic Research.

The Anatomy of Cyber Risk
Rustam Jamilov, Hélène Rey, and Ahmed Tahoun
NBER Working Paper No. 28906
June 2021, Revised December 2025
JEL No. F3, G0

ABSTRACT

This paper uses computational linguistics to introduce a novel measure of firm-level cyber risk exposure based on the quarterly earnings calls of listed firms. Our measure covers more than 14,000 firms from over 90 countries between 2003 and 2025. The measure is validated using human auditors and a large language model. We show that the measure affects stock returns and profits, is priced in the options market, and predicts actual cyberattacks. Cyber risk spills over across firms and propagates from firm to sector level. Back-of-the-envelope estimates suggest that the global cost of cyber risk exposure amounts to hundreds of billions of dollars annually.

Rustam Jamilov
All Souls College
rustam.jamilov@all-souls.ox.ac.uk

Ahmed Tahoun
London Business School
atahoun@london.edu

Hélène Rey
London Business School
and CEPR
and also NBER
hrey@london.edu

1 Introduction

The World Economic Forum identifies systemic cyber risk as one of the most likely and impactful risks for firms (WEF, 2016). This concern is growing in importance with geopolitical conflicts, hybrid war threats and the growing importance of cyber espionage linked to technological rivalries (WEF, 2025). The European Systemic Risk Board has characterized cyber security as a systemic risk to the European financial system (ESRB, 2020). Systemic risk surveys of financial market participants cite cyber security as the second most challenging risk for managing a firm, falling behind only political risk (BoE, 2020). During the COVID-19 pandemic, the world saw an unprecedented rise in cybercrime, to the point that multiple unique cyberattacks were being reported each day (Lallie et al., 2021). An International Monetary Fund survey warns that cybersecurity is a real threat to macroeconomic stability and that the majority of national supervisory authorities do not have a clear cyber strategy or a dedicated cyber incident reporting protocol (Adrian and Ferreira, 2023). As the frequency of realized cyberattacks continues to grow and uncertainty about potential future incidents intensifies, the measurement and quantification of *exposure* to cyber risk have become first-order concerns for academics and policymakers alike.

This paper makes progress by constructing a novel measure of firm-level exposure to cyber risk from quarterly earnings conference calls of listed firms. Our paper builds on recent work that leverages textual information in the 10-K files to measure exposure to cyber risk (Florackis et al., 2023), and the literature that uses earnings calls for quantifying firms' exposure to risk factors such as political risk or climate change risk (Hassan et al., 2019; Sautner et al., 2023). Conference calls usually take place concurrently with an earnings release and grant a chance for management to describe the overall business position of their company (Hollander et al., 2010). Earnings calls are forward-looking since many informative dialogues take place during post-announcement Q&A sessions when analysts ask questions about various pressing issues and future plans (Huang et al.,

2018).

Using the universe of available English-language earnings call transcripts, we measure the cyber risk exposure faced by each firm in a given quarter by counting the number of times cybersecurity-related terms are mentioned. Our universe of keywords is built in two steps. First, we assemble a word list that consists of cyber lexicon libraries from three reputable authorities on the subject: the Financial Stability Board (FSB), the National Cyber Security Centre (NCSC), and the Cybersecurity and Infrastructure Security Agency (CISA). Second, we employ a keyword discovery algorithm that proposes additional terms based on a set of initial bigrams. We can differentiate across distinct sections and participants of each earnings call. Accordingly, we construct four additional measures of cyber risk exposure: one for the management presentation, one for the Q&A session with analysts, one for firm executives, and one for external participants. This decomposition allows us to separate the voluntary and structured disclosure of information by firm executives in the presentation section from analyst attention and the generally unstructured nature of Q&A sessions. Our quarterly measures cover 14,317 unique firms across 91 countries from 2003Q1 to 2025Q3.

We perform numerous exercises to validate our measures. First, we follow the approach of Baker et al. (2016) and Sautner et al. (2023) and perform a human audit test. Nine graduate students from the University of Oxford have been recruited to evaluate 2,700 randomly drawn snippets of earnings call text. Each student provides their own "extensive" and "intensive" margin evaluation of each snippet. The former requires a yes or no answer to the question of whether a snippet contains cyber risk-related conversations. The latter asks the students to assign an intensity score, between 1 and 10, to the "yes" cases. Second, to complement the human audit we also employ a commercial Large Language Model (LLM). We use ChatGPT 5.0 to audit more than 50,000 randomly chosen snippets and produce the same extensive and intensive scores. Both the human and LLM audit exercises have confirmed that our measures realiabily capture actual cyber-

related conversations and ignore non-cyber-related conversations. In other words, our measurements exhibit low Type-I and Type-II errors. Third, we leverage the database of reported cyberattacks from the Privacy Rights Clearinghouse and show that our measure can predict them in an out-of-sample forecasting exercise that we run by following the literature on forecasting firm default (Campbell et al., 2008). This result confirms that our measures do not simply pick up past incidents but capture exposure to potential events in the future. Fourth, we compare time-series properties of our measure with alternative, independently developed cyber-risk indices. In particular, we show that our measure behaves in a similar way to the indices of cybersecurity that are based on 10-K filings (Florackis et al., 2023), major U.S. newspapers, Google Trends, and realized cyberattacks. Fifth and finally, we perform a case-study analysis of some of the largest cyberattacks in recent history and confirm that our measure correctly picks up the timing of each incident. For example, for the 2017 Equifax breach—which is one of the biggest firm-level cyber incidents to-date—our measures pick up abnormally high exposure.

Equipped with a validated measure of firm-level cyber risk exposure, we proceed by documenting several aggregate stylized facts. First, average cyber risk exposure has increased significantly over time, and especially so after 2013 when several high-profile cyberattacks occurred. The measure reached its time-series global peak during the COVID-19 pandemic when 3-4 unique cyber-attacks were being reported every day (Lallie et al., 2021). Second, decomposition of our measure by earnings call section reveals that around half of total exposure stems from the presentation and the remaining half from the Q&A section. When decomposing, instead, by the identity of the speaker, we find that around 90% of total exposure comes from firm executives and the rest from external participants. Third, while cyber risk exposure was predominantly a U.S.-centered concern a decade ago, by 2025 U.S. firms account for only about 50% of total global exposure, followed by firms from Asia, Europe, and the Americas ex-U.S. Fourth and finally, exposure to cyber risk is heterogeneous across sectors, with the three most affected industries being

manufacturing, information technology, and finance.

To understand the nature of firm-level cyber risk exposure, we perform two exercises. First, we characterize the profile of a typical firm with high exposure. Such a firm has a high ratio of intangible assets to total assets, high liquidity, and large size (as measured by total assets). These characteristics appear consistently across studies examining the determinants and drivers of cyber risk (Aldasoro et al., 2022). Second, we conduct a variance decomposition analysis to separate the relative contributions of firm-level, industry-level, and aggregate components to the total variation in our measures. We find that between 73% and 90% of the variation in firm-level cyber risk exposure occurs at the firm level, of which roughly half is non-persistent. This suggests that while aggregate components exist, substantial heterogeneity remains across firms even within the same industry.

Having shown that firm-level variation in cyber risk exposure is considerable, we now examine its implications for firm-level financial market and balance sheet outcomes. First, we show that our measures are priced in the equity market: high cyber risk exposure is systematically associated with lower stock returns and higher stock market volatility. This result is consistent with Kamiya et al. (2021), who document the stock market implications of realized cyberattacks, and Jiang et al. (2020), who show that cyber risk is priced in the cross section of stock returns. Second, high cyber risk exposure is associated with lower profitability, reduced cash flow, and weaker credit ratings. A simple back-of-the-envelope calculation suggests that the global cost of cyber risk exposure amounts to approximately $1.14 trillion annually—a figure broadly consistent with estimates from other contemporary studies. As our calculation does not account for indirect or second-order effects, the true financial cost of cyber risk exposure is likely even greater.

Third and finally, cyber risk exposure is priced in the options market. The values of option protection against price, variance, and downside risks are all greater for firms with higher cyber risk exposure. Our proxy for downside risk is the implied volatility slope measure of Kelly et al. (2016), which builds on the theoretical framework of Pastor and

Veronesi (2013). This finding is economically significant: a one-standard-deviation increase in our measure raises firms' implied volatility, variance risk premium, and implied volatility slope by roughly 5%, 4%, and 3% of the respective variable's standard deviation. To put these magnitudes into context, Sautner et al. (2023) employ earnings calls and find that the impact of firm-level climate change exposure on these same option-market variables ranges from 0.3% to 2.4% of the variables' standard deviations. A similar pattern holds for firm-level political risk exposure, as shown in Hassan et al. (2019). Overall, these magnitudes are consistent with the view that cyber risk constitutes a first-order source of risk for firms.

Moving beyond firm-level analysis, we now ask whether firm-level cyber risk can have systemic implications. First, we find that cyber risk exposure spills over from affected firms to unaffected peers. The latter are defined as firms operating in the same country and industry as the exposed firms but exhibiting no cyber risk exposure of their own. Second, firm-level cyber risk exposure does not wash out at the industry level. Industry-level cyber risk exposure is associated with lower stock returns, higher stock market volatility, greater costs of protection against price, variance, and downside risks, and lower returns on assets. Overall, these results suggest that idiosyncratic firm-level cyber risk can aggregate into systemic effects, amplifying financial and economic vulnerabilities.

Literature. Our paper contributes to the growing literature that estimates the economic and financial impacts of cybersecurity risk. Kamiya et al. (2021) employ the Privacy Rights Clearinghouse database and quantify the effects of reported cyberattacks on firm-level stock returns and subsequent economic outcomes. Eisenbach et al. (2022) study how cyberattacks get amplified through the U.S. financial system, with a focus on the wholesale payments network. Aldasoro et al. (2022) leverage the Advisen cyber loss database and provide a comprehensive analysis of the common characteristics and triggers of cyber incidents in the U.S. Crosignani et al. (2023) show that cyberattacks can propagate through firms' supply chain networks by examining the 2017 NotPetya malware attack—one of

the most damaging in history. Akey et al. (2024) find that data leaks and breaches cause deterioration in firm value and erase reputational capital, leading firms to rebuild that capital through activities such as corporate social responsibility. Kotidis and Schreft (2025) leverage a natural experiment to quantify the impact of a prolonged cyberattack on a technology service provider to the U.S. banking sector.[1]

Relative to the large sub-set of the literature which relies on reported cyberattacks, our approach is robust to the important critique that many cyberattacks go unreported and only the largest events get publicized (Amir et al., 2018). Our focus on cyber risk *exposure* is less likely to suffer from such selection issues: our dataset spans all English-language transcripts of listed firms and during the Q&A sessions of earnings calls analysts pressure firm executives on issues that the latter could potentially ignore or postpone otherwise, rendering timely information disclosure much more probable. Our decomposition analysis shows that around half of the total exposure stems precisely from the Q&A sessions.

The paper that is closest to ours is Florackis et al. (2023) (FLMW, henceforth). FLMW leverage tools from textual analysis and extract information from the annual 10-K filings of U.S. listed firms to construct cybersecurity risk proxies. As mentioned previously, our baseline measure and their index behave in a reassuringly similar fashion.[2] Our study differs from FLMW considerably along several dimensions. First, the quarterly frequency of earnings calls increases the number of observations and allows for more robust cyberattack forecasting and asset pricing analyses. Second, earnings calls feature Q&A sessions which make cyber-related conversations more unrehearsed, multi-dimensional, and timely. Third, while FLMW test whether cybersecurity risk is priced in the cross section of stock returns, our focus is primarily on the option market and the impact of cyber risk exposure on the premia for protection against price, variance, and tail risks.

The methodology of our paper builds on three streams of literature. First, we belong to

[1] See also, among others, Biener et al. (2015), Makridis and Dean (2018), Kashyap and Wetherilt (2019), Duffie and Younger (2019), Woods et al. (2019), Healey et al. (2021), Lhuissier and Tripier (2021), Tosun (2021), Anhert et al. (2022), Anand et al. (2022), Adeney et al. (2022), Eling et al. (2023).

[2] We thank the authors for sharing their data.

the growing body of work on the applications of textual analysis to "important-but-hard-to-measure" questions in accounting, economics, and finance (Loughran and McDonald, 2011; Baker et al., 2016; Koijen et al., 2016; Loughran and McDonald, 2016; Gentzkow et al., 2019; Neuhierl and Weber, 2020). Second, an important sub-set of this literature applies natural language processing tools to the texts of earnings calls. Our methodology builds on the insights that were developed in Hassan et al. (2019) and later applied to contexts such as epidemic diseases (Hassan et al., 2023a), Brexit uncertainty (Hassan et al., 2023b), country risks (Hassan et al., 2023c), the diffusion of new technologies (Bloom et al., 2025), and climate change risk (Sautner et al., 2023).

Third and finally, we follow the literature that employs forward-looking option-based risk measures. Option prices have been used for predicting future asset price dynamics (Chang et al., 2013), proxying investment opportunities (Vanden, 2008), and measuring the impact of inflation on public debt valuations (Hilscher et al., 2022). Bollerslev et al. (2009) show that the variance risk premium (VRP) predicts future excess returns. Kelly et al. (2016) show that political uncertainty is priced in the stock option market. They also introduce the implied volatility slope (SlopeD) measure which we adopt as a proxy of tail risk. Ilhan et al. (2021) find that climate policy uncertainty matters in the cross section of firms and has significant effects on option market variables such as the VRP and SlopeD. Sautner et al. (2023) quantify the impact of firm-level climate change exposure on economic and financial outcomes, including option market variables like SlopeD.

The rest of the paper is structured as follows. Section 2 describes the data and our measures of firm-level cyber risk exposure. Section 3 validates these measures. Section 4 presents a variance decomposition of our measures and discusses the nature of firm-level cyber risk. Section 5 presents the firm-level effects of cyber risk exposure. Section 6 shows the industry-level and spillover effects of cyber risk exposure. Section 7 presents additional results and robustness tests. Finally, section 8 concludes.

2 Measurement

This section lists our data sources, defines the cyber risk keyword dictionaries, and explains how our measures of firm-level cyber risk exposure are constructed.

2.1 Data Sources

Our primary data source for the construction of cyber risk measures is quarterly earnings conference calls of firms which are publicly listed in the United States. Our dataset comes from Thomson Reuters' StreetEvents. We have collected 405,034 English-language transcripts for 14,317 unique firms from 91 countries over 2003Q1-2025Q3. Firms normally host one earnings call per quarter, usually within 30 days of the start of each quarter. In our sample, there are therefore roughly four observations per firm per year. The structure of each earnings call is typically the following: firm management starts by delivering a prepared speech on issues and topics that they wish to willfully disclose and highlight, followed by Q&A sessions with call participants (e.g. financial analysts). Each call usually lasts around 45 minutes and the average number of spoken words per transcript is less than 8,000. We run a search of cybersecurity-related terms through each conference call in its entirety. We also run the same algorithm separately for the presentation, Q&A session, corporate executives, and external participants.[3]

The main source of our option data is the OptionMetrics' Ivy DB Volatility Surface File. We use three option market measures to identify the impact of cyber risk uncertainty: implied volatility (*IV*), variance risk premium (*VRP*), and implied volatility slope (SlopeD). Uncertainty should be positively related to all three variables. Following Carr and Wu (2009) and Bollerslev et al. (2009) we compute the *VRP* for each firm as the daily difference between implied and realized variance.[4] The *VRP* captures the cost of protection against

[3] As is done typically, all non-alphabet characters are removed. For example, any term with a dash in between (e.g. cyber-risk) gets concatenated into a single word (i.e. cyberrisk). The search is case insensitive. The algorithm does not need the bigram (two-word combination) if it already found the first or second word independently as a separate term.

[4] Our definition of realized variance follows Kelly et al. (2016) and Ilhan et al. (2021) and is the "ex-post"

general variance risk or uncertainty, as pointed out by Bali and Zhou (2016). Finally, we follow Kelly et al. (2016) and compute the SlopeD measure, defined as the steepness of the function that relates IV to moneyness, as measured by the option's Black-Scholes delta.[5][6] A higher SlopeD suggests that deeper OTM puts are more expensive, which in turn implies a relatively greater cost of protection against *downside* tail risks. We aggregate all three option-market variables to the firm-quarter level. For our baseline analysis, we use 91-day options as this is the maturity that closely corresponds to the quarterly release schedule of earnings calls. We provide robustness results for alternative maturities (30, 60, 182, and 365) in the Online Appendix.[7]

To trace out the association between our exposure measure and realized cyberattacks, we merge earnings call announcement data with the Privacy Rights Clearinghouse (PRC) database on reported cyberattacks. Because there is no common firm identifier, we employ a variant of the fuzzy search algorithm. Specifically, we create a vector of integers for each firm name in the PRC and earnings call datasets. Then, for each firm in PRC data, we take the cosine distance from each firm in the earnings call data and keep the closest match. To create the vector of integers for a firm name, we count all unique letters, adjacent two-letter, and adjacent three-letter combinations. Finally, we compute a measure of semantic distance between firm names in the two datasets. We impose a cutoff (equal to 0.7) to throw out bad matches. We then confirm each surviving match with manual checks. In the end, 1,118 unique firm-cyberattack pairs are matched to the earnings call data.[8]

as opposed to an "ex-ante" *VRP*. While our main results do not change if we adopt the ex-ante version, using the ex-post *VRP* sharpens our results because the ex-ante version is based only on expectations built prior to the actual observation date, which makes results noisier.

[5]Delta measures the rate of change of option value with respect to changes in the underlying asset's price.

[6]We follow Kelly et al. (2016) and Sautner et al. (2023) and ignore the deepest OTM options due to measurement errors in option prices (Hentschel, 2003).

[7]As argued in Beber and Brandt (2006), among others, very short-maturity options' implied volatilities are typically inaccurate due to various sources of measurement error. We therefore do not analyze maturities shorter than 30 days.

[8]One notable feature of the PRC data is that data coverage is predominantly U.S. centered. However, our exposure measures are available for firms headquartered in many countries. It is unlikely that firms that are cyberattacked in the rest of the world, especially in developed economies, have exposure that is fundamentally different from firms that have high exposure and get attacked in the U.S. In addition,

Finally, we obtain information on stock prices from the Center for Research in Security Prices (CRSP) and, for each firm-quarter, balance sheet and income statement information from Standard and Poors' Compustat. Table A.2 in Appendix A provides details on variable construction and data cleaning steps.

2.2 Cyber Risk Keywords

Our measurement approach consists of two phases. First, we follow Baker et al. (2016) and Hassan et al. (2019) to construct a comprehensive pre-defined dictionary of terms related to cybersecurity risk. We assemble this dictionary from three reputable institutional sources that act as information aggregators on the practical cyber-risk issues firms face on a daily basis. These libraries contain most of the keywords commonly used in cyber-related discussions among private market participants across industries. Our first source is the Financial Stability Board (FSB) "Cyber Lexicon".[9] The list is designed to support the work of the FSB, authorities, and private sector agents. It includes such terms as "cyber alert", "malware", and "patch management". Our second source is the "NCSC Glossary" of common cybersecurity terms provided by the National Cyber Security Centre.[10] The list includes terms such as "cyberattack", "botnet", and "virus". Finally, our third source for the dictionary is the "Glossary of Common Cybersecurity Terms and Phrases" made available by the NICCS, an initiative managed by the Cybersecurity and Infrastructure Security Agency (CISA).[11] This comprehensive source includes such diverse terms as "spam", "security breach", and "attack signature".

The second step of our measurement approach builds on the insights from Sautner et al. (2023) and involves a keyword discovery algorithm. This method is based on Facebook AI Research lab's word embedding tool FastText. The algorithm has been trained on a

our term libraries are sourced from institutions that are either international in nature or service market participants worldwide.

[9] Available at https://www.fsb.org/2018/11/cyber-lexicon/

[10] Available at https://www.ncsc.gov.uk/information/ncsc-glossary

[11] Available at https://niccs.cisa.gov/cybersecurity-career-resources/glossary

billion phrases in corporate earning calls to suggest related keywords. We use two initial bigrams—"data breach" and "cyber risk"—and obtain hundreds of suggestions that are semantically similar to the input. The vast majority of the suggestions get discarded, either because they are already present in the pre-defined dictionary or because a suggestion associates with a different risk factor. Out of more than four hundred suggestions, we retain 75 new unique terms.

Finally, we combine the pre-defined dictionary with the list of discovered keywords. We remove any duplicates and discard all terms that register a zero frequency across all transcripts and quarters. We are left with 247 terms on which our baseline measure of exposure is built. These terms are listed in Table A.1 in concatenated form.

2.3 Measuring Firm-Level Cyber Risk Exposure

We now construct our baseline quarterly measures of firm-level cyber risk exposure. Let the set of all terms in our final dictionary be $\mathbb{C}$. Our algorithm counts the number of sentences in earnings calls that contain at least one term in $\mathbb{C}$. Let $\mathrm{s} = 0, 1, \ldots, \mathrm{S_{i,t}}$ be the sentences in the earnings call transcript of firm i and quarter i, $\mathrm{S_{i,t}}$ be the total number of sentences in each transcript, and $\mathrm{K_{s,i,t}}$ the number of keywords from $\mathbb{C}$ in sentence s. Our baseline measure is defined as follows:

$$\mathrm{CRExposure_{i,t}} = \frac{1}{\mathrm{S_{i,t}}} \sum_{\mathrm{s}=1}^{\mathrm{S_{i,t}}} 1\Big\{\mathrm{K_{s,i,t}} > 0\Big\}, \tag{1}$$

where and $1[.]$ is an indicator function.

Figure 1 plots the average of $\mathrm{CRExposure_{i,t}}$ over time. It also shows notable cybersecurity-related incidents and events. For example, in 2004, service provider AOL was reportedly seeking legal action as BuddyLinks—a type of spyware—penetrated users' computers through instant messaging programs, collected private data, and modified software on affected machines. In 2007, McAfee released a Virtual Criminology Report, in which ex-

perts warned that based on all emerging statistics and trends cyber risk would become the following decade's biggest security threat. To the best of our knowledge, this was one of the first documented recognitions of cyber risk as a new source of systemic risk. Starting from 2020Q2, the COVID-19 pandemic contributed to cyber risk reaching historical highs.

We can observe a sharp increase in average cyber risk exposure over the past decade, starting from around 2013. This structural break corresponds to the 2011-2012 SEC mandate for listed firms to begin to report material cybersecurity incidents and exposure. Another possible explanation is that 2013 was the year of the Snowden leaks and the year when hackers operated on a massive scale: Target was attacked by the POS malware and 40 million clients were affected. Adobe was also hacked around 2013, and 153 million people were affected. Furthermore, 2014 saw the high-profile hacking of Sony by North Korea. It is therefore possible that these very salient events were both the symptoms of and increased the awareness of cyber risk exposure going forward.

Decomposition by Earnings Call Section and Speaker. The measure $\mathrm{CRExposure}_{\mathrm{i,t}}$ is constructed on the basis of the entire earnings call, including both the presentation of the management and the Q&A section. It also does not differentiate between corporate representatives and external participants (analysts). Our algorithm can decompose the baseline measure by section and by speaker. Measures of cyber risk exposure for the presentation and Q&A sections, as well as for corporate executives and external participants are defined accordingly. Let these be labeled as $\mathrm{CRExposure}^{\mathrm{Pres}}_{\mathrm{i,t}}$, $\mathrm{CRExposure}^{\mathrm{Q\&A}}_{\mathrm{i,t}}$, $\mathrm{CRExposure}^{\mathrm{Exec}}_{\mathrm{i,t}}$, and $\mathrm{CRExposure}^{\mathrm{Ext}}_{\mathrm{i,t}}$, respectively.

Figure 2 plots the time-series behavior of these four compositional measures. In Panel (a), we observe that around half of total cyber risk exposure originates in management presentations, while the other half in Q&A sections. This observation emphasizes the importance of unstructured Q&A sessions, which are absent in boilerplate reports, for fully capturing risk exposures. In Panel (b), we see that around 90% of the total exposure stems from firm executives. This is reassuring, because one concern with our approach

could be that the exposure measures simply pick up analyst questions, which could be misguided or misinformed and later negated by the management. While analysts could steer the conversations—during the Q&A sessions—into informative directions, it is ultimately the firm itself that discloses information about its cyber risk exposure.

Decomposition by Region and Industry. Figure 3 decomposes time-series variation in $\mathrm{CRExposure}_{i,t}$ by geographical region and industry. Panel (a) shows that the nature of the global distribution of cyber risk exposure has changed over the past two decades. Whereas in the past cyber risk could have been thought of as a uniquely US-based problem, only around half of total global exposure originated from American firms as of 2025. The US is followed by Asia, Europe, Americas ex-US, UK, and Africa. Figure A.1 in the Online Appendix presents the global spatial distribution of cyber risk exposure in 2024 in a map format.

Panel (b) of Figure 3 shows that exposure to cyber risk is heterogeneous by industry. The most exposed sectors are manufacturing, IT, finance, and healthcare. Figure A.2 further decomposes the broader finance industry into six sub-categories. The most exposed financial firms are banks, broker-dealers, and insurance firms. The IT industry, and especially cloud providers, acts as a connecting hub for firms in the economy that is increasingly more digitalized. The finance industry, in addition, is known to have lasting propagating effects on the real economy. Heavy exposure of these two sectors to cyber risk points to potentially high probabilities of spread and contagion, in line with the insights in Duffie and Younger (2019). We formally analyze the systemic implications of cyber risk exposure in Section 6.

Additional Statistics. Table I provides summary statistics for all cyber risk exposure measures as well as financial market and balance sheet variables used throughout the paper. For expositional reasons, the exposure measures are multiplied by 100. The average frequency of cyber risk exposure is 3.22, with a range between 0 and 45.56 and

a standard deviation of 3.35. In absolute terms (not shown), the average number of sentences that contain at least one cyber risk term is 13.39, with a range between 0 and 408.

Table II further reports the top 100 most frequently occurring keywords that constitute our main measure $\mathrm{CRExposure}_{i,t}$. This list includes many terms that capture the dangers and risks associated with cyber risk exposure. These terms include "virus", "cyber", "data security", "trojan", "spam", and "data breach". The list also includes terms that do not necessarily imply immediate riskiness or an imminent incident but a general form of exposure to the cybersecurity factor, e.g. "software", "data center", "information technology", and "personal data".

Table B.I reports the correlations across the exposure measures. All correlations are statistically significant at the 1% level. Most notably, the benchmark measure $\mathrm{CRExposure}_{i,t}$ is highly correlated with $\mathrm{CRExposure}_{i,t}^{\mathrm{Exec}}$, suggesting that it is speeches by corporate executives rather than questions from the analysts drive total exposure. Interestingly, $\mathrm{CRExposure}_{i,t}$ is highly correlated with both $\mathrm{CRExposure}_{i,t}^{\mathrm{Pres}}$ and $\mathrm{CRExposure}_{i,t}^{\mathrm{Q\&A}}$, implying that both the presentation and the Q&A sections of earnings calls are almost equally important for explaining overall exposure.

In addition, Figure A.3 presents the global histograms of all cyber risk exposure measures. Tables B.III, B.IV, and B.V report the number of observations and select summary statistics by country, industry, and year.

3 Validation

In this section, we validate our baseline cyber risk exposure measure with a series of tests. First, to evaluate the performance of our algorithm we run two independent audits of snippets of earnings call texts: one by a team of humans and the second by a commercial Large Language Model (LLM). Second, we run a pseudo out-of-sample forecasting

exercise to show that our measure can predict actual cyberattacks. Third, we compare our measure with several existing, externally created indices of cyber risk. Fourth and finally, we perform a case-study analysis to showcase how our measures pick up some of the most salient cyber incidents in recent history.

3.1 Audit by Human and LLM Readings

Our approach to auditing snippets of text follows the literature standard (Baker et al., 2016; Sautner et al., 2023). We have recruited nine graduate students at the University of Oxford. Altogether, the auditors have been assigned 2,700 snippets. Each auditor independently reviewed and assessed 300 randomly chosen snippets from the earnings call transcripts. The randomization process works as follows. First, we create global deciles of the exposure measure $\mathrm{CRExposure}_{\mathrm{i,t}}$. Within each decile, we randomly select 300 snippets of text. Finally, we randomly assign each snippet to each of the nine auditors. The human auditors have not been given our list of cyber keywords. Instead, they have been asked to evaluate each snippet based on its potential exposure to cyber security, either contemporaneously or in the future, and either in a positive or negative tone. The auditors were asked to produce two scores. The first is a simple "yes" or "no" answer to the question of whether a given snippet contains any information related to cyber security. This metric is intended to capture the extensive margin. The second is a numerical grade on the [1,10] scale, intended to represent the intensive margin of exposure.

To complement the audit by human readers, we have also leveraged a commercial generative AI (GenAI) model. Specifically, we have employed the off-the-shelf ChatGPT 5.0 model to read and assess a randomly chosen sample of 56,000 snippets. The model's task was to produce the same two evaluation variables: the extensive and intensive margin scores. Our prompt, similarly to that of our human helpers, is an attempt to capture general discussions of cyber security—either in a positive or negative tone—and not merely cyber incidents and attacks. The temperature setting was set to 1.0, which

is typically the default choice. One natural advantage of this approach is that we can evaluate a lot of text, at high speed, and at low cost. However, the disadvantage is that such models—unlike some of our human auditors who are advanced PhD students in economics or finance—are not fine-tuned to this specific task. We therefore view the LLM validation step as being complementary to the human audit.

After the completion of both audits, each snippet was merged back to the corresponding transcript (firm-quarter observation) via its unique ID. Thus, for each evaluated snippet we now have the extensive and intensive score from the human and LLM auditors as well as the $\mathrm{CRExposure}_{\mathrm{i,t}}$ value from our keyword counting algorithm. Figure 4 reports the results. In each panel, on the horizontal axes we show the deciles of the cyber risk exposure measure $\mathrm{CRExposure}_{\mathrm{i,t}}$. On the vertical axes of Panels (a) and (b), we show the predicted probabilities of correctly identifying a positive case—as scored by the human auditors and our GenAI model, respectively. Predicted probabilities are computed from logit models. On the vertical axes of Panels (c) and (d), we show the decile-specific averages and one standard-deviation bands for the intensive margin score—as scored by the human auditors and our GenAI model, respectively.

Overall, we find that our measure of cyber risk exposure, $\mathrm{CRExposure}_{\mathrm{i,t}}$, seems to be accurately capturing cyber-related conversations and correctly ignoring irrelevant, non-cyber information. We first observe from Panels (a) and (b) the positive slopes of the predicted probability curves. This means that, as $\mathrm{CRExposure}_{\mathrm{i,t}}$ increases, the rate of correct positives rises—for both the human auditors and the model. In other words, the probability of a Type-I error is low. Alternatively, for a poor and uninformative measure the slope of the predictive probability line would be flat. In addition, for the lower deciles of $\mathrm{CRExposure}_{\mathrm{i,t}}$, the predictive probabilities drop to almost zero. This suggests that the likelihood of a Type-II error in our measurement is also low. In the literature, the fraction of correct positives for the lower deciles of exposure reduces to less then 25%, which is in line with our findings (Hassan et al., 2023c). Panels (c) and (d) reveal a similar pattern.

Although there is more noise in the intensity variables, the slopes of the average score curves are positive. This suggests that both human auditors and the LLM assign greater intensity scores to snippets with higher $\mathrm{CRExposure}_{i,t}$ values.

Table B.II in the Online Appendix lists several snippets of earnings call texts with some of the highest and lowest realizations of $\mathrm{CRExposure}_{i,t}$ in our sample. It also reports the extensive and intensive margin scores for the human and GenAI auditors. For example, the following transcript for Equifax in 2018Q1 has a standardized $\mathrm{CRExposure}_{i,t}$ of 2.67. The snippet reads as follows: *"Our non-GAAP financial results will include all increased costs related to IT and data security that are ongoing or permanent in nature. We will exclude from our non-GAAP financial results both the incremental or bubble costs incurred to implement our IT and data security plans and the legal and our professional service cost being encourage specifically to address the litigation and governmental and regulatory investigations related to the cybersecurity incident."* Both extensive margins return a "yes" and the average intensive margin score across the two approaches is 9.5. Another example is the 2012Q4 snippet from Walt Disney Co, which reads as follows: *And then, Jay, on the Hurricane Sandy impact, you said you couldn't really quantify it as of yet. But would the majority of that impact, whatever it is, be due to disruption at the Parks? Just because folks in the tri-state area couldn't fly down to Orlando, obviously; may still not be able to fly down there."* The snippet clearly contains no cyber-related information. Both extensive margins return a "no" and the average intensive margin score is zero.

3.2 Predicting Actual Cyberattacks

Our next validation test involves using $\mathrm{CRExposure}_{i,t}$ to predict actual cyberattacks. Unless cyberattacks are completely randomly assigned, a good measure of exposure should be able to anticipate them in advance. Our main forecasting exercise involves predicting actual cyberattacks out-of-sample. We build on the literature that uses observables to predict firm default (Campbell et al., 2008; Bharath and Shumway, 2008). Our main data

source for realized cyberattacks is the Privacy Rights Clearinghouse database.

Our approach consists of the following steps. At each forecast origin q, we estimate a logistic regression using only information available strictly prior to that origin. The dependent variable, $\mathrm{CyberAttack}_{i,t+k}$, equals unity if a firm experiences a cyberattack within the subsequent k quarters (where k is the forecast horizon, e.g. $k = 1$ or $k = 4$), and zero otherwise. The main independent variable is $\mathrm{CRExposure}_{i,t}$ as of time *t*. The regression also includes a vector of contemporaneous controls: firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta.[12] We include industry fixed effects to absorb permanent differences in cyberattack propensity across sectors but exclude time fixed effects so as not to absorb the aggregate time variation the model is intended to forecast.

The above regression is estimated recursively on an expanding training window that begins with a minimum of 24 quarters of historical data; for a forecast origin q the training sample therefore excludes any observation whose outcome depends on periods $q, q+1, \ldots, q+k-1$ (equivalently, the latest allowed training observation is $q-k$), which prevents look-ahead bias. The sample is restricted to US firms only. Finally, for each origin, we estimate the model, store the fitted coefficients, and compute out-of-sample predicted probabilities $\hat{p}_{i,q}$ for all firms observed at quarter q.

Using the set of out-of-sample predicted probabilities $\hat{p}_{i,q}$, we form decile portfolios each quarter. At a given origin q, the cross section of firms is sorted by $\hat{p}_{i,q}$ and partitioned into ten equal-sized bins (deciles). For each decile in each quarter we compute two quantities: (i) the average predicted probability within the decile and (ii) the realized frequency of attacks within the relevant forecast horizon. Aggregating these outcomes across all out-of-sample quarters yields the cross-sectional mapping between predicted risk and realized outcomes.

Figure 5 plots this mapping by placing predicted-probability deciles on the horizontal

[12] Table A.2 describes in detail how each variable is constructed.

axes and the realized fraction of firms experiencing an attack on the vertical axes. In Panels (a) and (b) the realized attack occurs in the following quarter or at anytime within the next four quarters, respectively. The dashed lines report the mean predicted probability in each decile, while the solid lines report the empirical attack rates. Monotonicity of the solid lines and close alignment between the dashed and solid lines across deciles indicate that our exposure measure can predict attacks out-of-sample rather well. In other words, cyber risk exposure not only captures contemporaneous or recent cyberattacks but also forecasts future incidents.

Table B.VI in the Online Appendix reports results from an in-sample prediction exercise. We now run regressions of $\mathrm{CyberAttack}_{\mathrm{i,t+k}}$, which is a cyberattack indicator based on PRC data, on measures of cyber risk exposure. The forecast horizon k takes on the values of 1, 4, or 8. In Panel (A) of the Table, the independent variable is $\mathbb{I}[\mathrm{CRExposure}_{\mathrm{i,t}} > 0]$, which captures the extensive margin of exposure. In Panel (B) of the Table, the independent variable is the regular frequency variable $\mathrm{CRExposure}_{\mathrm{i,t}}$. All regressions include an industry fixed effect, a time fixed effect, and some regressions also control for firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. We report the odds ratio which, if greater than unity, suggests that cyber risk exposure is a good predictor of realized cyber attacks. Across all specifications, the odds ratios are greater than unity, which suggests that $\mathrm{CRExposure}_{\mathrm{i,t}}$ can also predict cyberattacks in-sample.

3.3 Comparison with Other Indices of Cyber Risk

There are two further potential issues with our measures that are based on earnings calls. First, earnings calls could be not representative of the general attention to and uncertainty about various risk factors. Second, earnings calls could be capturing the attention to specific topics by analysts and not any information discovery about *fundamental* risk factors. It is therefore useful to externally validate our exposure measure by benchmarking

it against several external sources.

We proceed by comparing the time-series average of $\mathrm{CRExposure}_{\mathrm{i,t}}$ with four independently generated measures. First, we obtain the cybersecurity risk index from Florackis et al. (2023). This index is based on firms' 10-K filings. Second, using data from Factiva, we run a search query for the word "cyber" and all of its derivatives for two major U.S. newspapers: The New York Times and The Washington Post. Third, we estimate worldwide interest in the keyword "cyber risk" using Google Trends data. Fourth and finally, we use the number of reported cyberattacks from the Privacy Rights Clearinghouse dataset as a proxy for fundamental cyber risk.

Figure 6 presents the external validation exercise by plotting the standardized time series of our cyber-risk measure with four benchmark indices in separate panels. Across all comparisons, the Figure shows that our measure co-moves closely with these four proxies. In particular, the upward trends are very similar quantitatively. This evidence indicates, first, that earnings calls do not have an unusually high coverage of cyber risk. Second, the strong association with realized cyberattack activity suggests that our measure captures underlying, fundamental variation in economy-wide cyber risk rather than merely reflecting analysts' attention, shifting sentiment, or other non-fundamental sources of noise.

3.4 Case Studies

The final validation test of our baseline cyber risk exposure measure is case study analysis. Can our measure pick up salient incidents at the granular level? We discuss six well-known historical firm-level cyberattacks.

First, in 2017, the American credit bureau Equifax reported that private records of about 150 million American and 15 million British citizens were stolen. To this day, the Equifax breach remains one of the biggest data compromises in history. Second, the 2013 Adobe data compromise where it was believed that usernames and encrypted passwords

had been stolen from about 38 million of the company's active users.[13] Third, the 2013 Target data breach that affected 40+ million customers. The company was forced to pay an $18.5 million multi-state settlement, the largest ever for a data breach at the time.[14]

Fourth, the 2014 Home Depot data breach which forced the firm to pay a $17.5 million settlement to resolve a multi-state probe into the breach where hackers accessed payment card data belonging to 40 million customers.[15] Fifth, the 2018-2019 Marriott Hotels cyber incident, which led the UK's data privacy watchdog to fine the Marriott Hotels chain £18.4m for a major data breach that could have affected up to 339 million guests.[16] Finally, the 2020-2021 SolarWinds cyberattack where advanced persistent threat (APT) actors infiltrated the supply chain of SolarWinds, inserting a backdoor into the product of the software developer. In January 2021, a class action lawsuit was filed against SolarWinds in relation to its security failures and subsequent fall in the share price.[17]

Figure 7 depicts the dynamic of (standardized) $\mathrm{CRExposure}_{\mathrm{i,t}}$ for the six aforementioned cyberattacked firms. We notice that the index correctly captures the exact timing of each incident. For example, it spikes by one or more standard deviations for Equifax in 2017, Hope Depot in 2015, or Target in 2013.

4 The Nature of Firm-level Cyber Risk

In this Section, we run two exercises in order to quantify and explain the nature of the variation in cyber risk at the firm level. First, we provide a variance decomposition of $\mathrm{CRExposure}_{\mathrm{i,t}}$ into its aggregate, sector-level, country-level, and firm-level components. Second, we ask which firm-level characteristics are most closely associated with high levels of $\mathrm{CRExposure}_{\mathrm{i,t}}$.

[13] https://www.bbc.co.uk/news/technology-24740873

[14] https://eu.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

[15] https://www.reuters.com/article/us-home-depot-cyber-settlement-idUSKBN2842W5

[16] https://www.bbc.co.uk/news/technology-54748843

[17] https://www.cisecurity.org/solarwinds

4.1 Variance Decomposition Analysis

Previous discussions have revealed that cyber risk exposure has clear aggregate, country-level, and industry-level patterns. We now formally quantify the statistical importance of the aggregate, industry-level, country-level, and firm-level variation in exposure. Table III reports the incremental R^2 from regressions of cyber risk exposure on various fixed effects. We consider our baseline measure, $\mathrm{CRExposure_{i,t}}$, as well as the four sub-indices that decompose it by earnings call section and speaker.

The time fixed effect provides little explanatory power: at most 5.76% of the total variation in cyber risk exposure. In contrast, the industry component is sizable as the incremental R^2 can be as high as 18.44%. This is consistent with the notion that certain sectors like IT and finance are systematically more exposed to cyber due to the nature of their businesses. The country fixed effect explains a small fraction of the total variation. This observation is reassuring and suggests that our approach is not seriously affected by persistent country-level factors such as local language or regulations. The interaction between sectoral and time fixed effects accounts for at most 1.59% of the total variation.

Across the five exposure measures, the fraction of the total variation that is left unexplained by the above fixed effects is in the 73%-90% range (74% for the baseline $\mathrm{CRExposure_{i,t}}$ measure). We can further decompose the firm-level residual into a firm fixed effect and the non-persistent component, namely the identity of firms affected by the exposure measure. Permanent differences across firms within sectors explain at most 39.7% of the total variation in exposure. The remaining 34.3%, i.e. a third of the total variation and roughly half of the firm-level variation, stems from time-varying firm characteristics. These results suggest that the main driver of the observed variation in our measures is firms' idiosyncratic exposure to cyber risk exposure.

4.2 Determinants of Firm-Level Cyber Risk Exposure

We have established that firm-level variation in cyber risk exposure is significant. What are the determinants of this variation? In order to answer this question, we assemble an array of firm-level balance sheet and income statement variables including firm size, market beta, intangible assets ratio, liquidity ratio, Tobin's Q, CAPEX ratio, cash flow ratio, (log) firm age, book to market ratio, leverage ratio, PP&E ratio, debt maturity ratio, equity issuance ratio, turnover ratio, and operational costs ratio. Table A.2 describes in detail how each variable is constructed.

Table IV reports the results from linear regressions of cyber risk exposure measures on these firm-level variables. Every specification also includes either an industry x time or country x time fixed effect. Overall, we see that firms which have greater exposure to cyber risk typically fit into the following profile: high ratio of intangible assets to total assets, high liquidity, high growth opportunities (as proxied by Tobin's Q), and large size (as measured by total assets). These characteristics seem to be recurring across studies who look at determinants of cyberattacks or exposure (Kamiya et al., 2021; Florackis et al., 2023). In terms of explanatory power, the pseudo-R^2 of our regressions is at most 0.306; a large fraction of cyber risk exposure is left unexplained.

In the Online Appendix, we provide three sets of additional results where we explore differences by earnings call agent and section, by region, and by industry. Tables B.VII, B.VIII, and B.IX, report those results. While there is rich heterogeneity along these dimensions, firm size and liquidity appear to be among the more consistent predictors of high exposure across sectors and regions.

5 Cyber Risk Exposure and Firm-level Implications

In this section, we study the firm-level economic implications of cyber risk exposure. We look at the effects on the stock market, the option market, and firm balance sheets.

5.1 Stock Market Effects

The first test of economic significance is whether our measures of cyber risk exposure have any meaningful effects on firms' stock market performance. Recall that $\mathrm{CRExposure}_{i,t}$ does not merely pick up realized cyber incidents. It is also a forward-looking measure, implying a heightened likelihood of a future cybersecurity crisis or event. This uncertainty alone can affect asset prices today. To test this theory, we run quarterly firm-level regressions of average stock returns ($\mathrm{Ret}_{i,t}$), cumulative stock returns ($\mathrm{CRet}_{i,t}$), and realized stock market volatility ($\mathrm{RV}_{i,t}$) on $\mathrm{CRExposure}_{i,t}$. All variables have been standardized to have a mean of zero and standard deviation of unity. Every specification includes either an industry x time or country x time fixed effect. Every specification controls for firm size, (log) age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed definitions of every variable.

Results are reported in Table V. First, we find that $\mathrm{CRExposure}_{i,t}$ has negative and significant effects on stock returns, as can be seen from columns (1)-(4). Both average and cumulative quarterly returns are low when cyber risk exposure is high. A one standard-deviation increase in $\mathrm{CRExposure}_{i,t}$ lowers returns by around 1% of the dependent variables' standard deviation. Similar magnitudes have been obtained elsewhere in the literature (Kamiya et al., 2021; Tosun, 2021). Second, $\mathrm{CRExposure}_{i,t}$ is positively associated with realized stock market volatility. The effect is statistically significant and in the order of 2% of the dependent variable's standard deviation. The observation that cyber risk exposure is associated with elevated volatility is an additional validation of our measure.

While our benchmark specification is for the main measure $\mathrm{CRExposure}_{i,t}$, we can estimate the same relationships with our four compositional indices. Table B.X reports the results for $\mathrm{CRexposure}^{\mathrm{Pres}}_{i,t}$ and $\mathrm{CRexposure}^{\mathrm{Q\&A}}_{i,t}$, and Table B.XI reports the results for $\mathrm{CRexposure}^{\mathrm{Exec}}_{i,t}$ and $\mathrm{CRexposure}^{\mathrm{Part}}_{i,t}$. Columns (1)-(2) in each table show that the main result is concentrated in the presentation section and speeches by firm executives. The

estimates $\text{CRexposure}_{i,t}^{Q\&A}$ are still borderline statistically significant. The estimates for $\text{CRExposure}_{i,t}^{Part}$ are not significant for returns but are for realized volatility.

5.2 Option Market Effects

We now turn to firm-level effects of cyber risk exposure on the option market. We run regressions on $\text{CRExposure}_{i,t}$ of the three main option market measures: implied volatility ($\text{IV}_{i,t}$), variance risk premium ($\text{VRP}_{i,t}$), and implied volatility slope ($\text{SlopeD}_{i,t}$). Recall that these three variables capture premia for protection against price, variance, and tail risks. Our main specification focuses on 91-day options with results on additional maturities available in the Appendix. All variables have been standardized to have a mean of zero and standard deviation of unity. Every specification includes either an industry x time or country x time fixed effect. Every specification controls for firm size, (log) age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed definitions of every variable.

Table VI reports the results. Cyber risk exposure has positive and significant effects on all three option market indicators. A one standard-deviation increase in $\text{CRExposure}_{i,t}$ increases $\text{IV}_{i,t}$, $\text{VRP}_{i,t}$, and $\text{SlopeD}_{i,t}$ by roughly 5%, 4% and 3% of the variables' standard deviations, respectively. These effects are quantitatively in the same range as what Hassan et al. (2019) find in the case of political risk and Sautner et al. (2023) find in the case of climate-change risk.

We now mitigate a concern that outlier observations, such as significant cyberattacks, drive these results. Figure A.4 in the Online Appendix plots binned scatter plots of the effects of $\text{CRExposure}_{i,t}$ on $\text{IV}_{i,t}$, $\text{VRP}_{i,t}$, and $\text{SlopeD}_{i,t}$. These plots are generated from regression specifications that include an industry x time fixed effect and the same firm controls. Each panel presents 100 equally-sized bins and lines of best fit. From panels (a)-(c), it is clear that the option market effects are not driven by outliers.

While our benchmark specification is for the main measure $\text{CRExposure}_{i,t}$, we can again

estimate the same relationships for our four compositional indices. Table B.X reports the results for $\text{CRexposure}_{i,t}^{\text{Pres}}$ and $\text{CRexposure}_{i,t}^{\text{Q\&A}}$, and Table B.XI reports the results for $\text{CRexposure}_{i,t}^{\text{Exec}}$ and $\text{CRexposure}_{i,t}^{\text{Part}}$. Columns (3)-(5) in each table show that the main result is not uniquely driven by any particular section or participant type. All estimates are statistically significant, although the point estimates are larger for $\text{CRexposure}_{i,t}^{\text{Pres}}$ and $\text{CRexposure}_{i,t}^{\text{Exec}}$ than $\text{CRexposure}_{i,t}^{\text{Q\&A}}$ and $\text{CRexposure}_{i,t}^{\text{Part}}$, respectively.

Our benchmark specification considers contemporaneous relationships between option market variables and cyber risk exposure. We now ask if the estimated effects are persistent. To this end, we estimate lag-augmented local projections in the spirit of Jordà (2005) and Montiel Olea and Plagborg-Møller (2021). The dependent variables are $\text{IV}_{i,t+h}$, $\text{VRP}_{i,t+h}$, and $\text{SlopeD}_{i,t+h}$, where h is a horizon that ranges from 0 to 12 quarters. Specifications include industry x time fixed effects and control for two lags of the dependent variable, two lags of $\text{CRExposure}_{i,t}$, and two lags of every firm control variable. Figure A.5 in the Online Appendix presents the results by plotting point estimates along with 68% and 90% confidence bands. Panels (a)-(c) show that the effects of cyber risk exposure on option market variables are persistent and can last for up to 12 quarters. One potential economic mechanism for this propagation result is laid out in Akey et al. (2024) and centers around the role of corporate reputation. High exposure to cyber risk constitutes a negative change to the firm's reputational capital, which takes time to re-build. This, in turn, causes prolonged increases in option market premia and, as we will see in the next section, decline in profitability.

5.3 Balance Sheet Effects

We now ask whether cyber risk exposure drives economic outcomes of firms beyond stock prices or option market premia. To this end, we run regressions of firms' return on assets ($\text{RoA}_{i,t}$), cash flow / assets ratio ($\text{CashFLow}_{i,t}$), and the S&P credit rating ($\text{Rating}_{i,t}$) on our baseline measure $\text{CRExposure}_{i,t}$. As before, all variables have been standardized to have

a mean of zero and standard deviation of unity. Every specification includes either an industry x time or country x time fixed effect. Every specification controls for firm size, (log) age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed definitions of every variable.

Table VII reports the results of this exercise. $\mathrm{CRExposure_{i,t}}$ is negatively associated with firm profitability, cash flow, and credit ratings. A one standard-deviation increase in $\mathrm{CRExposure_{i,t}}$ lowers $\mathrm{RoA_{i,t}}$, $\mathrm{CashFlow_{i,t}}$, and $\mathrm{Rating_{i,t}}$ by around 10%, 9%, and 10% of the variables' standard deviations. Panel (d) of Figure A.4 in the Online Appendix plots the binned scatter plot for the relationship between $\mathrm{RoA_{i,t}}$ and $\mathrm{CRExposure_{i,t}}$. As before, this specification includes an industry x time fixed effect and the usual firm controls. The negative association between firm profitability and cyber risk exposure is economically significant and not driven by outliers.

Table B.X in the Online Appendix reports the results for $\mathrm{CRexposure^{Pres}_{i,t}}$ and $\mathrm{CRexposure^{Q\&A}_{i,t}}$, and Table B.XI reports the results for $\mathrm{CRexposure^{Exec}_{i,t}}$ and $\mathrm{CRexposure^{Part}_{i,t}}$. Columns (6) in each table show that the effect on $\mathrm{RoA_{i,t}}$ is always statistically significant but marginally stronger for the Q&A session and firm executives.

We also estimate the dynamic effects of cyber risk exposure on profitability. Panel (d) in Figure A.5 presents the results from our local projection specification that includes an industry x time fixed effect and controls for two lags of the dependent variable, two lags of $\mathrm{CRExposure_{i,t}}$, and two lags of every firm control variable. The effect on $\mathrm{RoA_{i,t+h}}$ is persistently negative and significant for up to 12 quarters.

We can now compute the aggregate effects of cyber risk exposure on the full sample of firms. A one-standard deviation swing in $\mathrm{RoA_{i,t}}$ in our sample is roughly 3.35%. Given the point estimate for $\mathrm{RoA_{i,t}}$ of around 0.1, this translates into an $\mathrm{RoA_{i,t}}$ decline of the order of 0.34% (percentage points) for the average firm. The average firm in the sample possesses assets of about \$28,066M. This yields a loss of income for the average firm of \$95 million. To compute the loss of income for the aggregate economy we have to make some rough

assumptions. The number of unique firms in our estimation sample (i.e. after merging StreetEvents with Compustat and performing all the data cleaning steps) for which the value of total assets is not missing is 3,003. Thus, for the aggregate economy—which is approximated by our sample—the total loss in response to a one-standard deviation rise in cyber risk exposure is about $285 billion per quarter or $1.14 trillion per year.

According to Dreyer et al. (2018), the global cost of cyber risk is estimated to range from approximately $275 billion to $6.6 trillion in terms of gross domestic product (GDP) losses. Bouveret (2018) reports that the annual average loss from cyber risk amounts to about $100 billion for banks alone. Our aggregate estimate of roughly $1.1 trillion per year therefore lies well within the range of existing assessments. Importantly, unlike studies that focus on realized cyber incidents, our estimates capture the broader exposure to cyber risk—that is, the valuation effects associated with the perceived vulnerability and exposure to such changes.

In summary, in this section we have shown cyber risk exposure has significant and lasting firm-level implications. It is priced in the stock and option markets and is associated with lower cash flows and returns. This finding is consistent with a theory that links cyber risk exposure at present times with probabilities of future realized attacks and related monetary or reputational damages through forward-looking variables such as risk premia in the option market.

6 Cyber Risk Exposure and Systemic Implications

In this section, we move beyond the firm level and study the systemic implications of cyber risk exposure. We look at industry-level and spillover effects.

6.1 Industry-level Effects

Does firm-level cyber risk exposure wash out at the industry level? We now aggregate all variables to the level of a six-digit NAICS sector.[18] The main regressors of interest are now $\mathrm{CRExposure}^{\mathrm{u}}_{\mathrm{s,t}}$ and $\mathrm{CRExposure}^{\mathrm{w}}_{\mathrm{s,t}}$. The former is an unweighted sector-level average while the latter is the firm size-weighted sector-level average. Similarly, we construct equally- and size-weighted averages of all usual dependent variables and firm controls. All specifications include a country x time fixed effect.

Table VIII reports the results. Even at the industry level, cyber risk exposure is negatively associated with stock returns and profitability, and positively associated with realized stock market volatility, option-implied volatility, the variance risk premium, and the implied volatility slope. These relationships hold under both equal- and size-weighted aggregation approaches. A one–standard deviation increase in $\mathrm{CRExposure}^{\mathrm{u}}\mathrm{s,t}$ is associated with changes in $\mathrm{CRet}^{\mathrm{u}}\mathrm{s,t}$, $\mathrm{RV}^{\mathrm{u}}_{\mathrm{s,t}}$, $\mathrm{IV}^{\mathrm{u}}_{\mathrm{s,t}}$, $\mathrm{VRP}^{\mathrm{u}}_{\mathrm{s,t}}$, $\mathrm{SlopeD}^{\mathrm{u}}_{\mathrm{s,t}}$, and $\mathrm{RoA}^{\mathrm{u}}_{\mathrm{s,t}}$ of 2.0%, 3.4%, 5.8%, 3.7%, 4.9%, and 9.0% of their respective standard deviations, respectively. These findings suggest that the relevance of cyber risk exposure extends beyond firm-level effects to industry-level aggregate outcomes.

6.2 Spillover Effects

Can idiosyncratic, firm-level cyber risk exposure spill over across firms and generate systemic, ripple effects? Crosignani et al. (2023) have documented that cyberattack-driven disruptions propagate across supply chains. Eisenbach et al. (2022) reach a similar conclusion but in the context of the U.S. wholesale payments network. Kotidis and Schreft (2025) have shown that, via contagion, a cyberattack can indirectly impact financial firms that are not directly exposed to the attack themselves. Florackis et al. (2023) have estimated the spillover effects of the high-profile SolarWinds hack from the affected, customer firms and on the unaffected, non-customer firms. Our focus here is on the propagation through

[18] Our sample includes 603 unique industries.

financial markets. Our empirical strategy attempts to trace out the indirect, spillover effects of cyber risk exposure on firms that are not impacted directly but are "connected" to the exposed firms because they belong to the same tightly defined industry, and could thus be affected by association. In other words, we conjecture that financial markets begin to perceive certain firms as being operationally risky if new information about cyber risk exposure of their *peers* gets revealed to the public.

Specifically, affected firms are defined as those with a $\mathrm{CRExposure}_{i,t}$ of greater than x, where x is a threshold. This definition of unaffected peers follows the literature (Garg, 2020). The unaffected firms are defined as those that are headquartered in the same country and operate in the same six-digit NAICS industry as their affected peer but exhibit $\mathrm{CRExposure}_{i,t}$ of less than or equal to x. For the baseline threshold x, we choose the median of the $\mathrm{CRExposure}_{i,t}$ distribution in order to account for any possibility of measurement error. The median corresponds to around 9 counts in the sample. Our results do not change if we set x to alternative values, such as zero or the mean. All specifications include a country x time fixed effect and the usual set of controls.

Table IX reports the results. Panels (A) and (B) present the estimates for affected and unaffected firms, respectively. Two main observations emerge from this analysis. First, the direct effects are positive and statistically significant, consistent with our earlier firm-level findings. Second, cyber risk exposure significantly influences the profitability, stock market, and option market variables of unaffected firms. This evidence points to the presence of spillover effects: unaffected firms—those with little to no direct cyber risk exposure nonetheless experience higher costs of protection against price, variance, and downside market risks, as well as lower stock returns and profitability. An important caveat is that these results pertain to firm-specific, idiosyncratic exposures that generate spillovers. Correlated shocks—those that affect multiple firms simultaneously (e.g., a global cyberattack or a state-sponsored hacking campaign)—could have far more pronounced systemic implications.

7 Additional Results and Robustness Checks

This section lists tests of robustness of our main empirical findings. First, we control for additional variables in our firm-level regressions and run robustness tests excluding select industries. Second, we ask whether firm-level effects are driven more by the firm-level or aggregate cyber risk exposure. Third, we replicate our main regressions on options of different maturities to confirm that our results are not driven only by 91-day options. Fourth, we re-run our main analysis on two alternative samples: only for US firms and for the sample ending in 2020Q1. Fifth and finally, we run placebo exercises where we randomly re-assign the main regressor within a quarter and across firms.

Additional Controls. One concern with our benchmark firm-level estimations is omitted variable bias. First, our results could be driven by exposure to other risk factors, such as political risk or epidemic diseases. Recall that the time-series average of $\mathrm{CRExposure_{i,t}}$ peaked during the COVID-19 pandemic. Second, firms could be actively managing cyber risk exposure with spending on research and development or operational risk management. To address these issues, we now explicitly control for firm-level political risk exposure from Hassan et al. (2019), firm-level epidemic disease exposure from Hassan et al. (2023a), as well as the firm-level R&D expenditure to asset ratio and operational cost to asset ratio. Tables B.XII and B.XIII in the Online Appendix report the results for the main stock market, option market, and balance sheet outcomes. Results do not change.

Excluding IT and Financial Firms. Section 2.3 has shown that the incidence of cyber risk exposure is heterogeneous across industries. It is also plausible that the elasticity of exposure with respect to firm-level outcomes varies by sector. For example, while some firms may be adversely affected by rising cyber risk, others—such as IT firms—could benefit. Moreover, our measure may matter disproportionately more for the financial sector.

To address these possibilities, we conduct an additional robustness exercise in which we re-estimate our main regressions after excluding selected sectors. First, we remove all IT firms (NAICS 51). Second, we remove all financial firms (NAICS 52). Table B.XIV in the Online Appendix reports the results. Panel (A) shows that excluding IT firms, if anything, strengthens our estimates. This finding is consistent with the notion that the economic impact of rising cyber risk is not uniformly negative for all firms. Panel (B) shows that excluding financial firms has no meaningful effect on the results, indicating that our main findings are not driven solely by financial intermediaries.

Firm-level or Aggregate Cyber Risk. In Section 4.1, we have shown that the bulk of the total variation in $\mathrm{CRExposure}_{i,t}$ originates at the firm level. We now confirm, in a complementary exercise, that our main results are robust to the presence of aggregate cyber risk. Specifically, we aggregate $\mathrm{CRExposure}_{i,t}$ to the quarterly level and include this aggregate measure in our baseline firm-level regressions. All specifications include industry fixed effects and the usual set of firm-level controls. Table B.XV in the Online Appendix reports the results. Panels (A) and (B) present the estimates for $\mathrm{CRet}_{i,t}$, $\mathrm{RV}_{i,t}$, and $\mathrm{IV}_{i,t}$, and for $\mathrm{VRP}_{i,t}$, $\mathrm{SlopeD}_{i,t}$, and $\mathrm{RoA}_{i,t}$, respectively. In columns (2), (4), and (6), we additionally control for the cross-sectional mean of $\mathrm{CRExposure}_{i,t}$. Including this aggregate measure reduces the point estimates on $\mathrm{CRExposure}_{i,t}$ across all specifications, but they remain statistically significant at the 1% level. While the time-series component of exposure is relevant, it never dominates the firm-level variation.

Different Option Maturities. Are our baseline firm-level estimates robust to different option maturities? Table B.XVI reports the estimates from firm-level regressions for 30-day, 60-day, 182-day, and 365-day options. Results are presented for the benchmark exposure measure $\mathrm{CRExposure}_{i,t}$ and the main option market outcomes. Results do not change as all of the coefficients remain statistically and economically significant.

Alternative Samples. It is important to gauge the extent to which our main results are driven by US and non-US firms. In addition, cyber risk peaked globally during the COVID-19 pandemic—a period characterized by an unprecedented surge in attempted cyberattacks. Table B.XVII reports robustness regressions that are restricted to U.S. firms and to a subsample ending in 2020Q1. Results remain quantitatively unchanged, suggesting that our findings are not driven by non-U.S. firms or by the last several years of the sample.

Placebo Tests. Our final robustness test is a falsification exercise based on placebo regressions for our main firm-level specifications. Specifically, we regress firm-level stock market, option market, and balance sheet outcome variables on $\mathrm{CRExposure}_{\mathrm{i,t}}$, where $\mathrm{CRExposure}_{\mathrm{i,t}}$ has been randomly re-assigned within each quarter and across firms with replacement. Figure A.6 displays histograms of the resulting t-statistics from 1,000 regressions. In all four panels, the distributions are centered around zero and are approximately symmetric. The fraction of false-positive and false-negative cases—defined using a two-sided 95% confidence interval—is around 2.5%. We conclude that obtaining our baseline results by pure chance is highly unlikely.

8 Conclusion

Automation, disruptive technologies such as cloud computing, the rise of decentralized finance, and the work-from-home revolution are among the many factors that have rapidly increased the likelihood of both idiosyncratic and systemic cyberattacks. Uncertainty surrounding *exposure* to future attacks is difficult to quantify, primarily because of measurement challenges. Reliance on reported cyber incidents is an imperfect solution for reasons well documented in the existing literature. New approaches to measuring cyber risk are therefore required.

In this paper, we propose one such approach by leveraging tools from natural language

processing and the textual content of quarterly earnings calls of publicly listed firms to construct a quarterly firm-level text-based measure of cyber risk exposure. Our measure draws on term libraries assembled by three reputable institutions and is extensively validated through human and large language model audits, case-study analyses, and comparisons with multiple external indices of cyber risk. The validated measure forecasts actual cyberattacks out of sample, is priced in equity markets, affects premia in option markets, and is associated with lower profitability. Using simple back-of-the-envelope calculations, we estimate that the aggregate cost of cyber risk exposure exceeds one trillion dollars in annual net income losses.

We move beyond firm-level analysis and show that idiosyncratic cyber risk can have potential systemic implications. Firm-level exposure does not wash out in the aggregate and exerts economically significant effects at the industry level. Moreover, the effects of cyber risk exposure spill over across firms: affected firms exert a negative impact on their peers—defined as firms operating in the same country and industry. Financial markets therefore act as channels through which firm-level cyber risk exposure propagates, amplifying individual incidents and giving rise to systemic risk–type effects.

Our results open several avenues for future research. First, all our exposure measures are publicly available and could be used to explore novel effects of cyber risk on employment and other real economic aggregates. Second, future work could investigate links between cyber risk and the cryptocurrency ecosystem. Finally, our measures could help calibrate a new generation of economic models designed to quantify the welfare costs of cyber risk based on observed firm-level variation.

A Appendix

Table A.1: Cyber Risk Exposure Keywords

This table reports cybersecurity-related keywords—and their sources—that constitute the dictionary set $\mathbb{C}$ from main text. All keywords have been concatenated into single words for readability.

Source	Keyword
Predefined Dictionary	access, accesscontrol, accountability, activeattack, activecontent, adversary, airgap, alert, antispyware, antispywaresoftware, antivirus, antivirussoftware, app, asset, attacker, attackmethod, attackmode, attackpath, attackpattern, attacksignature, attacksurface, authenticate, authenticity, authentification, authorization, availability, behaviormonitoring, blacklist, blueteam, bot, botnet, breach, bug, byod, certificate, cipher, cloud, cloudcomputing, compromise, computerforensics, computersecurity, confidentiality, credentials, criticalinfrastructure, cyber, cyberadvisory, cyberalert, cyberattack, cyberecosystem, cyberevent, cyberexercise, cyberincident, cyberinfrastructure, cyberoperations, cyberresilience, cyberrisk, cybersecurity, cyberspace, cyberthreat, dataadministration, dataaggregation, dataarchitecture, databreach, dataintegrity, datamining, datarecovery, datatheft, decode, decrypt, decryption, detection, digitalfootprint, digitalforensics, digitalsignature, disruption, electronicsignature, encipher, encode, encrypt, encryption, exfiltration, exploit, exposure, firewall, forensics, hacker, hashing, hazard, honeypot, ict, incident, incidentmanagement, incidentresponse, informationassurance, informationcompliance, informationrecovery, informationsecurity, informationsharing, informationsystem, informationtechnology, insiderthreat, intrusion, intrusiondetection, iot, itasset, macrovirus, maliciouscode, maliciousemail, maliciousmessage, malvertising, malware, network, networkresilience, networkservices, operationalexercise, operationalrisk, operationstechnology, password, patching, patchmanagement, penetrationtesting, pharming, phishing, plaintext, precursor, privacy, privatekey, publickey, ransomware, router, saas, secretkey, securityarchitecture, securityautomation, securitybreach, securityengineering, securityevent, securityincident, securitymanagement, securitypolicy, securityprogram, securitysystems, situationalawareness, smishing, socialengineering, softwareassurance, spam, spearphishing, spillage, spoofing, spyware, systemadministration, systemintegrity, systemintrusion, tabletopexercise, threatactor, threatanalysis, threatassessment, threatintelligence, threatvector, trojan, trojanhorse, unauthorizedaccess, verification, virus, vpn, vulnerability, vulnerabilityassessment, vulnerabilitymanagement, whaling, whitelist, zeroday
Keyword Discovery Algorithm	accessmanagement, blackhat, cardbreach, cardfraud, cardloss, collectionoperation, computer, computerincident, computernetwork, cybercrime, cyberinsurance, cybersecurityincident, cybersystems, data, databreaches, datacenter, datacompromise, datafraud, dataleak, dataloss, dataprivacy, datasecurity, ddos, ddosattack, ddosattacks, digital, disclosure, domain, emailcompromise, fraudulentactivity, gdpr, hack, hacked, hacking, identifyinginformation, identityfraud, identitymanagement, identitytheft, informationbreach, informationcommunication, informationintegrity, informationleak, informationplatform, informationpolicy, informationtheft, insiderrisk, interruption, ipaddress, irregularoperations, login, maliciousattack, networkintegrity, networksecurity, operationaldisruption, operationalevent, operationalincident, personaldata, personalidentifying, personalinformation, privacyconcerns, ransomwareattack, securitybreaches, securityrisk, servicedisruption, software, systemarchitecture, systemdevelopment, systemoutage, threatdetection, unauthorized, unauthorizeddisclosure, username, wannacry, whitehat, worm

Table A.2: Variable Definitions

Variable	Definition	Coverage
CRExposure	Relative frequency with which cybersecurity-related keywords appear in the transcripts of quarterly earnings calls. Defined as the number of sentences that contain at least one cybersecurity-related keyword and divided by the total number of sentences in the transcripts. Source: Thomson Reuters StreetEvents. Self-constructed.	2003Q1-2025Q3
$\text{CRExposure}^{\text{Pres}}$	Relative frequency with which cybersecurity-related keywords appear in the presentation part of transcripts of quarterly earnings calls. Defined as the number of sentences in the presentation that contain at least one cybersecurity-related keyword and divided by the total number of sentences in the presentation. Source: Thomson Reuters StreetEvents. Self-constructed.	2003Q1-2025Q3
$\text{CRExposure}^{\text{Q\&A}}$	Relative frequency with which cybersecurity-related keywords appear in the Q&A session part of transcripts of quarterly earnings calls. Defined as the number of sentences in the Q&A session that contain at least one cybersecurity-related keyword and divided by the total number of sentences in the Q&A session. Source: Thomson Reuters StreetEvents. Self-constructed.	2003Q1-2025Q3
$\text{CRExposure}^{\text{Exec}}$	Relative frequency with which cybersecurity-related keywords that are spoken by corporate executives appear in the transcripts of quarterly earnings calls. Defined as the number of sentences that contain at least one cybersecurity-related keyword spoken by executives and divided by the total number of sentences in the transcripts. Source: Thomson Reuters StreetEvents. Self-constructed.	2003Q1-2025Q3
$\text{CRExposure}^{\text{Ext}}$	Relative frequency with which cybersecurity-related keywords that are spoken by external participants appear in the transcripts of quarterly earnings calls. Defined as the number of sentences that contain at least one cybersecurity-related keyword spoken by external participants and divided by the total number of sentences in the transcripts. Source: Thomson Reuters StreetEvents. Self-constructed.	2003Q1-2025Q3
FLMWIndex	Time-series index of cybersecurity risk exposure in the texts of firms' 10-K files. Source: Florackis et al. (2023).	2007-2018
NewsIndex	Time-series index of cybersecurity risk exposure in the texts of The New York Times and The Washington Post. Defined as the number of articles in a quarter that contain any word that starts with "cyber" (including, for example, "cybersecurity" and "cyber-risk") and divided by the total number of articles in a quarter. Source: Factiva.	2003Q1-2024Q4
CyberAttack	An indicator variable that takes the value of unity for firms that have experienced a reported cyberattack, and zero otherwise. Source Privacy Rights Clearinghouse.	2003Q1-2025Q2
GoogleIndex	Time-series index of cybersecurity risk exposure based on Google Trends. Defined as the worldwide search interest, relative to the highest point, in the keyword "cyber risk". Source: Google Trends.	2004Q1-2024Q4
IV	Implied volatility of (log) returns computed from 91-day options. Quarterly measure is constructed by averaging daily values. Similar measures using 30-, 60-, and 182-day maturity options are constructed. Winsorized at the 1% level. Source: Ivy DB OptionMetrics Volatility Surface File.	2003Q1-2023Q3
VRP	Variance risk premium, defined as the daily difference between the implied variance of (log) returns (IV^2) from t to t+91 calendar days and realized variance of daily (log) returns over the same period (t, t+91). Quarterly measure is constructed by averaging daily values. Similar measures using 30-, 60-, and 182-day maturity options are constructed. Winsorized at the 1% level. Source: Ivy DB OptionMetrics Volatility Surface File.	2003Q1-2023Q3

Variable	Definition	Coverage
SlopeD	Slope of the function that relates implied volatility to the Black-Scholes delta for OTM put options (with deltas between -0.5 and -0.1) with a 91-day maturity. Similar measures using 30-, 60-, and 182-day maturity options are constructed. Winsorized at the 1% level. Source: Ivy DB OptionMetrics Volatility Surface File.	2003Q1-2023Q3
Ret	Average quarterly returns, computed as quarterly averages of daily (log) returns in CRSP. Winsorized at the 1% level. Source: CRSP.	2003Q1-2024Q4
CRet	Cumulative returns, computed as quarterly sums of (log) returns in CRSP. Winsorized at the 1% level. Source: CRSP.	2003Q1-2024Q4
RV	Realized volatility of (log) returns over the period of t and t+91 calendar days in CRSP. Winsorized at the 1% level. Source: CRSP.	2003Q1-2024Q4
Size	Total assets at the end of the quarter (in logs). ATQ variable in Compustat. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Age	Firm age (in logs) in Compustat. Self-constructed. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Tobin's Q	(Total assets (ATQ) - total common equity (CEQ) + share price (PRCCQ) $\times$ common shares outstanding (CSHOQ)) / total assets (ATQ). We drop observations with PRCCQ$\leq$1 (penny stocks) and >1000. We drop observations with Tobin's Q >1000. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Leverage	(Long term debt (DLTTQ) + debt in current liabilities (DLCQ)) / total assets. We drop observations with Leverage >1. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Liquidity	Cash and short-term investments (CHEQ) / total assets (ATQ). Winsorized at the 1% level. Coverage: Source: Compustat Global.	2003Q1-2025Q2
Intangibles / Assets	Intangible assets (INTANQ) / total assets (ATQ). We drop observations with Intangibles / Assets of >1. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Operational Costs / Assets	Operating expense (XOPRQ) / total assets (ATQ). Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Market Beta	Sensitivity of quarterly stock returns to quarterly S&P returns. For each firm and quarter, we run daily regressions of excess (log) returns on a constant and the market factor. For each firm x quarter combination, Market Beta corresponds to the estimated regression coefficient. Winsorized at the 1% level. Source: CRSP, Kenneth French's website.	2003Q1-2024Q4
RoA	Net income (NIQ) / total assets. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Cash Flow / Assets	(Income before extraordinary items (IBQ) + depreciation and amortization (DPQ)) / total assets (ATQ). We drop observations with Cash Flow / Assets of >1 or < -1. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Market Value	Market value (in logs). MKVALTQ in Compustat. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
S&P Rating	S&P quality ranking (SPCSRC variable in Compustat). Source: Compustat Global.	2003Q1-2025Q2
CAPEX / Assets	Invested capital (ICAPTQ) / total assets. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Book to Market Ratio	Total common equity / (share price $\times$ common shares outstanding). Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
PP&E / Assets	Property plant and equipment (PPENTQ) / total assets. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Debt Maturity Ratio	Long-term debt / (long-term debt + debt in current liabilities). Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2

Variable	Definition	Coverage
Valuation	Variable (mkvaltq), defined as stock price times common shares outstanding. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Equity Issuance Ratio	Common shares issued (CSHIQ) / total assets. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
Turnover Ratio	Sales (SALEQ) / total assets. We drop observations with SALEQ<0. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2
R&D costs / Assets	R&D expenses (xrdq) / total assets. Winsorized at the 1% level. Source: Compustat Global.	2003Q1-2025Q2

References

Adeney, R., J. Healey, P. Mosser, and D. M. Waiss (2022): "Cyber Risk and Financial Stability - An Atlas for Macroprudential Analysis," *Working Paper*.

Adrian, T. and C. Ferreira (2023): "Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards," *IMF Blog*.

Akey, P., S. Lewellen, I. Liskovich, and C. Schiller (2024): "Hacking Corporate Reputations," *SSRN Working Paper*, 3143740.

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach (2022): "The Drivers of Cyber Risk," *Journal of Financial Stability*, 60.

Amir, E., S. Levi, and T. Livne (2018): "Do firms underreport information on cyber-attacks? Evidence from capital markets," *Review of Accounting Studies*, 23.

Anand, K., C. Duley, and P. Gai (2022): "Cybersecurity and Financial Stability," *Deutsche Bundesbank Discussion Paper*, 08.

Anhert, T., M. Brolley, D. Cimon, and R. Riordan (2022): "Cyber security and ransomware in financial markets," *CEPR Discussion Paper 17403*.

Baker, S., N. Bloom, S. Davis, and A. Notes (2016): "Measuring Economic Policy Uncertainty," *Quarterly Journal of Economics*, 131, 1593–1636.

Bali, T. and H. Zhou (2016): "Risk, uncertainty, and expected returns," *Journal of Financial and Quantitative Analysis*, 707–735.

Beber, A. and M. Brandt (2006): "The effect of macroeconomic news on beliefs and preferences: Evidence from the options market," *Journal of Monetary Economics*, 53.

Bharath, S. T. and T. Shumway (2008): "Forecasting Default with the Merton Distance to Default Model," *The Review of Financial Studies*, 21, 1339–1369.

Biener, C., M. Eing, and J. H. Wirfs (2015): "Insurability of Cyber Risk: An Empirical Analysis," *The Geneva Papers on Risk and Insurance - Issues and Practice*, 40.

Bloom, N., T. Hassan, A. Kalyani, J. Lerner, and A. Tahoun (2025): "The Diffusion of New Technologies," *The Quarterly Journal of Economics*, 140, 1299–1365.

BoE (2020): "Bank of England Systemic Risk Survey," .

Bollerslev, T., G. Tauchen, and H. Zhou (2009): "Expected stock returns and variance risk premia," *The Review of Financial Studies*, 22, 4463–4492.

Bouveret, A. (2018): "Cyber risk for the financial sector: A framework for quantitative assessment," *IMF Working Paper 18/143*.

Campbell, J., J. Hilscher, and J. Szilagyi (2008): "In Search of Distress Risk," *The Journal of Finance*, 63, 2899–2939.

Carr, P. and L. Wu (2009): "Variance risk premiums," *The Review of Financial Studies*, 22, 1311–1341.

Chang, B., P. Christoffersen, and K. Jacobs (2013): "Market skewness risk and the cross section of stock returns," *Journal of Financial Economics*, 107.

Crosignani, M., M. Macchiavelli, and A. F. Silva (2023): "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains," *Journal of Financial Economics*, 147, 432–448.

Dreyer, P., T. M. Jones, K. Klima, J. Oberholtzer, A. S. and. J. Welburn, and Z. Winkelman (2018): "Estimating the Global Cost of Cyber Risk: Methodology and Examples," *RAND Corporation Research Report*.

Duffie, D. and J. Younger (2019): "Cyber Runs," *Hutchins Center Working Paper*, 51.

Eisenbach, T., A. Kovner, and M. J. Lee (2022): "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," *Journal of Financial Economics*, 145, 802–826.

Eling, M., R. Ibragimov, and D. Ning (2023): "Time Dynamics of Cyber Risk," *SSRN Working Paper*.

ESRB (2020): "Systemic Cyber Risk," *Report*, February.

Florackis, C., C. Louca, R. Michaely, and M. Weber (2023): "Cybersecurity Risk," *The Review of Financial Studies*, 36, 351–407.

Garg, P. (2020): "Cybersecurity breaches and cash holdings: Spillover effect," *Financial Management*, 49, 503–519.

Gentzkow, M., B. T. Kelly, and M. Taddy (2019): "Text as Data," *Journal of Economic Literature*, 57, 535–574.

Hassan, T., S. Hollander, L. v. Lent, and A. Tahoun (2019): "Firm-Level Political Risk: Measurement and Effects," *Quarterly Journal of Economics*, 134, 2135–2202.

——— (2023a): "Firm-Level Exposure to Epidemic Diseases: Covid-19, SARS, and H1N1," *The Review of Financial Studies*, 36, 4919–4964.

——— (2023b): "The Global Impact of Brexit Uncertainty," *The Journal of Finance*, 79, 413–458.

Hassan, T., J. Schreger, M. Schwedeler, and A. Tahoun (2023c): "Sources and Transmission of Country Risk," *Review of Economic Studies*, 91, 2307–2346.

Healey, J., P. Mosser, K. Rosen, and A. Wortman (2021): "The Ties That Bind: A Framework To Assess The Linkage Between Cyber Risks And Financial Stability," *Journal of Financial Transformation*, 53.

Hentschel, L. (2003): "Errors in implied volatility estimation," *Journal of Financial and Quantitative Analysis*, 38.

Hilscher, J., A. Raviv, and R. Reis (2022): "Inflating Away the Public Debt? An Empirical Assessment," *The Review of Financial Studies*, 35(3).

Hollander, S., M. Pronk, and E. Roelofsen (2010): "Does silence speak? An empirical analysis of disclosure choices during conference calls," *Journal of Accounting Research*, 48, 531–563.

Huang, A., R. Lehavy, A. Zang, and R. Zheng (2018): "Analyst information discovery and interpretation roles: A topic modeling approach," *Management Science*, 2833–2855.

Ilhan, E., Z. Sautner, and G. Vilkov (2021): "Carbon Tail Risk," *The Review of Financial Studies*, 34, 1540–1571.

Jiang, H., N. Khanna, and Q. Yang (2020): "The Cyber Risk Premium," *SSRN Working Paper 3637142*.

Jordà, Ó. (2005): "Estimation and Inference of Impulse Responses by Local Projections," *American Economic Review*, 95, 161–182.

Kamiya, S., J. Kang, J. Kim, A. Milidonis, and R. Stulz (2021): "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms," *Journal of Financial Economics*, 139, 719–749.

Kashyap, A. and A. Wetherilt (2019): "Some Principles for Regulating Cyber Risk," *AEA Papers and Proceedings*, 109, 482–487.

Kelly, B., L. Pastor, and P. Veronesi (2016): "The Price of Political Uncertainty: Theory and Evidence from the Option Market," *The Journal of Finance*, 71, 2417–2480.

Koijen, R., T. Philipson, and H. Uhlig (2016): "Financial health economics," *Econometrica*, 84, 195–242.

Kotidis, A. and S. L. Schreft (2025): "The Propagation of Cyberattacks through the Financial System: Evidence from an Actual Event," *The Journal of Finance*, 80, 3313–3358.

Lallie, H. S., L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens (2021): "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers Security*, 105.

Lhuissier, S. and F. Tripier (2021): "Measuring Cyber Risk," *Working Paper*.

Loughran, T. and B. McDonald (2011): "When is a liability not a liability? Textual analysis, dictionaries, and 10-Ks," *The Journal of Finance*, 66, 35–65.

——— (2016): "Textual analysis in accounting and finance: A survey," *Journal of Accounting Research*, 54(14).

Makridis, C. and B. Dean (2018): "Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities," *Journal of Economic and Social Measurement*, 43.

Montiel Olea, J. L. and M. Plagborg-Møller (2021): "Local Projection Inference Is Simpler and More Robust Than You Think," *Econometrica*, 89, 1789–1823.

Neuhierl, A. and M. Weber (2020): "Monetary policy communication, policy slope, and the stock market," *Journal of Monetary Economics*, 108, 140–155.

Pastor, L. and P. Veronesi (2013): "Political uncertainty and risk premia," *Journal of Financial Economics*, 110, 520–545.

Sautner, Z., L. van Lent, G. Vilkov, and R. Zhang (2023): "Firm-level climate change exposure," *The Journal of Finance*, 78, 1449–1498.

Tosun, O. K. (2021): "Cyber Attacks and Stock Market Activity," *International Review of Financial Analysis*, 76.

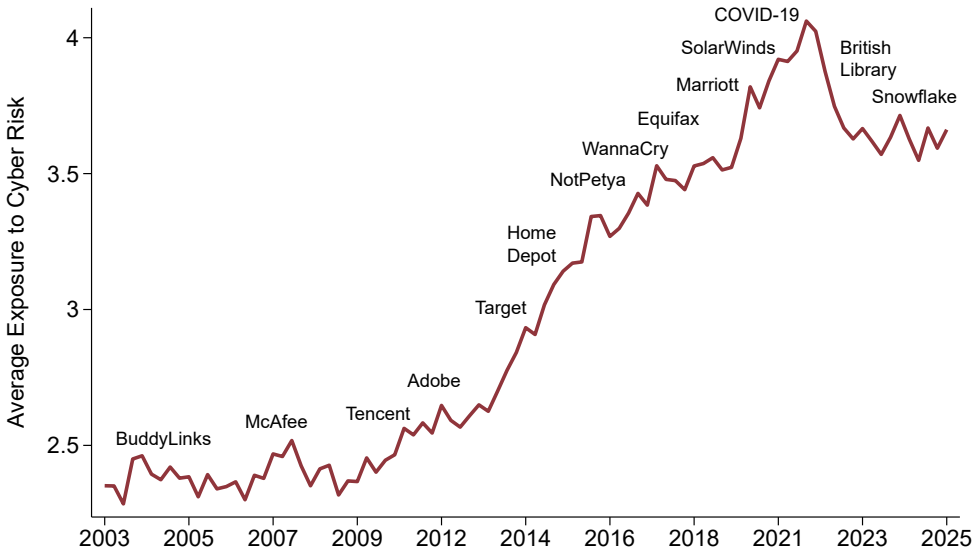
Vanden, J. M. (2008): "Information quality and options," *The Review of Financial Studies*, 21, 2635–2676.

WEF (2016): "Understanding Systemic Cyber Risk," *World Economic Forum: Global Agenda Council on Risk and Resilience*.

——— (2025): "The Global Risks Report 2025," *World Economic Forum*.

Woods, D., T. Moore, and A. Simpson (2019): "The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices," *Working Paper*.

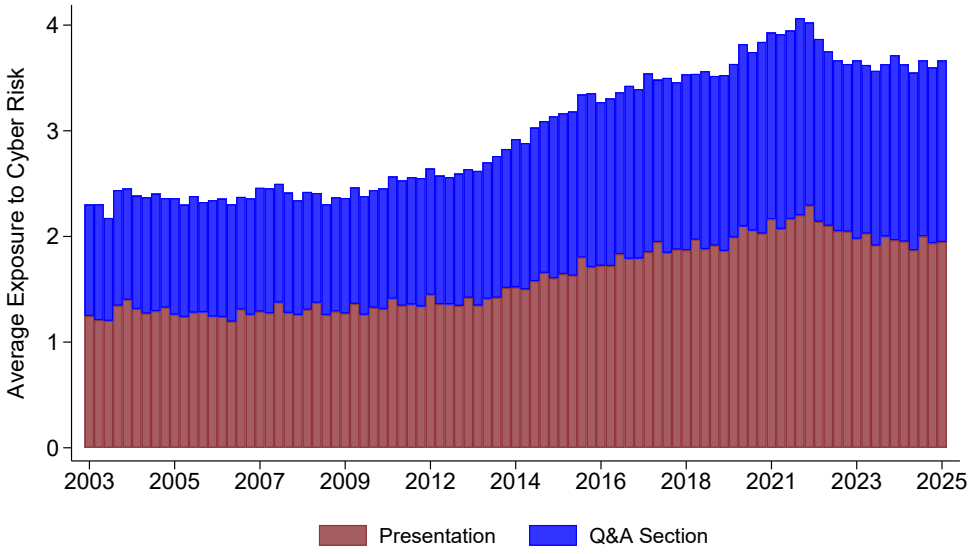
Figure 1: Average Cyber Risk Exposure over Time



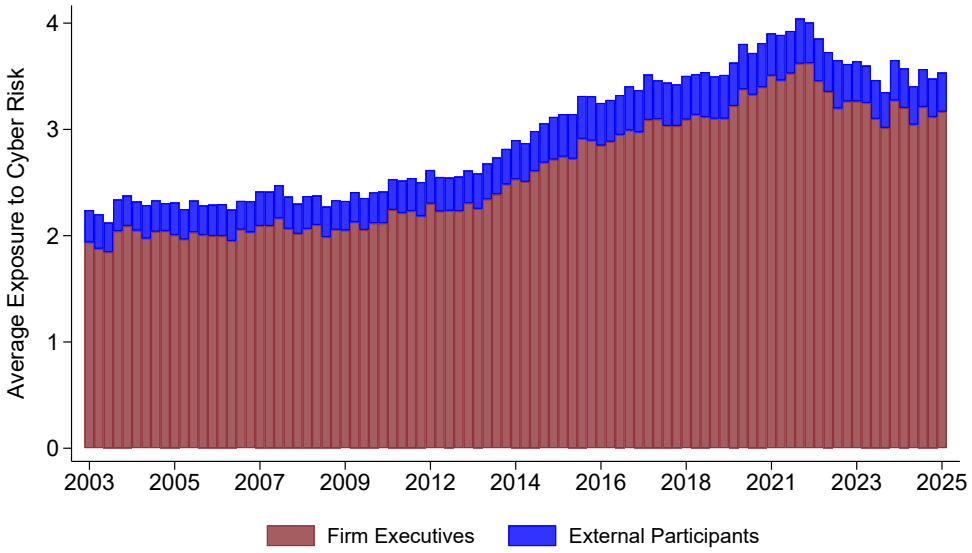
Notes: This figure plots the average of $\text{CRExposure}_{i,t}$ and notable cybersecurity-related incidents over time. CRExposure_{t} measures the relative frequency with which cyber risk exposure keywords get mentioned in the earnings calls. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions.

Figure 2: Cyber Risk Exposure by Earnings Call Section and Participant

(a) Section



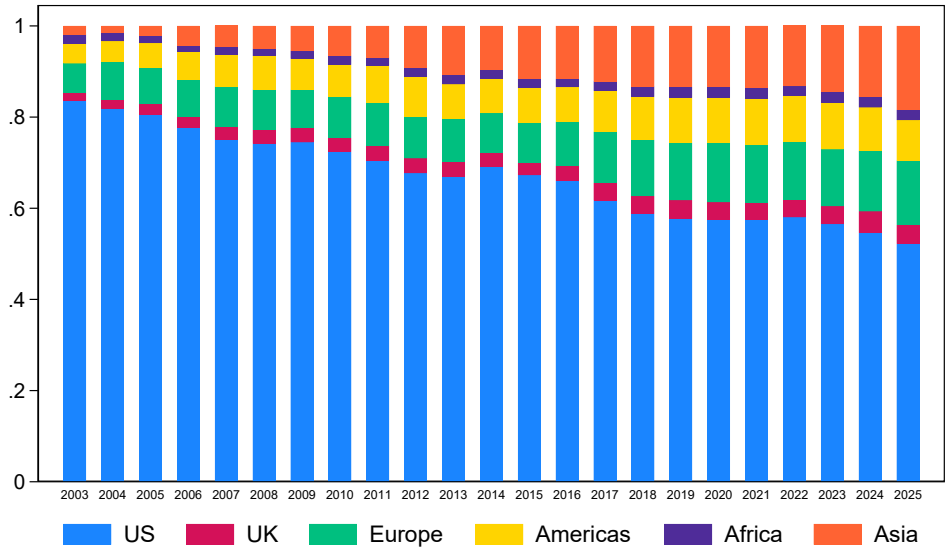
(b) Participant



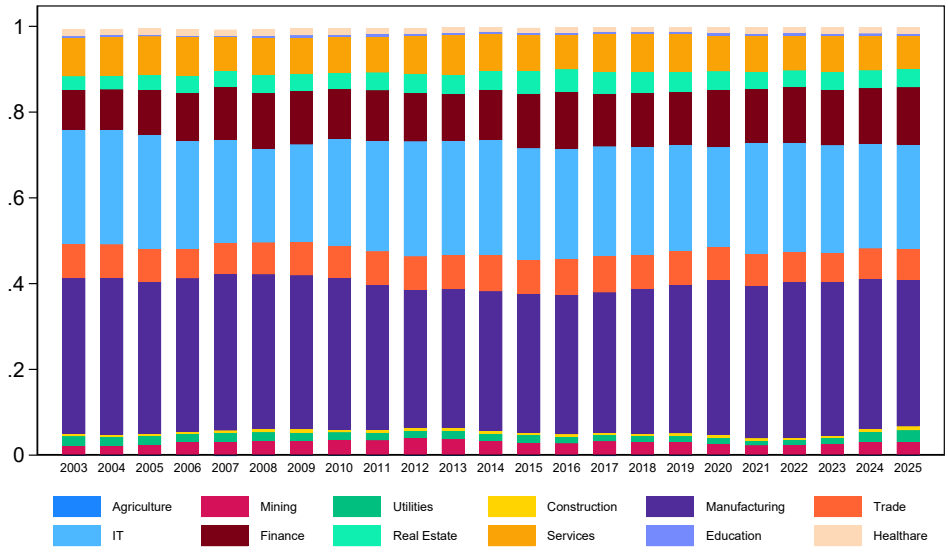
Notes: This figure plots the decomposition of the baseline index of cyber risk exposure, $\mathrm{CRExposure_t}$, by earnings call section (Panel (a)) and participant (Panel (b)). Panel (a) shows the measures of relative frequency with which cyber risk exposure keywords get mentioned in the presentation and Q&A sections of earnings calls. Panel (b) shows the measures of relative frequency with which cyber risk exposure keywords get mentioned by corporate executives and external participants.

Figure 3: Decomposition of Cyber Risk Exposure by Region and Sector

(a) Region

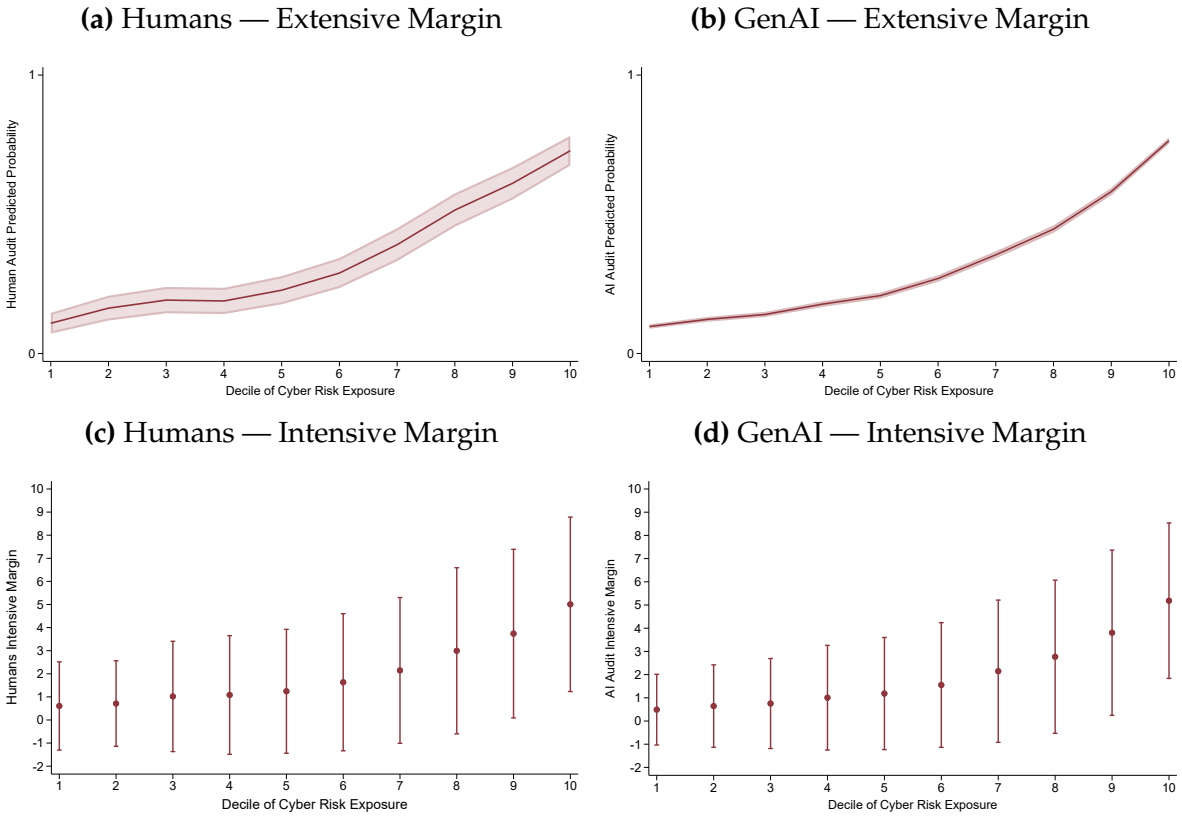


(b) Sector



Notes: This figure plots the decompositions of the baseline index of cyber risk exposure, CRExposure_t, by geographical region and industry over time. Panel (a) shows the measure of relative frequency with which cyber risk exposure keywords get mentioned in earnings calls across six major regions. Panel (b) shows the measure of relative frequency with which cyber risk exposure keywords get mentioned in earnings calls across twelve industries that are grouped according to two-digit NAICS codes.

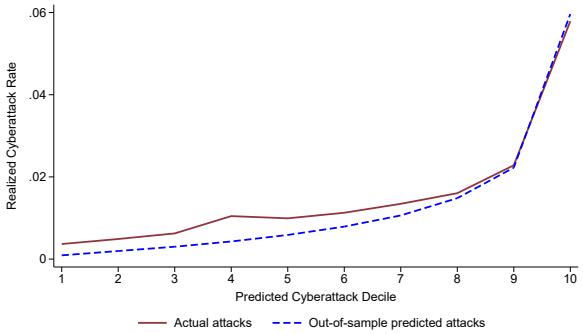
Figure 4: Validation of the Cyber Risk Exposure Measure by Human Auditors and a GenAI Model



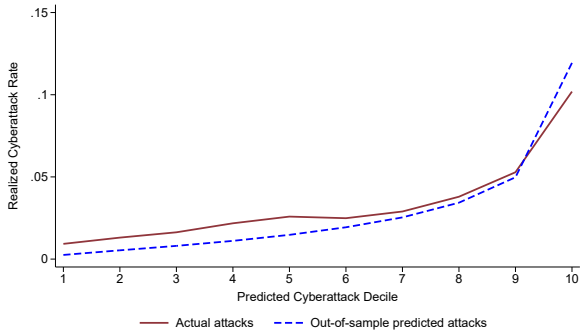
Notes: This figure plots results from the internal validation exercise of the baseline measure of cyber risk exposure, $\mathrm{CRExposure}_{i,t}$. Panels (a) and (b) plot on the vertical axes predicted probabilities of correctly identifying a positive case—by a team of nine human auditors and a GenAI model, respectively—against deciles of the $\mathrm{CRExposure}_{i,t}$ distribution. Predicted probabilities are computed from logit models. Panels (c) and (d) show on the vertical axes average scores of intensity of cybersecurity-related discussions together with one standard deviation bands—as scored by a team of nine human auditors and a GenAI model, respectively—against deciles of the $\mathrm{CRExposure}_{i,t}$ distribution. Both predicted probabilities and intensity scores are computed based on samples of 56,000 and 2,700 transcript snippets, chosen randomly for the GenAI model and human auditors, respectively.

Figure 5: Out-of-sample Forecast of Cyberattacks with Cyber Risk Exposure

(a) One Quarter Ahead

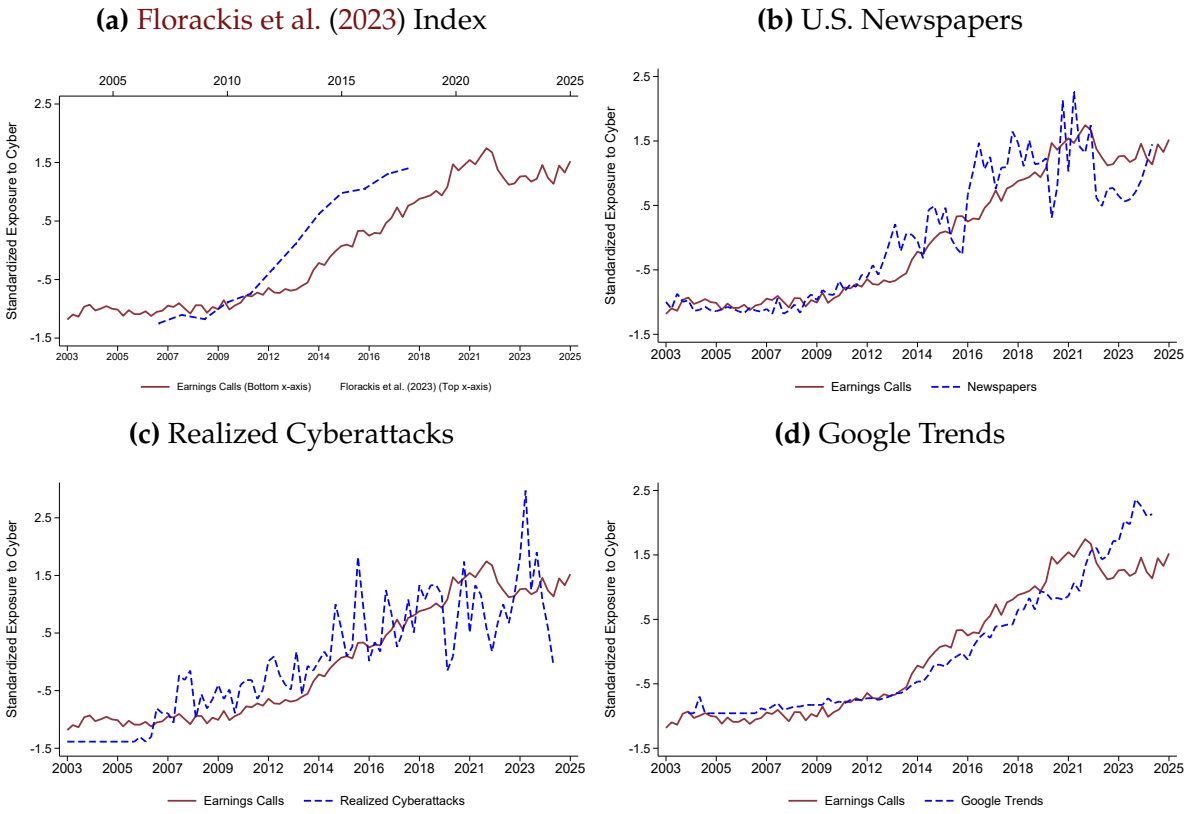


(b) Four Quarters Ahead



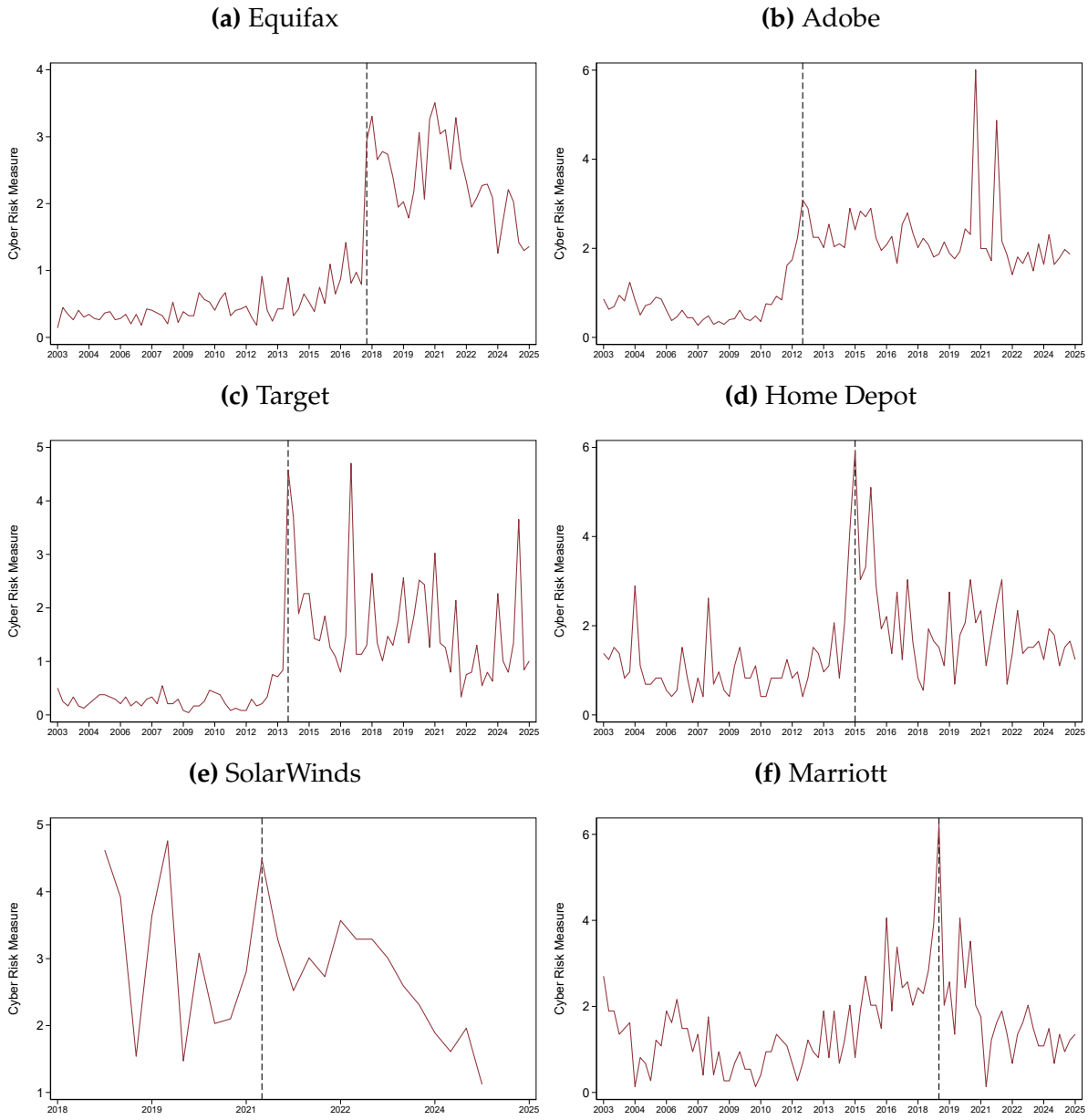
Notes: This figure plots on the horizontal axes predicted cyberattack deciles against realized cyberattack rates. Predicted cyberattacks are calculated using fitted values of a pseudo out-of-sample forecasting model. The model recursively regresses an indicator value that takes the value of unity if a cyberattack takes place, and zero otherwise, on $\mathrm{CRExposure}_{i,t}$ and a vector of controls that includes firm size, (log) age, Tobin's Q, leverage ratio, liquidity ratio, intangibles ratio, operational cost ratio, and the market beta. In Panels (a) and (b) the cyberattack occurs in the following quarter and within the next four quarters, respectively. The sample is restricted to US firms only.

Figure 6: External Validation of Cyber Risk Exposure with Alternative Indices



Notes: This figure plots the index of cyber risk exposure, $\mathrm{CRExposure_{i,t}}$, from this paper together with four externally developed time-series measures. Panel (a) shows the index of cybersecurity risk from Florackis et al. (2023) that is based on firms' 10-K filings. Panel (b) plots $\mathrm{NewsIndex_t}$, which measures average exposure to cyber risk in the texts of major U.S. newspapers. Panel (c) plots the time-series index $\mathrm{CyberAttack_t}$, which is the quarterly number of realized cyberattacks from the Privacy Rights Clearinghouse. Panel (d) plots $\mathrm{GoogleIndex_t}$, which is the time-series measure of worldwide search interest in the keyword "cyber risk" based on Google Trends. All measures have been standardized to have a mean of zero and standard deviation of unity. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions.

Figure 7: Case Studies



Notes: This figure plots the time series of exposure, $\mathrm{CRExposure}_{i,t}$, towards cyber risk for select firms. Vertical dashed lines correspond to the timings of individual cybersecurity incidents that are described in main text.

Table I: Summary Statistics

This table reports summary statistics for the key firm-level variables used throughout the paper. For the cyber risk measures, the sample includes 14,317 unique firms over 2003Q1-2025Q3. The stock market, option market, and balance sheet variables have been standardized to have a mean of zero and standard deviation of unity. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions.

	N	Mean	St. Dev.	Min	Max
Cyber Risk Measures (x100)					
$\text{CRExposure}_{i,t}$	128,659	3.22	3.35	0.00	45.56
$\text{CRExposure}_{i,t}^{\text{Pres}}$	128,659	1.73	2.13	0.00	32.74
$\text{CRExposure}_{i,t}^{\text{Q\&A}}$	128,659	1.49	1.77	0.00	31.25
$\text{CRExposure}_{i,t}^{\text{Exec}}$	128,659	2.81	3.05	0.00	44.02
$\text{CRExposure}_{i,t}^{\text{Part}}$	128,659	0.37	0.55	0.00	25.07
Stock Market Variables (std)					
Average Return	128,658	0.01	1.00	-3.47	2.70
Cumulative Return	128,659	0.00	1.00	-3.43	2.67
Realized Volatility	128,619	1.72	1.00	0.53	5.63
Option Market Variables (std)					
Implied Volatility	128,469	1.68	1.00	0.59	6.35
Variance Risk Premium	128,431	0.12	1.00	-3.38	6.55
Implied Volatility Slope	128,419	4.75	1.00	1.33	6.58
Firm Balance Sheet Variables (std)					
Assets (log)	109,689	4.30	1.00	2.16	6.99
Age (log)	109,689	4.34	1.00	0.86	5.58
Tobin's Q	109,030	1.31	1.00	0.45	6.21
Debt / Assets (leverage)	103,557	1.33	1.00	0.00	3.98
Cash / Assets (liquidity)	109,653	0.88	1.00	0.00	4.46
Intangibles / Assets	109,103	0.94	1.00	0.00	3.69
Operational Costs / Assets	109,623	1.14	1.00	0.02	5.07
Market Beta	128,658	3.05	1.00	0.95	5.97
Return on Assets	109,689	0.21	1.00	-4.59	2.61
Cash Flow / Assets	109,689	0.47	1.00	-4.26	2.86
Credit Rating (1=highest)	93,220	2.89	1.00	0.60	4.17

Table II: Top 100 Cyber Risk Exposure Keywords

This table reports the count of the top 100 keywords that constitute the baseline index of cyber risk exposure $\text{CRExposure}_{i,t}$. Table A.2 provides detailed variable definitions.

Term	Count	Term	Count	Term	Count
data	1,237,242	firewall	6,572	system development	965
asset	774,132	hazard	6,372	incident response	928
network	559,335	credentials	6,251	login	913
digital	554,123	network services	5,139	hacking	899
access	410,713	bot	4,613	cyber attack	886
software	364,457	critical infrastructure	4,525	vulnerability management	884
cloud	255,998	router	4,507	byod	870
exposure	254,863	precursor	4,129	situational awareness	863
availability	174,621	encryption	4,028	phishing	862
app	89,828	vpn	4,017	cyber incident	802
disruption	80,870	operational risk	3,863	authenticate	786
disclosure	75,617	vulnerability	3,763	hack	746
data center	70,676	intrusion	2,889	data breach	676
authorization	60,418	data security	2,878	security management	676
saas	49,946	information system	2,832	data integrity	666
domain	32,816	network security	2,682	personal information	660
iot	32,140	unauthorized	2,593	information assurance	562
computer	29,994	gdpr	2,585	cyber resilience	558
virus	26,853	bug	2,360	attack surface	538
cyber	25,887	ransomware	2,133	data architecture	532
detection	23,557	malware	2,093	cyber risk	531
incident	21,600	password	1,910	system architecture	529
accountability	15,312	authenticity	1,823	1linformation sharing	511
interruption	14,988	spam	1,785	it asset	494
exploit	12,999	information security	1,749	spyware	489
verification	12,978	security systems	1,660	security program	471
information technology	12,476	forensics	1,658	decode	464
compromise	10,998	ddos	1,610	data loss	462
certificate	10,981	identity management	1,452	data aggregation	462
privacy	9,187	access management	1,451	personal data	458
ict	8,769	cipher	1,269	operational disruption	444
alert	8,543	trojan	1,109	intrusion detection	430
confidentiality	8,294	antivirus	1,069		
breach	6,843	threat intelligence	1,049		

Table III: Variance Decomposition of Firm-level Cyber Risk Measures

This table reports variance decompositions of baseline firm-level cyber risk exposure measures. Regressions of cyber risk exposure measures on various sets of fixed effects are estimated at the firm-quarter level. Each row reports the incremental R^2 from adding a specific fixed effect. Industries are defined at the 2-digit NAICS level. $\text{CRExposure}_{i,t}$ measures the relative frequency with which cyber risk exposure keywords get mentioned in the earnings calls. $\text{CRExposure}^{\text{Pres}}_{i,t}$ and $\text{CRExposure}^{\text{Q\&A}}_{i,t}$ measure relative frequency with which cyber risk exposure keywords get mentioned in the presentation and Q&A sections of earnings calls, respectively. $\text{CRExposure}^{\text{Exec}}_{i,t}$ and $\text{CRExposure}^{\text{Part}}_{i,t}$ measure relative frequency with which cyber risk exposure keywords get mentioned by corporate executives and external participants, respectively. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions.

Dependent Variable:	$\text{CRExposure}_{i,t}$	$\text{CRExposure}^{\text{Pres}}_{i,t}$	$\text{CRExposure}^{\text{Q\&A}}_{i,t}$	$\text{CRExposure}^{\text{Exec}}_{i,t}$	$\text{CRExposure}^{\text{Part}}_{i,t}$
	(1)	(2)	(3)	(4)	(5)
Time FE	5.37%	4.60%	3.41%	5.76%	1.28%
Sector FE	18.40%	15.23%	12.68%	18.44%	6.13%
Sector x Time FE	1.60%	1.43%	1.54%	1.59%	1.45%
Country FE	0.59%	0.52%	0.77%	0.53%	0.61%
Firm-level Variation	74.00%	78.18%	81.57%	73.65%	90.48%
of which					
Firm FE	39.74%	37.60%	35.81%	39.13%	24.68%
Residual	34.26%	40.58%	45.76%	34.53%	65.80%

Table IV: The Nature of Firm-level Cyber Risk

This table reports regressions of quarterly firm-level cyber risk exposure on various firm characteristics. Column (1) includes industry x time fixed effects. Column (2) includes country x time fixed effects. All variables have been standardized to have a mean of zero and standard deviation of unity. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

Dependent Variable (std):	$\text{CRExposure}_{i,t}$	$\text{CRExposure}_{i,t}$
	(1)	(2)
Log (Size)	0.075***	0.084***
	(0.017)	(0.021)
Market Beta	0.014	0.016
	(0.011)	(0.012)
Intangibles / Assets	0.057***	0.153***
	(0.016)	(0.017)
Liquidity Ratio	0.209***	0.292***
	(0.020)	(0.022)
Tobin's Q	0.060***	0.103***
	(0.017)	(0.018)
CAPEX / Assets	-0.013	-0.060***
	(0.016)	(0.016)
Cash Flow / Assets	0.092***	0.180***
	(0.026)	(0.034)
Log (Age)	0.040***	-0.003
	(0.012)	(0.012)
Book to Market Ratio	0.000	0.029**
	(0.010)	(0.013)
Leverage	0.024**	0.039***
	(0.012)	(0.013)
ROA	-0.109***	-0.181***
	(0.025)	(0.033)
PP&E / Assets	-0.058***	-0.049***
	(0.019)	(0.014)
Debt Maturity Ratio	0.003	0.005
	(0.009)	(0.009)
Equity Issuance Ratio	0.027*	0.029*
	(0.015)	(0.017)
Turnover Ratio	-0.274***	-0.283***
	(0.046)	(0.051)
Operat. Costs / Assets	0.222***	0.204***
	(0.046)	(0.050)
Controls	Yes	Yes
Sector FE	Yes	Yes
Time FE	Yes	Yes
Level	Firm	Firm
Frequency	Quarterly	Quarterly
Observations	116,939	115,945
R^2	0.306	0.198

Table V: Firm-level Cyber Risk Exposure and Stock Market Effects

This table reports regressions of stock market variables on the baseline firm-level cyber risk exposure measure, $\mathrm{CRExposure_{i,t}}$. $\mathrm{Ret_{i,t}}$ is average quarterly return, $\mathrm{CRet_{i,t}}$ is cumulative quarterly return, $\mathrm{RV_{i,t}}$ is realized volatility of returns. $\mathrm{CRExposure_{i,t}}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. Columns (1), (3), and (5) include industry x time fixed effects. Columns (2), (4), and (6) include country x time fixed effects. All dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}\mathrm{p} < 0.1$; $^{**}\mathrm{p} < 0.05$; $^{***}\mathrm{p} < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std):	$\mathrm{Ret_{i,t}}$	$\mathrm{Ret_{i,t}}$	$\mathrm{CRet_{i,t}}$	$\mathrm{CRet_{i,t}}$	$\mathrm{RV_{i,t}}$	$\mathrm{RV_{i,t}}$
$\mathrm{CRExposure_{i,t}}$	-0.008***	-0.012***	-0.010***	-0.014***	0.021***	0.020***
	(0.003)	(0.003)	(0.003)	(0.003)	(0.007)	(0.007)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	×	✓	×	✓	×
Country x Time FE	×	✓	×	✓	×	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,369	101,479	102,369	101,479	102,353	101,461
$\mathrm{R^2}$	0.306	0.275	0.325	0.295	0.552	0.530

Table VI: Firm-level Cyber Risk Exposure and Option Market Effects

This table reports regressions of option market variables on the baseline firm-level cyber risk exposure measure, $\mathrm{CRExposure}_{i,t}$. $\mathrm{IV}_{i,t}$ is implied volatility, $\mathrm{VRP}_{i,t}$ is the variable risk premium, and $\mathrm{SlopeD}_{i,t}$ is the implied volatility slope. $\mathrm{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. Columns (1), (3), and (5) include industry x time fixed effects. Columns (2), (4), and (6) include country x time fixed effects. All dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std):	$\mathrm{IV}_{i,t}$	$\mathrm{IV}_{i,t}$	$\mathrm{VRP}_{i,t}$	$\mathrm{VRP}_{i,t}$	$\mathrm{SlopeD}_{i,t}$	$\mathrm{SlopeD}_{i,t}$
$\mathrm{CRExposure}_{i,t}$	0.051***	0.047***	0.043***	0.037***	0.030**	0.040***
	(0.008)	(0.008)	(0.007)	(0.007)	(0.013)	(0.012)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	×	✓	×	✓	×
Country x Time FE	×	✓	×	✓	×	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,251	101,362	102,236	101,345	102,213	101,323
R^2	0.570	0.561	0.187	0.188	0.280	0.273

Table VII: Firm-level Cyber Risk Exposure and Balance Sheet Effects

This table reports regressions of balance sheet variables on the baseline firm-level cyber risk exposure measure, $\text{CRExposure}_{i,t}$. $\text{RoA}_{i,t}$ is the return on assets, $\text{CashFlow}_{i,t}$ is the cash flow to assets ratio, and $\text{Rating}_{i,t}$ is the S&P credit rating that is normalized such that a greater value indicates a better rating. $\text{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. Columns (1), (3), and (5) include industry x time fixed effects. Columns (2), (4), and (6) include country x time fixed effects. All dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std):	$\text{RoA}_{i,t}$	$\text{RoA}_{i,t}$	$\text{CashFlow}_{i,t}$	$\text{CashFlow}_{i,t}$	$\text{Rating}_{i,t}$	$\text{Rating}_{i,t}$
$\text{CRExposure}_{i,t}$	-0.102***	-0.095***	-0.091***	-0.082***	-0.100***	-0.116***
	(0.012)	(0.011)	(0.012)	(0.011)	(0.015)	(0.016)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	×	✓	×	✓	×
Country x Time FE	×	✓	×	✓	×	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,369	101,479	102,369	101,479	87,432	86,779
R^2	0.251	0.230	0.273	0.243	0.284	0.238

Table VIII: Cyber Risk Exposure and Industry-level Effects

This table reports regressions of industry-level stock market, option market, and balance sheet outcomes on the measure of cyber risk exposure. CRet is cumulative stock return, RV is realized volatility, IV is implied option-market volatility, VRP is the variance risk premium, SlopeD is the implied volatility slope, and RoA is the return on assets. Controls include size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Firm assets are used as the weight. In panels (A) and (B), all variables are industry-level unweighted and weighted-average aggregates of the firm-level variables, respectively. All dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions. All specifications include a country x time fixed effect. Standard errors, clustered at the country level, are in parentheses. $^{*}\mathrm{p} < 0.1$; $^{**}\mathrm{p} < 0.05$; $^{***}\mathrm{p} < 0.01$.

	Panel A: Unweighted Average					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std):	$\mathrm{CRet}^{\mathrm{u}}_{\mathrm{s,t}}$	$\mathrm{RV}^{\mathrm{u}}_{\mathrm{s,t}}$	$\mathrm{IV}^{\mathrm{u}}_{\mathrm{s,t}}$	$\mathrm{VRP}^{\mathrm{u}}_{\mathrm{s,t}}$	$\mathrm{SlopeD}^{\mathrm{u}}_{\mathrm{s,t}}$	$\mathrm{RoA}^{\mathrm{u}}_{\mathrm{s,t}}$
$\mathrm{CRExposure}^{\mathrm{u}}_{\mathrm{s,t}}$	-0.020***	0.034*	0.058***	0.037***	0.049***	-0.090***
	(0.004)	(0.017)	(0.019)	(0.010)	(0.012)	(0.017)
Controls	✓	✓	✓	✓	✓	✓
Country x Time FE	✓	✓	✓	✓	✓	✓
Level	Industry	Industry	Industry	Industry	Industry	Industry
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	41,472	41,468	41,451	41,447	41,441	41,472
R^2	0.406	0.593	0.577	0.266	0.369	0.243
	Panel B: Weighted Average					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std):	$\mathrm{CRet}^{\mathrm{w}}_{\mathrm{s,t}}$	$\mathrm{RV}^{\mathrm{w}}_{\mathrm{s,t}}$	$\mathrm{IV}^{\mathrm{w}}_{\mathrm{s,t}}$	$\mathrm{VRP}^{\mathrm{w}}_{\mathrm{s,t}}$	$\mathrm{SlopeD}^{\mathrm{w}}_{\mathrm{s,t}}$	$\mathrm{RoA}^{\mathrm{w}}_{\mathrm{s,t}}$
$\mathrm{CRExposure}^{\mathrm{w}}_{\mathrm{s,t}}$	-0.017***	0.027*	0.055**	0.034***	0.051***	-0.075***
	(0.003)	(0.015)	(0.020)	(0.010)	(0.011)	(0.016)
Controls	✓	✓	✓	✓	✓	✓
Country x Time FE	✓	✓	✓	✓	✓	✓
Level	Industry	Industry	Industry	Industry	Industry	Industry
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	41,472	41,468	41,451	41,447	41,440	41,472
R^2	0.391	0.586	0.587	0.264	0.353	0.239

Table IX: Cyber Risk Exposure and Spillover Effects

This table reports regressions of stock market, option market, and balance sheet outcomes of affected and unaffected firms on the measure of cyber risk exposure. Affected firms are defined as those with a $\mathrm{CRExposure}_{i,t}$ of greater than the median exposure. Unaffected firms are defined as those with a $\mathrm{CRExposure}_{i,t}$ of lower than or equal to the median exposure. Regressions are run at the firm-time level and the cyber risk exposure measure is aggregated to the country-sector-time level. All specifications include a country x time fixed effect. CRet is cumulative stock return, RV is realized volatility, IV is implied option-market volatility, VRP is the variance risk premium, SlopeD is the implied volatility slope, and RoA is the return on assets. Controls include size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. All dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions. Standard errors, clustered at the country level, are in parentheses. $^{*}\mathrm{p} < 0.1$; $^{**}\mathrm{p} < 0.05$; $^{***}\mathrm{p} < 0.01$.

	Panel A: Affected Firms					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std):	$\mathrm{CRet}_{i,t}$	$\mathrm{RV}_{i,t}$	$\mathrm{IV}_{i,t}$	$\mathrm{VRP}_{i,t}$	$\mathrm{SlopeD}_{i,t}$	$\mathrm{RoA}_{i,t}$
Cyber Risk Exposure	-0.017***	0.014*	0.027**	0.016**	0.047***	-0.062***
	(0.002)	(0.008)	(0.012)	(0.006)	(0.009)	(0.007)
Controls	✓	✓	✓	✓	✓	✓
Country x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	48,224	48,217	48,158	48,151	48,137	48,224
R^2	0.294	0.535	0.565	0.191	0.247	0.281
	Panel B: Peer Firms					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std):	$\mathrm{CRet}_{i,t}$	$\mathrm{RV}_{i,t}$	$\mathrm{IV}_{i,t}$	$\mathrm{VRP}_{i,t}$	$\mathrm{SlopeD}_{i,t}$	$\mathrm{RoA}_{i,t}$
Cyber Risk Exposure	-0.038***	0.061***	0.107***	0.062***	0.118***	-0.121***
	(0.002)	(0.004)	(0.004)	(0.006)	(0.006)	(0.004)
Controls	✓	✓	✓	✓	✓	✓
Country x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	52,081	52,074	52,036	52,030	52,020	52,081
R^2	0.299	0.521	0.555	0.187	0.298	0.175

Online Appendix for "The Anatomy of Cyber Risk"

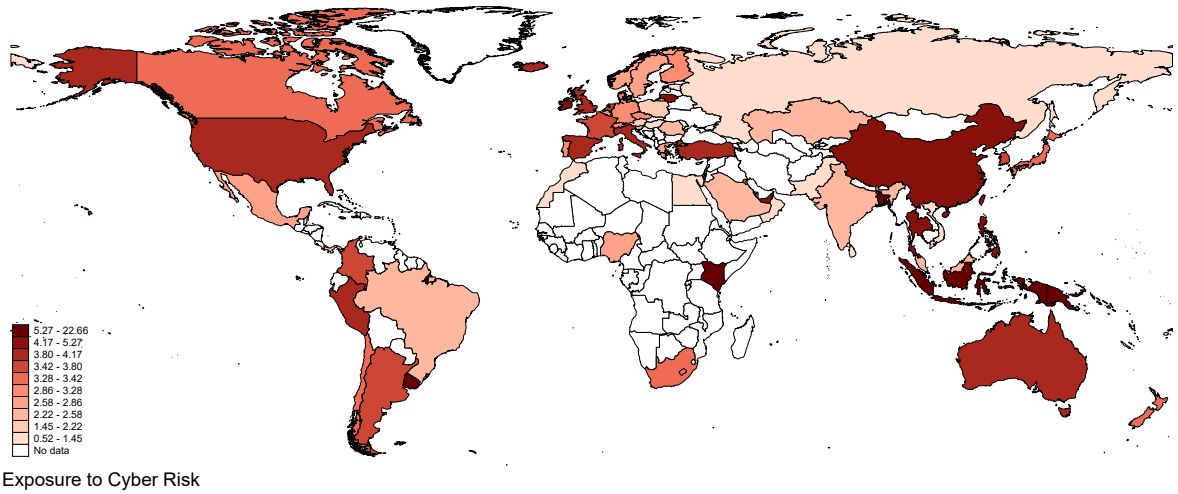
Rustam Jamilov Hélène Rey Ahmed Tahoun

December 2025

Contents

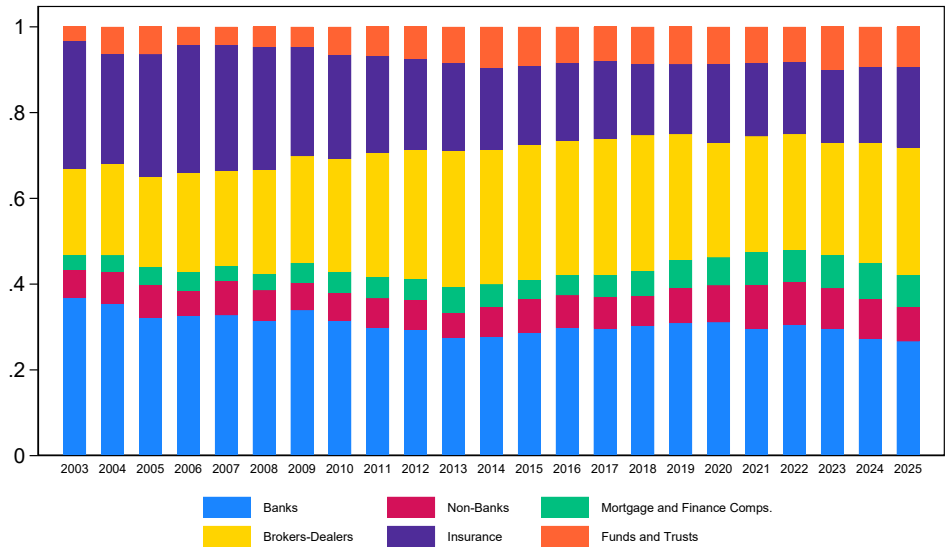
A Additional Figures

Figure A.1: Global Cyber Risk Exposure in 2024



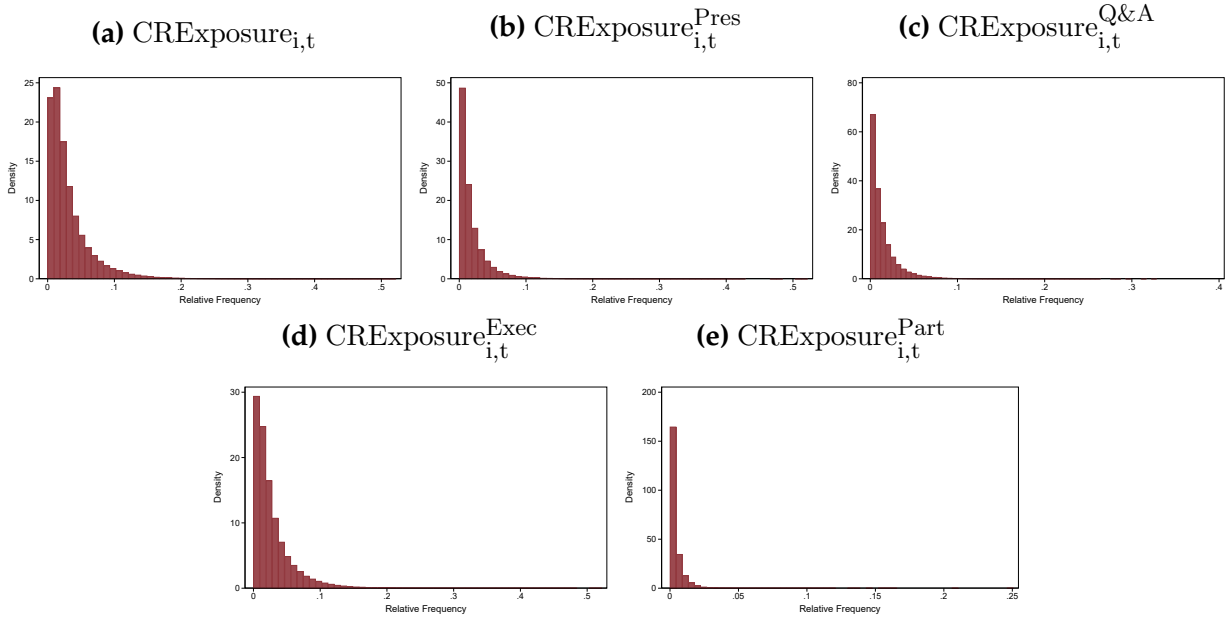
Notes: This figure plots the decompositions of the baseline index of cyber risk exposure, $\mathrm{CRExposure}_{i,t}$, by country for the year 2024. Country-level aggregates are obtained by taking unweighted averages of the firm-level measure.

Figure A.2: Finance-Industry Decomposition of Cyber Risk Exposure over Time



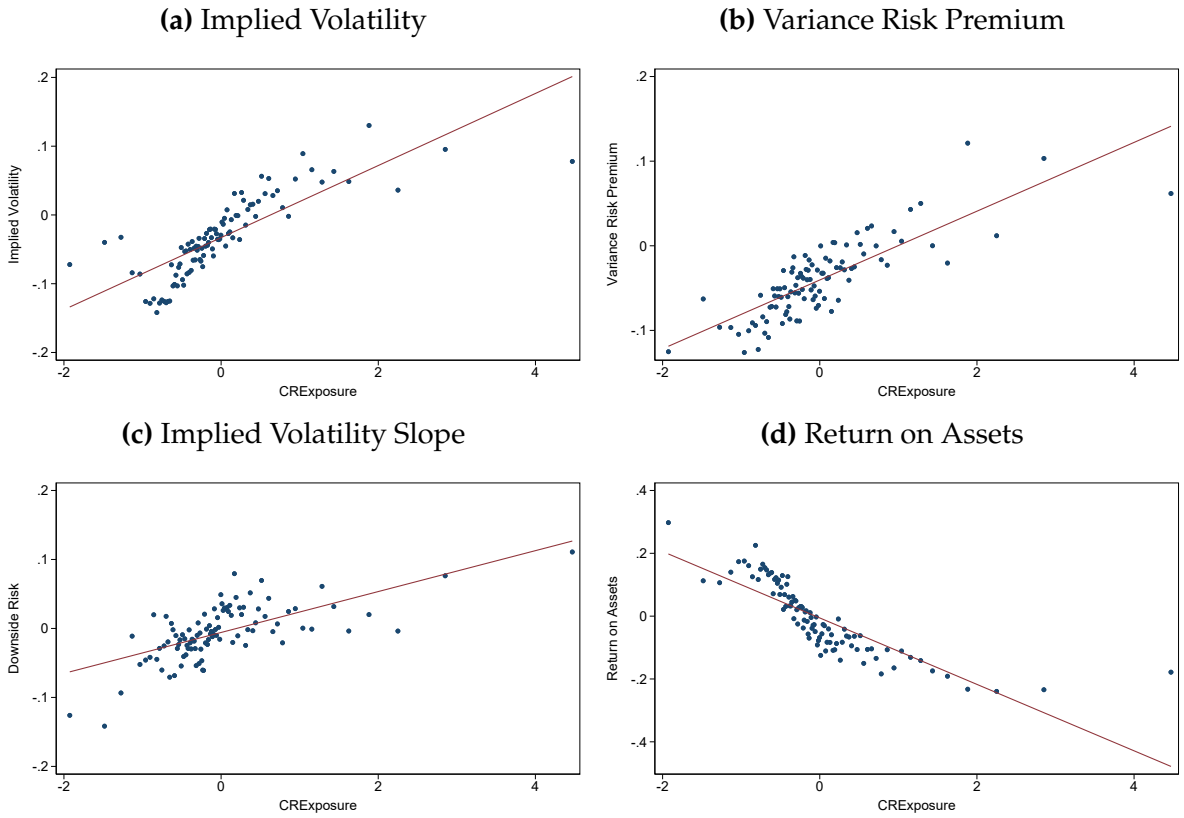
Notes: This figure plots the decomposition of the baseline index of cyber risk exposure, $\mathrm{CRExposure}_{i,t}$, by finance sub-industry over time. It shows the measure of relative frequency with which cyber risk exposure keywords get mentioned in earnings calls across six finance sub-industries, defined as sectors in the 52 NAICS category.

Figure A.3: Histograms of Cyber Risk Measures



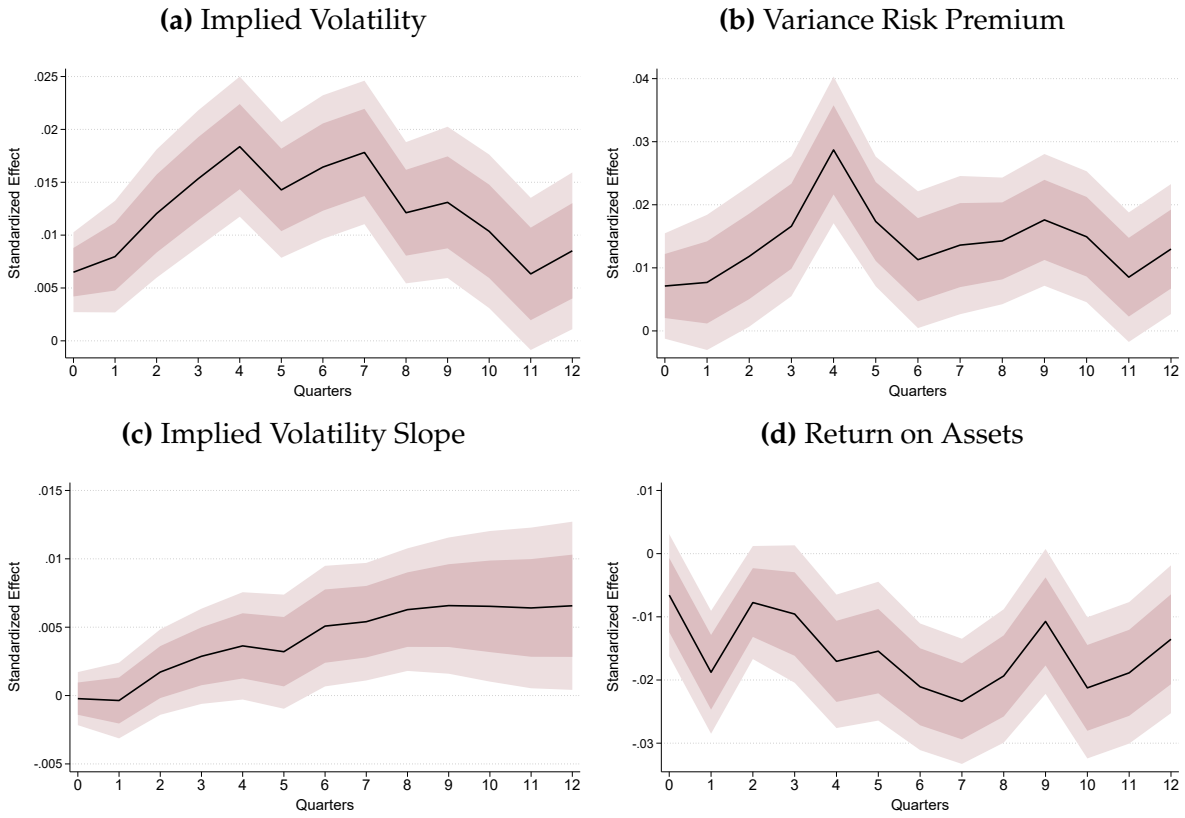
Notes: This figure plots histograms of cyber risk measures used throughout this paper. In every panel, values have been pooled across all quarters and firms.

Figure A.4: Binned Scatterplots of Firm-level Effects of Cyber Risk Exposure



Notes: This figure plots binned scatterplots of firm-level regressions of balance sheet and option market variables on $\mathrm{CRExposure}_{i,t}$. Regressions are estimated at the firm-quarter level. Each plot presents 100 equally-sized bins. IV is implied option-market volatility, VRP is the variance risk premium, SlopeD is the implied volatility slope, and RoA is the return on assets. Each specification includes industry x time fixed effects and controls for firm size, (log) age, Tobin's Q, leverage ratio, liquidity ratio, intangibles ratio, operational cost ratio, and the market beta. All estimates have been standardized.

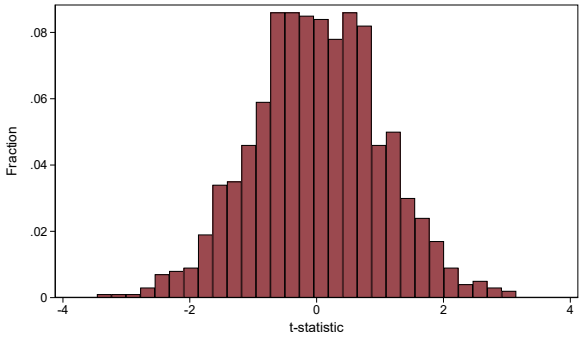
Figure A.5: Dynamic Firm-level Effects of Cyber Risk Exposure



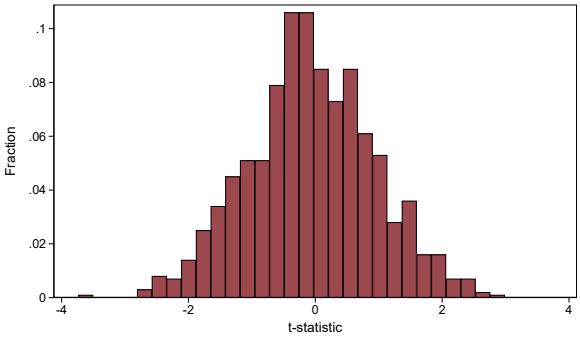
Notes: This figure plots estimates of dynamic effects of $\mathrm{CRExposure}_{i,t}$ on balance sheet and option market variables. Regressions are estimated at the firm-quarter level. IV is implied option-market volatility, VRP is the variance risk premium, SlopeD is the implied volatility slope, and RoA is the return on assets. Each panel reports point estimates along with 68% and 90% confidence bands on the vertical axes against forward horizons on the horizontal axes. Each specification includes industry x time fixed effects and controls for two lags of the dependent variable, two lags of $\mathrm{CRExposure}_{i,t}$, and two lags of firm size, (log) age, Tobin's Q, leverage ratio, liquidity ratio, intangibles ratio, operational cost ratio, and the market beta. All estimates have been standardized. Standard errors are clustered at the firm level.

Figure A.6: Placebo Regressions: t-statistic Distributions

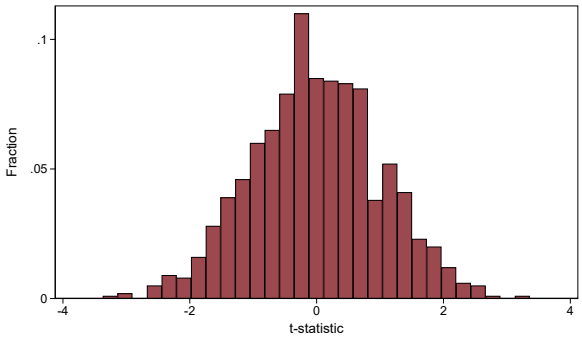
(a) Return on Assets



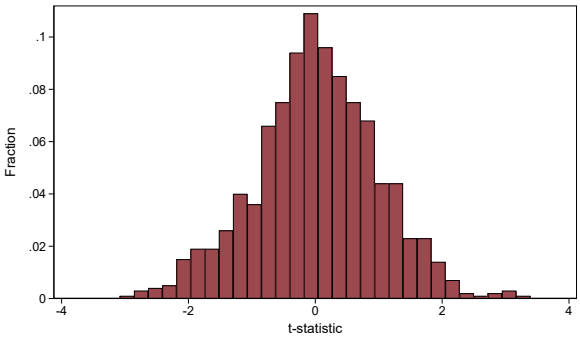
(b) Implied Volatility



(c) Variance Risk Premium



(d) Implied Volatility Slope



Notes: This figure reports placebo regressions of firm-level outcomes on cyber risk exposure. Each panel presents a histogram of 1,000 t-statistics from regressions of corresponding firm-level variables on the baseline measure of cyber risk exposure, $\mathrm{CRExposure_{i,t}}$, where values of $\mathrm{CRExposure_{i,t}}$ have been randomly re-assigned within a quarter and across firms with replacement. IV is implied option-market volatility, VRP is the variance risk premium, SlopeD is the implied volatility slope, and RoA is the return on assets. Each specification includes industry x time fixed effects and controls for firm size, (log) age, Tobin's Q, leverage ratio, liquidity ratio, intangibles ratio, operational cost ratio, and the market beta. Standard errors are clustered at the firm level.

B Additional Tables

Table B.I: Cyber Risk Exposure Measures: Correlations

This table reports pairwise correlations and standard errors for different cyber risk exposure measures. All variables are defined in Table A.2 of the Appendix.

$\text{CRExposure}_{i,t}$	1				
$\text{CRExposure}^{\text{Pres}}_{i,t}$	0.88	1			
	0.00				
$\text{CRExposure}^{\text{Q\&A}}_{i,t}$	0.83	0.47	1		
	0.00	0.00			
$\text{CRExposure}^{\text{Exec}}_{i,t}$	0.99	0.91	0.77	1	
	0.00	0.00	0.00		
$\text{CRExposure}^{\text{Part}}_{i,t}$	0.60	0.34	0.73	0.48	1
	0.00	0.00	0.00	0.00	

Table B.II: Snippets of Cyber Risk Exposure in Earnings Calls Transcripts

Company	Snippet	Date	CRExposure (std)	AI Extensive	AI Intensive	Human Extensive	Human Intensive
Equifax Inc	Our non-GAAP financial results will include all increased costs related to IT and data security that are ongoing or permanent in nature. We will exclude from our non-GAAP financial results both the incremental or bubble costs incurred to implement our IT and data security plans and the legal and our professional service cost being encourage specifically to address the litigation and governmental and regulatory investigations related to the cybersecurity incident.	2018Q1	2.67	1	10	1	9
Splunk Inc	On the state and local level, the City of Los Angeles expanded with the purchase of Splunk Cloud ES and ITSI. LA is correlating cyber threat information from external and internal sources, and analyzing network traffic in real time. Splunk enables them to compare their patterns with national and regional ones to identify anomalies that might indicate malicious attacks.	2016Q3	2.78	1	6	1	8
Palo Alto Networks Inc	A recent internal study amongst our customers showed GenAI traffic is up over 890% in 2024. Following this, data security incidents related to GenAI more than doubled since last year. With this rapid adoption of AI comes a new and complex attack surface.	2025Q3	3.19	1	9	1	10
Solarwinds Corp	These statements are based on currently available information and assumptions, and we undertake no duty to update this information, except as required by law. These statements are also subject to a number of risks and uncertainties, including the numerous risks related to the cyber incident and the recently completed spin-off of the N-able business.	2021Q4	0.55	1	5	1	7
SecureWorks Corp	One such new customer example, a global European chemicals company with operations in more than 100 countries, was seeking a security partner to focus on threat detection and response. They were concerned about ransomware attacks. They purchased our TDR software to give them a unified approach to managing their security program with holistic detection and automated investigation capabilities	2020Q4	2.55	1	10	1	9

Salesforce Inc	And I really wanted to just point that out as one of the reasons Service Cloud it has had such an incredible success. And if you looked at Service Cloud against any other cloud company, that's amazing in terms of its size. But also, if you look at our growth for next year, you might note that we're going to grow more next year than I think the second largest enterprise cloud company in absolute numbers.	2014Q4	2.22	1	8	1	5
CVS Group PLC	Whilst this remains within our stated ambition, it was adversely impacted in the year by the cyber incident, inflationary pressures on wages and utilities alongside our continued investment in people. In accordance with our strategy, we invested GBP43.1 million in capital expenditure to improve our facilities and equipment and our technology.	2024Q3	1.67	1	5	1	9
Cyren Ltd	The rate of new cyber threats continues to grow at a blistering pace and it reminds us that no enterprise, whether large or small, is immune from the technical and financial impacts of malware, including botnets, Ransomewares, zero day and phishing attacks.	2016Q2	2.78	1	10	1	10
Abercrombie & Fitch Co	We're seeing nice paybacks in those spaces. And when we marry that stores and the digital component, which continues obviously to be a critical growth channel, it's a nice experience for that consumer. We don't see it as an either or, ✓, A&F is a little bit more distorted to digital today, but really what it is, it's about omnichannel.	2025Q3	-1.01	0	0	0	0
Walt Disney Co	And then, Jay, on the Hurricane Sandy impact, you said you couldn't really quantify it as of yet. But would the majority of that impact, whatever it is, be due to disruption at the Parks? Just because folks in the tri-state area couldn't fly down to Orlando, obviously; may still not be able to fly down there.	2012Q4	-1.02	0	0	0	0

Table B.III: Observations by Country

This table reports the number of earnings calls, average transcript length, and average cyber risk exposure by country.

Country	Number of Earnings Calls	Average Transcript Length	Average $\mathrm{CRExposure}_{i,t}$
Antigua and Barbuda	4	280.50	4.56
Argentina	869	237.46	3.44
Australia	6641	456.14	3.77
Austria	1235	401.64	2.03
Bahamas	47	346.04	1.04
Bahrain	29	478.03	2.23
Bangladesh	21	216.29	19.23
Belgium	1511	466.50	3.23
Bermuda	3036	372.18	2.74
Brazil	6671	340.83	2.37
British Virgin Islands	50	342.64	1.22
Canada	24448	365.65	2.86
Cayman Islands	478	277.86	3.35
Chile	1076	293.16	2.92
China	5522	322.41	3.52
Colombia	563	376.79	2.99
Cyprus	223	344.57	2.04
Czech Republic	220	412.13	4.06
Denmark	2527	443.16	2.61
Egypt	162	418.80	4.70
Estonia	21	230.00	0.77
Faroe Islands	31	291.06	0.92
Finland	2800	361.35	2.25
France	5062	537.94	3.30
Gabon	1	270.00	1.48
Germany	7502	487.77	2.67
Ghana	1	642.00	3.74
Gibraltar	57	445.12	2.74
Greece	1254	327.21	2.49
Guernsey	229	325.04	5.96
Hong Kong	2265	344.86	4.02
Hungary	243	435.46	2.80
Iceland	95	306.81	2.64
India	14025	532.23	2.63
Indonesia	449	446.49	5.84
Ireland	2600	494.37	3.16
Isle of Man	79	505.27	4.19
Israel	3589	291.31	4.82
Italy	3357	430.55	3.28
Jamaica	4	497.75	3.38
Japan	7573	225.57	2.30
Jersey	267	398.17	2.98
Kazakhstan	57	968.54	5.05
Kenya	37	495.92	7.90
Kuwait	72	277.14	4.00
Lithuania	19	288.00	4.38
Luxembourg	1197	420.88	2.43

Macao	9	243.67	0.65
Malaysia	387	507.14	4.12
Malta	88	406.84	1.96
Marshall Islands	54	305.72	3.72
Mauritius	17	517.82	3.52
Mexico	3185	332.83	2.18
Monaco	401	307.14	2.24
Morocco	19	304.58	5.41
Netherlands	3135	523.05	2.63
New Zealand	930	419.69	3.67
Nigeria	185	463.97	3.67
Norway	3491	302.52	2.69
Oman	83	323.84	6.36
Pakistan	26	410.62	4.19
Panama	159	347.37	3.75
Papua New Guinea	33	483.42	2.14
Peru	322	283.08	2.03
Philippines	436	447.37	5.42
Poland	1097	400.36	2.61
Portugal	741	381.96	2.76
Puerto Rico	297	339.52	3.09
Qatar	197	298.33	3.76
Romania	133	300.05	2.08
Russia	1216	380.03	2.25
Saudi Arabia	112	420.54	2.02
Singapore	1243	435.48	3.68
Slovenia	22	744.23	3.09
South Africa	1977	513.56	3.15
South Korea	1820	287.86	3.69
Spain	2788	419.50	2.67
Sri Lanka	5	378.40	1.92
Sweden	7964	377.66	2.15
Switzerland	3719	539.89	2.79
Taiwan	1810	357.99	3.19
Thailand	579	426.89	4.60
Turkey	967	333.79	3.20
U.S. Virgin Islands	11	178.00	5.16
Ukraine	14	501.86	1.14
United Arab Emirates	395	325.11	3.21
United Kingdom	12508	494.16	3.32
United States	244159	391.20	3.35
Uruguay	55	326.53	4.13
Venezuela	17	313.29	4.20
Vietnam	3	323.33	0.81

Table B.IV: Observations by Industry

This table reports the number of earnings calls, average transcript length, and average cyber risk exposure by industry.

NAICS-3	Industry Name	Number of Calls	Average Length	$\text{CRExposure}_{i,t}$
42	Wholesale Trade	176	300.47	2.65
61	Educational Services	20	228.35	2.12
111	Crop Production	527	373.97	1.95
211	Oil and Gas Extraction	6016	395.01	2.33
212	Mining (except Oil and Gas)	4881	388.94	1.81
213	Support Activities for Mining	2799	390.90	1.96
221	Utilities	7784	370.62	2.13
236	Construction of Buildings	1550	424.03	1.26
237	Heavy Engineering	1620	381.44	1.47
238	Specialty Trade Contractors	810	403.35	2.01
311	Food Manufacturing	4032	429.64	1.57
312	Beverage & Tobacco	2075	412.63	1.61
313	Textile Mills	340	301.32	1.07
314	Textile Product Mills	260	363.57	1.20
315	Apparel Manufacturing	2157	429.40	1.56
316	Leather Manufacturing	1019	443.34	1.72
321	Wood Product Manufacturing	1088	367.47	1.37
322	Paper Manufacturing	2120	423.19	1.47
323	Printing and Related Activities	514	366.11	3.87
324	Petroleum & Coal Products	2163	465.67	1.67
325	Chemical Manufacturing	29371	367.64	4.65
326	Plastics & Rubber Products	1213	406.29	1.38
327	Nonmetallic Mineral Products	1303	426.87	1.51
331	Primary Metal Manufacturing	2526	421.38	1.30
332	Fabricated Metal Products	3633	394.97	1.57
333	Machinery Manufacturing	9589	408.15	1.76
334	Computer & Electronics	29243	396.73	3.64
335	Electrical Equipment	4248	398.96	2.00
336	Transportation Equipment	7697	427.64	1.68
337	Furniture and Related Products	1381	368.46	1.68
339	Miscellaneous Manufacturing	6867	389.23	2.41
422	Wholesale Trade, Nondurable	1	737.00	3.66
423	Merchant Wholesalers, Durable	4445	373.16	3.12
424	Merchant Wholesalers, Nondurable	2795	357.98	1.88
425	Wholesale Electronic Markets	122	415.05	1.90
441	Motor Vehicle & Parts Dealers	1487	435.15	2.17
442	Furniture & Home Furnishings Stores	141	481.48	1.10
443	Electronics & Appliance	96	381.36	1.78
444	Building Material & Gardens	343	445.02	2.08
445	Food & Beverage Stores	808	464.39	2.14
446	Health & Personal Care	336	426.73	1.99
447	Gasoline Stations	93	427.85	1.75
448	Clothing & Accessories	1503	387.35	1.47
449	General Merchandise Retailers	1094	391.96	3.10
451	Sporting Goods and Stores	408	369.25	1.92
452	General Merchandise Stores	369	456.96	1.98
453	Miscellaneous Store Retailers	140	425.58	1.33

454	Nonstore Retailers	701	315.09	2.53
455	Food and Beverage Retailers	1938	417.68	2.81
456	Health Retailers	585	425.84	2.43
457	Gasoline Stations (Retail Trade)	594	308.05	1.81
458	Clothing Retailers	2199	398.96	2.23
459	Sporting Goods Retailers	770	416.39	2.38
481	Air Transportation	1715	490.71	2.59
482	Rail Transportation	571	591.63	3.22
483	Water Transportation	2864	328.36	1.85
484	Truck Transportation	1291	448.93	3.17
485	Transit & Ground Transportation	162	429.84	2.69
486	Pipeline Transportation	2214	356.07	2.35
488	Support for Transportation	601	350.14	1.94
492	Couriers and Messengers	412	485.61	3.97
511	Publishing Industries	5335	377.63	5.56
512	Motion Picture and Sound	843	356.95	3.91
513	Internet, Broadcasting, Web Search	4816	390.52	8.69
514	Data Processing & Hosting	1	403.00	2.23
515	Broadcasting & Content	1200	379.74	4.08
516	Internet Publishing	2136	395.87	5.22
517	Telecommunications	7406	419.34	7.24
518	Data Processing & Hosting	7787	401.06	7.43
519	Other Information Services	7305	372.87	5.90
522	Credit Intermediation	16860	397.19	3.15
523	Securities & Commodity Contracts	8248	364.10	4.05
524	Insurance Carriers	9608	396.81	2.52
525	Funds & Trusts	2601	296.53	3.62
531	Real Estate	11098	398.67	3.11
532	Rental and Leasing	1638	381.16	2.14
533	Lessors of Nonfinancial Intangibles	1130	347.56	3.23
541	Professional & Scientific Services	11197	394.90	4.52
561	Administrative and Support Services	4755	372.27	2.82
562	Waste Management Services	921	439.11	1.45
611	Educational Services	1962	368.19	2.49
621	Ambulatory Health Services	3525	382.85	2.70
622	Hospitals	893	442.01	2.12
623	Nursing and Residential Care	765	335.57	1.56
624	Social Assistance	72	371.76	1.72
711	Performing Arts Industries	424	274.43	2.16
713	Amusement & Gambling	1406	399.30	2.34
721	Accommodation	1711	378.63	2.05
722	Food Services and Drinking Places	3674	416.94	2.01
811	Repair and Maintenance	120	403.55	3.29
812	Personal and Laundry Services	825	381.60	2.23
999	Unclassified Establishments	1160	417.80	2.81

Table B.V: Observations by Year

This table reports the nmber of earnings calls, average transcript length, and average cyber risk exposure by year.

Year	Number of Earnings Calls	Average Transcript Length	Average $\mathrm{CRExposure}_{\mathrm{i,t}}$
2003	8865	456.81	2.44
2004	10729	441.61	2.49
2005	11820	444.73	2.42
2006	13063	429.96	2.39
2007	14133	416.35	2.47
2008	15488	415.96	2.48
2009	15334	407.61	2.43
2010	15597	402.42	2.50
2011	16115	395.87	2.62
2012	16412	397.73	2.62
2013	14838	404.47	2.67
2014	15903	398.74	2.96
2015	16263	400.48	3.21
2016	16087	393.88	3.35
2017	18348	377.07	3.44
2018	21074	373.66	3.51
2019	22210	374.13	3.57
2020	22593	412.19	3.82
2021	23663	403.86	4.00
2022	25022	381.72	3.90
2023	25871	375.88	3.67
2024	25789	379.55	3.68
2025	19817	380.21	3.71

Table B.VI: In-Sample Prediction of Cyberattacks

Notes: This table reports logit regressions of $\text{CyberAttack}_{i,t}$, a cyberattack indicator based on PRC data, on measures of cyber risk exposure. Panel (A) reports results on the extensive margin, i.e for $\mathbb{I}[\text{CRExposure}_{i,t} > 0]$. Panel (B) reports results on the intensive margin, i.e for $\text{CRExposure}_{i,t}$. $\text{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.1 provides the full list of keywords. All specifications include industry and time fixed effects. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

Panel A: Independent Variable - $\mathbb{I}[\text{CRExposure}_{i,t} > 0]$						
Dependent Variable:	Future Cyberattack					
	Within 1 Quarter		Within 4 Quarters		Within 8 Quarters	
	(1)	(2)	(3)	(4)	(5)	(6)
Odds Ratio	1.428***	1.309***	1.395***	1.334***	1.401***	1.368***
	(0.166)	(0.144)	(0.162)	(0.129)	(0.141)	(0.122)
Controls	×	✓	×	✓	×	✓
Industry FE	✓	✓	✓	✓	✓	✓
Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly
Observations	119,521	95,088	122,640	97,617	125,470	99,890
Pseudo R^2	0.058	0.117	0.050	0.102	0.047	0.096
Panel B: Independent Variable - $\text{CRExposure}_{i,t}$						
Dependent Variable:	Future Cyberattack					
	Within 1 Quarter		Within 4 Quarters		Within 8 Quarters	
	(1)	(2)	(3)	(4)	(5)	(6)
Odds Ratio	1.093***	1.102***	1.085***	1.128***	1.119***	1.139***
	(0.019)	(0.039)	(0.018)	(0.024)	(0.029)	(0.030)
Controls	×	✓	×	✓	×	✓
Industry FE	✓	✓	✓	✓	✓	✓
Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly
Observations	119,521	95,088	122,640	97,617	125,470	99,890
Pseudo R^2	0.057	0.117	0.050	0.103	0.046	0.096

Table B.VII: Cyber Risk Exposure and Firm Characteristics by Earnings Call Section and Participant

This table reports regressions of quarterly firm-level cyber risk measures on various firm characteristics. Specifications in columns (1)-(4) use as dependent variables $\text{CRExposure}^{\text{Pres}}_{\text{i,t}}$, $\text{CRExposure}^{\text{Q\&A}}_{\text{i,t}}$, $\text{CRExposure}^{\text{Exec}}_{\text{i,t}}$, and $\text{CRExposure}^{\text{Part}}_{\text{i,t}}$, respectively. $\text{CRExposure}^{\text{Pres}}_{\text{i,t}}$ and $\text{CRExposure}^{\text{Q\&A}}_{\text{i,t}}$ measure relative frequency with which cyber risk exposure keywords get mentioned in the presentation and Q&A sections of earnings calls, respectively. $\text{CRExposure}^{\text{Exec}}_{\text{i,t}}$ and $\text{CRExposure}^{\text{Part}}_{\text{i,t}}$ measure relative frequency with which cyber risk exposure keywords get mentioned by corporate executives and external participants, respectively. Table A.1 provides the full list of keywords. Table A.2 provides detailed variable definitions. All specifications include an industry x time fixed effect. All variables have been standardized to have a mean of zero and standard deviation of unity. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

Dependent Variable:	$\text{CRExposure}^{\text{Pres}}_{\text{i,t}}$	$\text{CRExposure}^{\text{Q\&A}}_{\text{i,t}}$	$\text{CRExposure}^{\text{Exec}}_{\text{i,t}}$	$\text{CRExposure}^{\text{Part}}_{\text{i,t}}$
	(1)	(2)	(3)	(4)
Log (Size)	-0.011	0.158***	0.067***	0.113***
	(0.017)	(0.015)	(0.017)	(0.012)
Market Beta	0.001	0.026**	0.012	0.023**
	(0.011)	(0.010)	(0.011)	(0.009)
Intangibles / Assets	0.042**	0.056***	0.055***	0.030**
	(0.016)	(0.015)	(0.016)	(0.012)
Liquidity Ratio	0.130***	0.237***	0.193***	0.194***
	(0.019)	(0.019)	(0.020)	(0.016)
Tobin's Q	0.004	0.111***	0.054***	0.077***
	(0.015)	(0.024)	(0.016)	(0.018)
CAPEX / Assets	-0.024	0.004	-0.016	0.019
	(0.016)	(0.015)	(0.016)	(0.012)
Cash Flow / Assets	0.075***	0.082***	0.092***	0.043**
	(0.027)	(0.023)	(0.026)	(0.019)
Log (Age)	0.036***	0.032***	0.037***	0.031***
	(0.011)	(0.010)	(0.011)	(0.009)
Book to Market Ratio	0.029**	-0.037***	0.001	-0.016*
	(0.012)	(0.010)	(0.011)	(0.009)
Leverage	0.025**	0.013	0.024**	0.010
	(0.012)	(0.011)	(0.012)	(0.010)
PP&E / Assets	-0.053***	-0.044***	-0.060***	-0.018
	(0.019)	(0.017)	(0.019)	(0.014)
Debt Maturity Ratio	-0.004	0.011	0.003	-0.002
	(0.009)	(0.008)	(0.009)	(0.007)
Equity Issuance Ratio	0.051***	-0.014	0.033**	-0.031**
	(0.015)	(0.015)	(0.015)	(0.012)
Turnover Ratio	-0.147***	-0.341***	-0.247***	-0.299***
	(0.041)	(0.048)	(0.045)	(0.043)
Operat. Costs / Assets	0.110***	0.288***	0.199***	0.250***
	(0.041)	(0.048)	(0.044)	(0.043)
Controls	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm
Frequency	Quarterly	Quarterly	Quarterly	Quarterly
Observations	116,939	116,939	116,939	116,939
R^2	0.241	0.252	0.305	0.131

Table B.VIII: Cyber Risk Exposure and Firm Characteristics by Region

This table reports regressions of quarterly firm-level cyber risk exposure on various firm characteristics by region. Columns (1)-(6) restrict the estimation sample to firms that are headquartered only in the U.S., Americas excluding U.S., Europe, U.K, Asia, and Africa, respectively. $\text{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include industry and time fixed effects. All variables have been standardized to have a mean of zero and standard deviation of unity. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

Dependent Variable (std):	$\text{CRExposure}_{i,t}$					
Region:	US	Americas	Europe	UK	Asia	Africa
	(1)	(2)	(3)	(4)	(5)	(6)
Log (Size)	0.080***	0.001	0.053	0.084	-0.126	-0.091
	(0.019)	(0.054)	(0.066)	(0.106)	(0.097)	(0.181)
Market Beta	0.017	-0.062**	0.062	-0.017	0.027	0.123
	(0.012)	(0.025)	(0.043)	(0.051)	(0.074)	(0.156)
Intangibles / Assets	0.058***	0.091*	-0.020	0.015	0.146	0.393*
	(0.017)	(0.051)	(0.110)	(0.052)	(0.128)	(0.232)
Liquidity Ratio	0.221***	0.170**	0.163	0.184*	-0.235*	0.226
	(0.022)	(0.071)	(0.112)	(0.099)	(0.125)	(0.148)
Tobin's Q	0.066***	-0.007	0.051	0.193**	-0.011	0.087
	(0.017)	(0.034)	(0.063)	(0.083)	(0.053)	(0.212)
CAPEX / Assets	-0.009	-0.028	-0.109	0.003	-0.140	-0.071
	(0.017)	(0.055)	(0.090)	(0.049)	(0.105)	(0.133)
Cash Flow / Assets	0.102***	0.048	0.010	0.021	0.319	0.163
	(0.029)	(0.077)	(0.079)	(0.084)	(0.203)	(0.192)
Log (Age)	0.036***	0.019	0.022	0.010	0.126	0.100
	(0.013)	(0.029)	(0.055)	(0.053)	(0.079)	(0.207)
Book to Market Ratio	0.009	-0.014	-0.016	-0.071	-0.131***	-0.195
	(0.012)	(0.021)	(0.021)	(0.057)	(0.042)	(0.121)
Leverage	0.032**	0.028	-0.046	-0.106	-0.146**	-0.117
	(0.012)	(0.040)	(0.111)	(0.071)	(0.066)	(0.115)
PP&E / Assets	-0.074***	0.109***	-0.265**	0.098	0.006	0.133
	(0.020)	(0.041)	(0.132)	(0.162)	(0.110)	(0.245)
Debt Maturity Ratio	-0.006	0.071***	0.076	-0.078	0.137**	-0.005
	(0.009)	(0.022)	(0.047)	(0.054)	(0.055)	(0.065)
Equity Issuance Ratio	0.022	-0.007	0.012	0.047	-0.006	0.082
	(0.017)	(0.037)	(0.093)	(0.076)	(0.099)	(0.087)
Turnover Ratio	-0.264***	-0.476***	-0.411*	-0.336	-1.091***	-0.362
	(0.050)	(0.150)	(0.238)	(0.313)	(0.362)	(0.376)
Operat. Costs / Assets	0.214***	0.462***	0.110	0.181	0.872**	0.133
	(0.050)	(0.145)	(0.209)	(0.346)	(0.355)	(0.346)
Controls	✓	✓	✓	✓	✓	✓
Industry FE	✓	✓	✓	✓	✓	✓
Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly
Observations	100,757	8,072	3,692	971	2,595	884
R^2	0.287	0.384	0.369	0.697	0.506	0.404

Table B.IX: Cyber Risk Exposure and Firm Characteristics by Industry

This table reports regressions of quarterly firm-level cyber risk exposure on various firm characteristics by industry. Columns (1)-(6) restrict the estimation sample to firms that belong only to the mining, manufacturing, trade, I.T., finance, or real estate sector. $\text{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include country and time fixed effects. All variables have been standardized to have a mean of zero and standard deviation of unity. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

Dependent Variable:	$\text{CRExposure}_{i,t}$					
Industry:	Mining	Manufacturing	Trade	IT	Finance	Real Estate
	(1)	(2)	(3)	(4)	(5)	(6)
Log (Size)	-0.115	0.074**	0.103***	-0.124*	0.071***	0.107***
	(0.087)	(0.031)	(0.029)	(0.063)	(0.028)	(0.034)
Market Beta	0.030	-0.045**	0.102***	0.126***	0.016	0.015
	(0.043)	(0.022)	(0.037)	(0.045)	(0.016)	(0.030)
Intangibles / Assets	-0.209	-0.009	0.062	0.024	0.045*	0.020
	(0.128)	(0.091)	(0.049)	(0.035)	(0.024)	(0.043)
Liquidity Ratio	-0.125	0.020	-0.072	-0.110	0.322***	0.039
	(0.117)	(0.064)	(0.091)	(0.069)	(0.028)	(0.047)
Tobin's Q	-0.137	-0.039	0.028	0.135	0.053**	-0.048*
	(0.190)	(0.027)	(0.100)	(0.110)	(0.025)	(0.025)
CAPEX / Assets	0.036	-0.092**	0.017	-0.084	-0.134***	-0.144***
	(0.056)	(0.038)	(0.046)	(0.074)	(0.032)	(0.040)
Cash Flow / Assets	-0.110*	0.129**	0.002	0.100	0.065**	0.123
	(0.056)	(0.050)	(0.102)	(0.124)	(0.027)	(0.075)
Log (Age)	-0.063	-0.026	-0.075**	-0.004	0.022	-0.003
	(0.051)	(0.024)	(0.033)	(0.032)	(0.016)	(0.021)
Book to Market Ratio	0.012	0.003	0.002	-0.020	0.038*	-0.001
	(0.063)	(0.011)	(0.025)	(0.046)	(0.021)	(0.012)
Leverage	-0.040	0.021	0.042	0.004	-0.012	-0.061**
	(0.090)	(0.024)	(0.045)	(0.040)	(0.016)	(0.026)
PP&E / Assets	-0.178	-0.016	-0.052	-0.028	-0.099***	-0.039
	(0.186)	(0.052)	(0.048)	(0.066)	(0.031)	(0.035)
Debt Maturity Ratio	0.084	0.027*	-0.064	0.044**	0.017	0.010
	(0.075)	(0.015)	(0.042)	(0.022)	(0.014)	(0.021)
Equity Issuance Ratio	-0.019	-0.011	0.086	-0.098	0.021	-0.027
	(0.073)	(0.025)	(0.124)	(0.165)	(0.018)	(0.034)
Turnover Ratio	0.288	-0.215***	-0.030	-0.220	-0.308***	-0.060
	(0.164)	(0.076)	(0.260)	(0.172)	(0.054)	(0.060)
Operat. Costs / Assets	-0.298*	0.151**	-0.002	0.238	0.217***	0.040
	(0.151)	(0.066)	(0.250)	(0.198)	(0.059)	(0.058)
Controls	✓	✓	✓	✓	✓	✓
Country FE	✓	✓	✓	✓	✓	✓
Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly	Quarterly
Observations	240	5,301	4,347	1,850	48,903	14,038
R^2	0.277	0.118	0.278	0.191	0.283	0.149

Table B.X: Firm-level Cyber Risk Exposure and Economic Outcomes by Earnings Call Section

This table reports regressions of stock market, option market, and balance sheet variables on measures of cyber risk exposure by earnings call section. In Panel A, the independent variable is $\text{CRExposure}_{i,t}^{\text{Pres}}$. In Panel B, the independent variable is $\text{CRExposure}_{i,t}^{\text{Q\&A}}$. $\text{CRet}_{i,t}$ is cumulative quarterly return, $\text{RV}_{i,t}$ is realized volatility of returns, $\text{IV}_{i,t}$ is implied option volatility, $\text{VRP}_{i,t}$ is the variance risk premium, $\text{SlopeD}_{i,d}$ is implied volatility slope, and $\text{RoA}_{i,t}$ is the return on assets. $\text{CRExposure}_{i,t}^{\text{Pres}}$ and $\text{CRExposure}_{i,t}^{\text{Q\&A}}$ measure relative frequency with which cyber risk exposure keywords get mentioned in the presentation and Q&A sections of earnings calls. Table A.1 provides the full list of keywords. All specifications include an industry x time fixed effect. Dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

	Panel A: Presentation Section					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{CRet}_{i,t}$	$\text{RV}_{i,t}$	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$	$\text{RoA}_{i,t}$
$\text{CRExposure}_{i,t}^{\text{Pres}}$	-0.008**	0.023***	0.050***	0.042***	0.020	-0.072***
	(0.003)	(0.007)	(0.008)	(0.007)	(0.012)	(0.010)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,369	102,353	102,251	102,236	102,213	102,369
R^2	0.325	0.552	0.570	0.187	0.279	0.248
	Panel B: Question and Answer Section					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{CRet}_{i,t}$	$\text{RV}_{i,t}$	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$	$\text{RoA}_{i,t}$
$\text{CRExposure}_{i,t}^{\text{Q\&A}}$	-0.008**	0.010*	0.028***	0.025***	0.029***	-0.092***
	(0.003)	(0.006)	(0.006)	(0.006)	(0.010)	(0.011)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,369	102,353	102,251	102,236	102,213	102,369
R^2	0.325	0.552	0.568	0.186	0.280	0.250

Table B.XI: Firm-level Cyber Risk Exposure and Economic Outcomes by Earnings Call Participant

This table reports regressions of stock market, option market, and balance sheet variables on measures of cyber risk exposure by earnings call participant. In Panel A, the independent variable is $\text{CRExposure}^{\text{Exec}}_{\text{i,t}}$. In Panel B, the independent variable is $\text{CRExposure}^{\text{Part}}_{\text{i,t}}$. $\text{CRet}_{\text{i,t}}$ is cumulative quarterly return, $\text{RV}_{\text{i,t}}$ is realized volatility of returns, $\text{IV}_{\text{i,t}}$ is implied option volatility, $\text{VRP}_{\text{i,t}}$ is the variance risk premium, $\text{SlopeD}_{\text{i,d}}$ is implied volatility slope, and $\text{RoA}_{\text{i,t}}$ is the return on assets. $\text{CRExposure}^{\text{Exec}}_{\text{i,t}}$ and $\text{CRExposure}^{\text{Part}}_{\text{i,t}}$ measure relative frequency with which cyber risk exposure keywords get mentioned by corporate executives and external participants, respectively. Table A.1 provides the full list of keywords. All specifications include an industry x time fixed effect. Dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}\text{p} < 0.1$; $^{**}\text{p} < 0.05$; $^{***}\text{p} < 0.01$.

	Panel A: Firm Executives					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{CRet}_{\text{i,t}}$	$\text{RV}_{\text{i,t}}$	$\text{IV}_{\text{i,t}}$	$\text{VRP}_{\text{i,t}}$	$\text{SlopeD}_{\text{i,t}}$	$\text{RoA}_{\text{i,t}}$
$\text{CRExposure}^{\text{Exec}}_{\text{i,t}}$	-0.012***	0.021***	0.050***	0.042***	0.028**	-0.098***
	(0.003)	(0.007)	(0.008)	(0.007)	(0.013)	(0.012)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,369	102,353	102,251	102,236	102,213	102,369
R^2	0.325	0.552	0.570	0.187	0.280	0.251
	Panel B: External Participants					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{CRet}_{\text{i,t}}$	$\text{RV}_{\text{i,t}}$	$\text{IV}_{\text{i,t}}$	$\text{VRP}_{\text{i,t}}$	$\text{SlopeD}_{\text{i,t}}$	$\text{RoA}_{\text{i,t}}$
$\text{CRExposure}^{\text{Part}}_{\text{i,t}}$	-0.001	0.010**	0.024***	0.022***	0.024***	-0.069***
	(0.003)	(0.004)	(0.005)	(0.005)	(0.008)	(0.008)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,369	102,353	102,251	102,236	102,213	102,369
R^2	0.325	0.552	0.568	0.186	0.280	0.248

Table B.XII: Firm-level Cyber Risk Exposure Effects with Additional Risk Exposure Controls

This table reports regressions of stock market, option market, and balance sheet variables on $\text{CRExposure}_{i,t}$ with additional controls. In Panel A, the additional control is firm-level political risk exposure from Hassan et al. (2019) In Panel B, the additional control is firm-level exposure to epidemic diseases from Hassan et al. (2023). $\text{CRet}_{i,t}$ is cumulative quarterly return, $\text{RV}_{i,t}$ is realized volatility of returns, $\text{IV}_{i,t}$ is implied option volatility, $\text{VRP}_{i,t}$ is the variance risk premium, $\text{SlopeD}_{i,d}$ is implied volatility slope, and $\text{RoA}_{i,t}$ is the return on assets. $\text{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include an industry x time fixed effect. Dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

	Panel A: Controlling for Firm-level Political Risk					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{CRet}_{i,t}$	$\text{RV}_{i,t}$	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$	$\text{RoA}_{i,t}$
$\text{CRExposure}_{i,t}$	-0.008**	0.019***	0.050***	0.041***	0.027**	-0.100***
	(0.004)	(0.007)	(0.008)	(0.007)	(0.014)	(0.013)
Political Risk Exposure	-0.010***	0.007*	0.011**	0.003	-0.001	-0.012**
	(0.003)	(0.004)	(0.004)	(0.003)	(0.010)	(0.006)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	88,504	88,491	88,430	88,418	88,399	88,504
R^2	0.337	0.561	0.566	0.200	0.286	0.226
	Panel B: Controlling for Firm-level COVID-19 Exposure					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{CRet}_{i,t}$	$\text{RV}_{i,t}$	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$	$\text{RoA}_{i,t}$
$\text{CRExposure}_{i,t}$	-0.009**	0.019***	0.050***	0.041***	0.027*	-0.100***
	(0.004)	(0.007)	(0.008)	(0.007)	(0.014)	(0.013)
COVID-19 Exposure	-0.028***	-0.000	0.008	0.008	0.001	0.001
	(0.005)	(0.006)	(0.007)	(0.007)	(0.009)	(0.009)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	88,507	88,494	88,433	88,421	88,402	88,507
R^2	0.337	0.561	0.566	0.200	0.286	0.226

Table B.XIII: Firm-level Cyber Risk Exposure Effects with Additional Balance Sheet Controls

This table reports regressions of stock market, option market, and balance sheet variables on $\mathrm{CRExposure_{i,t}}$ with additional controls. In Panel A, the additional control is the ratio of R&D expenditures to total assets. In Panel B, the additional control is the ratio of operational costs to total assets. $\mathrm{CRet_{i,t}}$ is cumulative quarterly return, $\mathrm{RV_{i,t}}$ is realized volatility of returns, $\mathrm{IV_{i,t}}$ is implied option volatility, $\mathrm{VRP_{i,t}}$ is the variance risk premium, $\mathrm{SlopeD_{i,d}}$ is implied volatility slope, and $\mathrm{RoA_{i,t}}$ is the return on assets. $\mathrm{CRExposure_{i,t}}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include an industry x time fixed effect. Dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}\mathrm{p} < 0.1$; $^{**}\mathrm{p} < 0.05$; $^{***}\mathrm{p} < 0.01$.

	Panel A: Controlling for R&D Costs					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\mathrm{CRet_{i,t}}$	$\mathrm{RV_{i,t}}$	$\mathrm{IV_{i,t}}$	$\mathrm{VRP_{i,t}}$	$\mathrm{SlopeD_{i,t}}$	$\mathrm{RoA_{i,t}}$
$\mathrm{CRExposure_{i,t}}$	0.005	0.009	0.028***	0.025***	0.044***	-0.029**
	(0.004)	(0.009)	(0.010)	(0.009)	(0.014)	(0.013)
R&D Costs	-0.047***	0.060***	0.123***	0.110***	0.020	-0.447***
	(0.008)	(0.012)	(0.015)	(0.017)	(0.022)	(0.026)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	44,474	44,468	44,437	44,432	44,436	44,474
$\mathrm{R^2}$	0.324	0.541	0.592	0.188	0.293	0.397
	Panel B: Controlling for Operational Costs					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\mathrm{CRet_{i,t}}$	$\mathrm{RV_{i,t}}$	$\mathrm{IV_{i,t}}$	$\mathrm{VRP_{i,t}}$	$\mathrm{SlopeD_{i,t}}$	$\mathrm{RoA_{i,t}}$
$\mathrm{CRExposure_{i,t}}$	-0.010***	0.019***	0.046***	0.039***	0.029**	-0.096***
	(0.003)	(0.007)	(0.008)	(0.007)	(0.013)	(0.012)
Operational Costs	0.001	-0.005	-0.029***	-0.023*	-0.011	0.163***
	(0.016)	(0.010)	(0.009)	(0.014)	(0.013)	(0.044)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	96,488	96,478	96,418	96,409	96417	96488
$\mathrm{R^2}$	0.331	0.554	0.570	0.187	0.286	0.243

Table B.XIV: Firm-level Cyber Risk Exposure Effects and Excluding Select Firms

This table reports regressions of stock market, option market, and balance sheet variables on $\mathrm{CRExposure_{i,t}}$ while excluding select industries. In Panel A, the estimation sample excludes IT firms (NAICS 51 sector). In Panel B, the estimate sample excludes financial firms (NAICS 52 sector). $\mathrm{CRet_{i,t}}$ is cumulative quarterly return, $\mathrm{RV_{i,t}}$ is realized volatility of returns, $\mathrm{IV_{i,t}}$ is implied option volatility, $\mathrm{VRP_{i,t}}$ is the variance risk premium, $\mathrm{SlopeD_{i,d}}$ is implied volatility slope, and $\mathrm{RoA_{i,t}}$ is the return on assets. $\mathrm{CRExposure_{i,t}}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include an industry x time fixed effect. Dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}\mathrm{p} < 0.1$; $^{**}\mathrm{p} < 0.05$; $^{***}\mathrm{p} < 0.01$.

	Panel A: Excluding IT Firms					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\mathrm{CRet_{i,t}}$	$\mathrm{RV_{i,t}}$	$\mathrm{IV_{i,t}}$	$\mathrm{VRP_{i,t}}$	$\mathrm{SlopeD_{i,t}}$	$\mathrm{RoA_{i,t}}$
$\mathrm{CRExposure_{i,t}}$	-0.022***	0.047***	0.083***	0.055***	0.033*	-0.141***
	(0.004)	(0.009)	(0.009)	(0.008)	(0.017)	(0.015)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	91,596	91,580	91,483	91,468	91,451	91,596
$\mathrm{R^2}$	0.328	0.556	0.574	0.196	0.291	0.264
	Panel B: Excluding Financial Firms					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\mathrm{CRet_{i,t}}$	$\mathrm{RV_{i,t}}$	$\mathrm{IV_{i,t}}$	$\mathrm{VRP_{i,t}}$	$\mathrm{SlopeD_{i,t}}$	$\mathrm{RoA_{i,t}}$
$\mathrm{CRExposure_{i,t}}$	-0.008**	0.026***	0.055***	0.045***	0.037***	-0.110***
	(0.003)	(0.007)	(0.008)	(0.008)	(0.014)	(0.013)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	90,378	90,362	90,280	90,265	90,245	90,378
$\mathrm{R^2}$	0.321	0.548	0.579	0.184	0.290	0.275

Table B.XV: Firm-level and Time-series Dimensions of Cyber Risk Exposure

This table reports regressions of stock market, option market, and balance sheet variables on firm-level cyber risk exposure, $\mathrm{CRExposure}_{i,t}$, and the time-series average of $\mathrm{CRExposure}_{i,t}$. $\mathrm{CRet}_{i,t}$ is cumulative quarterly return, $\mathrm{RV}_{i,t}$ is realized volatility of returns, $\mathrm{IV}_{i,t}$ is implied option volatility, $\mathrm{VRP}_{i,t}$ is the variance risk premium, $\mathrm{SlopeD}_{i,d}$ is implied volatility slope, and $\mathrm{RoA}_{i,t}$ is the return on assets. $\mathrm{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include an industry fixed effect. Dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}\mathrm{p} < 0.1$; $^{**}\mathrm{p} < 0.05$; $^{***}\mathrm{p} < 0.01$.

	Panel A: CRet, RV, IV					
Dependent Variable (std)	$\mathrm{CRet}_{i,t}$		$\mathrm{RV}_{i,t}$		$\mathrm{IV}_{i,t}$	
	(1)	(2)	(3)	(4)	(5)	(6)
$\mathrm{CRExposure}_{i,t}$ (std)	-0.025***	-0.015***	0.060***	0.027***	0.090***	0.052***
	(0.004)	(0.004)	(0.008)	(0.007)	(0.009)	(0.008)
Mean of $\mathrm{CRExposure}_{i,t}$ (std)		-0.251***		0.773***		0.907***
		(0.016)		(0.028)		(0.031)
Controls	✓	✓	✓	✓	✓	✓
Industry FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,435	102,435	102,419	102,419	102,317	102,317
R^2	0.027	0.030	0.251	0.278	0.399	0.441
	Panel B: VRP, SlopeD, RoA					
Dependent Variable (std)	$\mathrm{VRP}_{i,t}$		$\mathrm{SlopeD}_{i,t}$		$\mathrm{RoA}_{i,t}$	
	(1)	(2)	(3)	(4)	(5)	(6)
$\mathrm{CRExposure}_{i,t}$ (std)	0.055***	0.038***	0.040***	0.029**	-0.128***	-0.106***
	(0.007)	(0.007)	(0.012)	(0.013)	(0.012)	(0.012)
Mean of $\mathrm{CRExposure}_{i,t}$ (std)		0.389***		0.253***		-0.524***
		(0.029)		(0.047)		(0.045)
Controls	✓	✓	✓	✓	✓	✓
Industry FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,302	102,302	102,279	102,279	102,435	102,435
R^2	0.072	0.081	0.221	0.224	0.223	0.234

Table B.XVI: Firm-level Cyber Risk Exposure and Option Outcomes by Maturity

This table reports robustness regressions of option market variables of different maturity on the baseline firm-level cyber risk exposure, $\text{CRExposure}_{i,t}$. $\text{IV}_{i,t}$ is implied volatility, $\text{VRP}_{i,t}$ is the variable risk premium, and $\text{SlopeD}_{i,t}$ is the implied volatility slope. $\text{CRExposure}_{i,t}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include an industry x time fixed effect. All dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}p < 0.1$; $^{**}p < 0.05$; $^{***}p < 0.01$.

	Panel A: 30 Days			Panel B: 60 Days		
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$
$\text{CRExposure}_{i,t}$	0.051***	0.042***	0.026**	0.052***	0.046***	0.025**
	(0.008)	(0.008)	(0.012)	(0.008)	(0.008)	(0.013)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,251	102,224	102,214	102,251	102,232	102,212
R^2	0.487	0.138	0.266	0.540	0.160	0.287
	Panel C: 182 days			Panel D: 365 days		
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$	$\text{IV}_{i,t}$	$\text{VRP}_{i,t}$	$\text{SlopeD}_{i,t}$
$\text{CRExposure}_{i,t}$	0.050***	0.039***	0.031**	0.051***	0.038***	0.036***
	(0.008)	(0.007)	(0.013)	(0.008)	(0.007)	(0.013)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	102,251	102,245	102,165	102,251	102,247	1019,99
R^2	0.592	0.231	0.322	0.598	0.270	0.348

Table B.XVII: Further Robustness of Firm-Level Cyber Risk Exposure Effects

This table reports regressions of stock market, option market, and balance sheet variables on the baseline measure of firm-level cyber risk exposure, $\mathrm{CRExposure_{i,t}}$, for various sub-samples. In Panel A, the sample is restricted to U.S. firms only. In Panel B, the sample ends in 2020Q1. $\mathrm{CRet_{i,t}}$ is cumulative quarterly return, $\mathrm{RV_{i,t}}$ is realized volatility of returns, $\mathrm{IV_{i,t}}$ is implied option volatility, $\mathrm{VRP_{i,t}}$ is the variance risk premium, $\mathrm{SlopeD_{i,d}}$ is implied volatility slope, and $\mathrm{RoA_{i,t}}$ is the return on assets. $\mathrm{CRExposure_{i,t}}$ measures the relative frequency with which cybersecurity-related keywords are mentioned in the earnings calls. Table A.1 provides the full list of keywords. All specifications include an industry x time fixed effect. All dependent and independent variables have been standardized to have a mean of zero and standard deviation of unity. Firm controls include firm size, age, Tobin's Q, leverage ratio, liquidity ratio, intangible asset ratio, operational cost ratio, and the market beta. Table A.2 provides detailed variable definitions. Standard errors, clustered at the firm level, are in parentheses. $^{*}\mathrm{p} < 0.1$; $^{**}\mathrm{p} < 0.05$; $^{***}\mathrm{p} < 0.01$.

	Panel A: Only US Firms					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\mathrm{CRet_{i,t}}$	$\mathrm{RV_{i,t}}$	$\mathrm{IV_{i,t}}$	$\mathrm{VRP_{i,t}}$	$\mathrm{SlopeD_{i,t}}$	$\mathrm{RoA_{i,t}}$
$\mathrm{CRExposure_{i,t}}$	-0.012***	0.028***	0.060***	0.048***	0.029**	-0.100***
	(0.004)	(0.008)	(0.008)	(0.008)	(0.014)	(0.013)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	88623	88609	88536	88523	88506	88623
R^2	0.329	0.558	0.588	0.192	0.280	0.262
	Panel B: Sample Ends in 2020Q1					
	(1)	(2)	(3)	(4)	(5)	(6)
Dependent Variable (std)	$\mathrm{CRet_{i,t}}$	$\mathrm{RV_{i,t}}$	$\mathrm{IV_{i,t}}$	$\mathrm{VRP_{i,t}}$	$\mathrm{SlopeD_{i,t}}$	$\mathrm{RoA_{i,t}}$
$\mathrm{CRExposure_{i,t}}$	-0.009**	0.024***	0.055***	0.040***	0.028*	-0.114***
	(0.004)	(0.008)	(0.008)	(0.007)	(0.015)	(0.015)
Controls	✓	✓	✓	✓	✓	✓
Industry x Time FE	✓	✓	✓	✓	✓	✓
Level	Firm	Firm	Firm	Firm	Firm	Firm
Frequency	Quarter	Quarter	Quarter	Quarter	Quarter	Quarter
Observations	73999	73990	73949	73941	73933	73999
R^2	0.336	0.571	0.542	0.201	0.295	0.212

References

Hassan, T., S. Hollander, L. v. Lent, and A. Tahoun (2019): "Firm-Level Political Risk: Measurement and Effects," *Quarterly Journal of Economics*, 134, 2135–2202.

——— (2023): "Firm-Level Exposure to Epidemic Diseases: Covid-19, SARS, and H1N1," *The Review of Financial Studies*, 36, 4919–4964.